

Изучи, подготовься, попрактикуйся и успешно сдай экзамен!

Официальное руководство Cisco

по подготовке к сертификационным экзаменам



- ▶ Изучите темы экзамена ICND1 640-822
- ▶ Оцените свои знания с помощью контрольных вопросов
- ▶ Повторите ключевые концепции в разделах для подготовки к экзаменам
- ▶ Попрактикуйтесь в сдаче тестов с помощью программного обеспечения на прилагаемом DVD

CCENT/ CCNA ICND1 640-822

Третье издание



Официальное
руководство Cisco
по подготовке к сертификационным экзаменам
CCENT/CCNA ICND1 640-822

Третье издание

CCENT/CCNA ICND1

640-822 Official Cert Guide

Third Edition

Wendell Odom, CCIE No. 1624

Cisco Press

800 East 96th Street
Indianapolis, IN 46240 USA

Официальное **руководство Cisco** по подготовке к сертификационным экзаменам **CCENT/CCNA ICND1 640-822**

Третье издание

Уэнделл Одом, CCIE No. 1624



Москва • Санкт-Петербург • Киев
2013

ББК 32.973.26-018.2.75

О-44

УДК 681.3.07

Издательский дом “Вильямс”

Зав. редакцией *С.Н. Тригуб*

Перевод с английского и редакция *В.А. Коваленко*

По общим вопросам обращайтесь в Издательский дом “Вильямс” по адресу:
info@williamspublishing.com, <http://www.williamspublishing.com>

Одом, Уэнделл.

О-44 Официальное руководство Cisco по подготовке к сертификационным экзаменам CCENT/CCNA ICND1 640-822, 3-е изд. : Пер. с англ. — М. : ООО “И.Д. Вильямс”, 2013. — 720 с. : ил. — Парал. тит. англ.

ISBN 978-5-8459-1807-9 (рус.)

ББК 32.973.26-018.2.75

Все названия программных продуктов являются зарегистрированными торговыми марками соответствующих фирм.

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

Authorized translation from the English language edition published by Cisco Press, Copyright © 2012 by Pearson Education, Inc.

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without written permission from the Publisher, except for the inclusion of brief quotations in a review.

Russian language edition published by Williams Publishing House according to the Agreement with R&I Enterprises International, Copyright © 2013

Научно-популярное издание

Уэнделл Одом

Официальное руководство Cisco

по подготовке к сертификационным

экзаменам CCENT/CCNA ICND1 640-822, 3-е издание

Литературный редактор *И.А. Попова*

Верстка *О.В. Мишутина*

Художественный редактор *В.Г. Павлютин*

Корректор *Л.А. Гордиенко*

Подписано в печать 28.08.2012. Формат 70x100/16.

Гарнитура Times. Печать офсетная.

Усл. печ. л. 58,05. Уч.-изд. л. 44,05.

Тираж 1000 экз. Заказ № 0000.

Первая Академическая типография “Наука”

199034, Санкт-Петербург, 9-я линия, 12/28

ООО “И. Д. Вильямс”, 127055, г. Москва, ул. Лесная, д. 43, стр. 1

ISBN 978-5-8459-1807-9 (рус.)

ISBN 978-1-58-720425-8 (англ.)

© Издательский дом “Вильямс”, 2013

© Pearson Education, Inc., 2012

Оглавление

Введение	18
<hr/>	
Часть I. Основы сетей	39
Глава 1. Введение в компьютерные сети	41
Глава 2. Сетевые модели TCP/IP и OSI	53
Глава 3. Основы сетей LAN	81
Глава 4. Основы сетей WAN	111
Глава 5. Основы адресации и маршрутизации IPv4	137
Глава 6. Основы протокола TCP/IP: передача данных, приложения и безопасность	171
<hr/>	
Часть II. Коммутация в локальных сетях	205
Глава 7. Базовые концепции коммутации Ethernet	207
Глава 8. Работа с коммутаторами компании Cisco	235
Глава 9. Настройка коммутаторов Ethernet	267
Глава 10. Поиск и устранение неисправностей в коммутаторах Ethernet	299
Глава 11. Беспроводные локальные сети	329
<hr/>	
Часть III. IPv4-адресация и создание подсетей	361
Глава 12. Перспективы создания подсетей IPv4	363
Глава 13. Анализ классовых сетей IPv4	389
Глава 14. Преобразование маски подсети	405
Глава 15. Анализ существующих масок подсети	415
Глава 16. Разработка маски подсети	427
Глава 17. Анализ существующих подсетей	441
Глава 18. Поиск всех идентификаторов подсети	469

Часть IV. Маршрутизация IPv4	485
Глава 19. Работа с маршрутизаторами компании Cisco	487
Глава 20. Концепции и конфигурирование протоколов маршрутизации	521
Глава 21. Поиск и устранение неисправностей маршрутизации	557
Часть V. Распределенные сети	593
Глава 22. Базовые концепции распределенных сетей	595
Глава 23. Конфигурирование соединений WAN	623
Часть VI. Подготовка к экзамену	645
Глава 24. Подготовка к сертификационному экзамену	647
Часть VII. Приложения (в книге)	657
Приложение А. Ответы на контрольные вопросы	659
Приложение Б. Справочные числовые таблицы	681
Приложение В. Обновление экзамена ICND1: версия 1.0	687
Словарь терминов	691
Предметный указатель	712
Часть VIII. Приложения (на компакт-диске)	722
Приложение Г. “Практические задачи для главы 13: анализ классовых сетей IPv4”	724
Приложение Д. “Практические задачи для главы 14: преобразование маски подсети”	727
Приложение Е. “Практические задачи для главы 15: анализ существующих масок подсети”	733
Приложение Ж. “Практические задачи для главы 16: разработка маски подсети”	738
Приложение З. “Практические задачи для главы 17: анализ существующих подсетей”	748
Приложение И. “Практические задачи для главы 18: поиск всех идентификаторов подсети”	785
Приложение К. “Дополнительные сценарии”	795
Приложение Л. “Видеоматериалы”	815
Приложение М. “Таблицы для запоминания материала”	838
Приложение Н. “Таблицы для запоминания материала с ответами”	851
Приложение О. “Дополнительные вопросы ICND1”	862
План изучения лабораторных работ эмулятора Network Simulator	898

Содержание

Об авторе	14
Технические рецензенты	14
Посвящения	15
Благодарности	15
Условные обозначения сетевых устройств	17
Соглашения по синтаксису команд	17
Введение	18
Структура экзаменов	18
Книги новые, а экзамены Cisco остались старые	19
Формат экзамена CCNA	20
Как проводится экзамен CCNA	22
Темы экзамена ICND1	22
Темы экзамена ICND2	25
Темы экзамена CCNA 640-802	27
Темы курсов ICND1 и ICND2	27
О книге	27
Цели и методы	28
Особенности книги	28
Структура книги	30
Как использовать эту книгу для подготовки к экзаменам ICND1 и CCNA	34
Как использовать эту книгу для подготовки к экзамену CCNA 640-802	35
Дополнительная информация	36
От издательства	37
Часть I. Основы сетей	39
Глава 1. Введение в компьютерные сети	41
Что такое современные сети	41
Глава 2. Сетевые модели TCP/IP и OSI	53
Контрольные вопросы: знаете ли вы уже темы главы	54
Основные темы	57
Эталонная модель TCP/IP	57
Эталонная модель OSI	72
Подготовка к экзамену	78
Повторите все ключевые темы	78
Заполните таблицы и списки по памяти	78
Ключевые термины	78
Эталонная модель OSI	78
Глава 3. Основы сетей LAN	81
Контрольные вопросы: знаете ли вы уже темы главы	81
Основные темы	85
Обзор современных локальных сетей Ethernet	85
Краткая история технологии Ethernet	88

Витая пара в сетях Ethernet	92
Использование коммутаторов вместо концентраторов для повышения производительности сети	98
Средства канального уровня Ethernet	103
Подготовка к экзамену	109
Повторите все ключевые темы	109
Заполните таблицы и списки по памяти	109
Ключевые термины	109
Глава 4. Основы сетей WAN	111
Контрольные вопросы: знаете ли вы уже темы главы	111
Основные темы	114
Уровень 1 модели OSI в двухточечных каналах распределенной сети	114
Уровень 2 модели OSI в двухточечных каналах распределенной сети	125
Технология Frame Relay и службы с коммутацией пакетов	128
Подготовка к экзамену	134
Повторите все ключевые темы	134
Заполните таблицы и списки по памяти	134
Ключевые термины	134
Глава 5. Основы адресации и маршрутизации IPv4	137
Контрольные вопросы: знаете ли вы уже темы главы	137
Основные темы	141
Обзор функций сетевого уровня	141
IP-адресация	148
Маршрутизация IP	157
Протоколы маршрутизации IP	161
Утилиты сетевого уровня	163
Подготовка к экзамену	168
Повторите все ключевые темы	168
Заполните таблицы и списки по памяти	169
Ключевые термины	169
Глава 6. Основы протокола TCP/IP: передача данных, приложения и безопасность	171
Контрольные вопросы: знаете ли вы уже темы главы	171
Основные темы	174
Протоколы 4-го уровня стека TCP/IP: TCP и UDP	174
Приложения TCP/IP	187
Безопасность сети	194
Подготовка к экзамену	203
Повторите все ключевые темы	203
Заполните таблицы и списки по памяти	203
Ключевые термины	203
Часть II. Коммутация в локальных сетях	205
Глава 7. Базовые концепции коммутации Ethernet	207
Контрольные вопросы: знаете ли вы уже темы главы	207

Основные темы	210
Концепции коммутации в локальных сетях	210
Принципы построения локальных сетей	222
Подготовка к экзамену	233
Повторите все ключевые темы	233
Заполните таблицы и списки по памяти	233
Ключевые термины	233
Глава 8. Работа с коммутаторами компании Cisco	235
Контрольные вопросы: знаете ли вы уже темы главы	235
Основные темы	238
Доступ к интерфейсу командной строки коммутатора Cisco Catalyst 2960	239
Конфигурирование программного обеспечения Cisco IOS	253
Повторите все ключевые темы	263
Заполните таблицы и списки по памяти	264
Ключевые термины	264
Список команд	264
Глава 9. Настройка коммутаторов Ethernet	267
Контрольные вопросы: знаете ли вы уже темы главы	267
Основные темы	270
Настройка функций, общих для коммутаторов и маршрутизаторов	270
Настройка коммутаторов локальных сетей и управление ими	282
Подготовка к экзамену	295
Повторите все ключевые темы	295
Заполните таблицы и списки по памяти	295
Ключевые термины	295
Список команд	295
Глава 10. Поиск и устранение неисправностей в коммутаторах Ethernet	299
Контрольные вопросы: знаете ли вы уже темы главы	299
Основные темы	303
Принципы проверки сетей, а также поиск	303
и устранение неисправностей	303
Построение топологии сети с помощью протокола обнаружения	309
устройств Cisco	309
Анализ состояния интерфейса на 1- и 2-м уровнях	314
Анализ маршрута коммутации фреймов	321
на основе таблиц MAC-адресов	321
Подготовка к экзамену	326
Повторите все ключевые темы	326
Заполните таблицы и списки по памяти	326
Ключевые термины	326
Список команд	326
Глава 11. Беспроводные локальные сети	329
Контрольные вопросы: знаете ли вы уже темы главы	329
Основные темы	332

Концепции беспроводных сетей	332
Развертывание беспроводных сетей	345
Безопасность беспроводных сетей	350
Подготовка к экзамену	358
Повторите все ключевые темы	358
Заполните таблицы и списки по памяти	358
Ключевые термины	358
Часть III. IPv4-адресация и создание подсетей	361
Глава 12. Перспективы создания подсетей Pv4	363
Контрольные вопросы: знаете ли вы уже темы главы	363
Основные темы	366
Введение в подсети	366
Анализ потребности в подсетях и адресации	368
Выбор проекта	374
Реализация плана	384
Подготовка к экзамену	386
Повторите все ключевые темы	386
Заполните таблицы и списки по памяти	387
Ключевые термины	387
Глава 13. Анализ классовых сетей IPv4	389
Контрольные вопросы: знаете ли вы уже темы главы	389
Основные темы	391
Концепции классовых сетей	391
Практические задачи по классовым сетям	397
Подготовка к экзамену	400
Повторите все ключевые темы	400
Заполните таблицы и списки по памяти	400
Ключевые термины	400
Практика	400
Глава 14. Преобразование маски подсети	405
Контрольные вопросы: знаете ли вы уже темы главы	405
Основные темы	407
Преобразование масок подсети	407
Практические задания по преобразованию масок подсети	411
Подготовка к экзамену	413
Повторите все ключевые темы	413
Ключевые термины	413
Практика	413
Глава 15. Анализ существующих масок подсети	415
Контрольные вопросы: знаете ли вы уже темы главы	415
Основные темы	417
Определение формата IPv4-адресов	417
Практические задания по анализу масок подсети	421

Подготовка к экзамену	423
Повторите все ключевые темы	423
Ключевые термины	423
Практика	423
Глава 16. Разработка маски подсети	427
Контрольные вопросы: знаете ли вы уже темы главы	427
Основные темы	430
Выбор маски, удовлетворяющей требованиям	430
Практические задания по выбору масок подсети	436
Подготовка к экзамену	438
Повторите все ключевые темы	438
Ключевые термины	438
Практика	438
Глава 17. Анализ существующих подсетей	441
Контрольные вопросы: знаете ли вы уже темы главы	441
Основные темы	444
Определение подсети	444
Анализ существующих подсетей: двоичный	448
Анализ существующих подсетей: десятичный	454
Практические задания по анализу существующих подсетей	462
Подготовка к экзамену	464
Повторите все ключевые темы	464
Заполните таблицы и списки по памяти	464
Ключевые термины	464
Практика	464
Глава 18. Поиск всех идентификаторов подсети	469
Контрольные вопросы: знаете ли вы уже темы главы	469
Основные темы	471
Поиск всех идентификаторов подсети	471
Практические задания по поиску всех идентификаторов подсети	479
Подготовка к экзамену	481
Повторите все ключевые темы	481
Ключевые термины	481
Часть IV. Маршрутизация IPv4	485
Глава 19. Работа с маршрутизаторами компании Cisco	487
Контрольные вопросы: знаете ли вы уже темы главы	487
Основные темы	490
Установка маршрутизаторов Cisco	490
Интерфейс командной строки маршрутизатора	496
Обновление операционной системы Cisco IOS и процесс начальной загрузки устройства	507
Подготовка к экзамену	517
Повторите все ключевые темы	517

Заполните таблицы и списки по памяти	517
Ключевые термины	517
Задания приложения К	518
Список команд	518
Глава 20. Концепции и конфигурирование протоколов маршрутизации	521
Контрольные вопросы: знаете ли вы уже темы главы	521
Основные темы	525
Подключенные и статические маршруты	525
Обзор протоколов маршрутизации	534
Конфигурирование и проверка работы протокола RIP-2	542
Подготовка к экзамену	553
Повторите все ключевые темы	553
Заполните таблицы и списки по памяти	553
Ключевые термины	553
Список команд	554
Глава 21. Поиск и устранение неисправностей маршрутизации	557
Контрольные вопросы: знаете ли вы уже темы главы	557
Основные темы	561
Советы по устранению неисправностей и необходимый инструментарий	561
Сценарий поиска и устранения ошибок в маршрутизации	576
Подготовка к экзамену	590
Повторите все ключевые темы	590
Заполните таблицы и списки по памяти	590
Список команд	590
Часть V. Распределенные сети	593
Глава 22. Базовые концепции распределенных сетей	595
Контрольные вопросы: знаете ли вы уже темы главы	595
Основные темы	598
Технологии WAN	598
Службы IP для доступа к Интернету	612
Подготовка к экзамену	621
Повторите все ключевые темы	621
Заполните таблицы и списки по памяти	621
Ключевые термины	621
Глава 23. Конфигурирование соединений WAN	623
Контрольные вопросы: знаете ли вы уже темы главы	623
Основные темы	626
Конфигурирование двухточечных каналов WAN	626
Конфигурирование, поиск и устранение неисправностей для маршрутизаторов доступа к Интернету	630
Подготовка к экзамену	642
Повторите все ключевые темы	642

Заполните таблицы и списки по памяти	642
Ключевые термины	642
Список команд	642
Часть VI. Подготовка к экзамену	645
Глава 24. Подготовка к сертификационному экзамену	647
Утилиты для подготовки к экзамену	647
План подготовки к экзамену	651
Резюме	654
Часть VII. Приложения (в книге)	657
Приложение А. Ответы на контрольные вопросы	659
Приложение Б. Справочные числовые таблицы	681
Приложение В. Обновление экзамена ICND1: версия 1.0	686
Получите самые свежие материалы на веб-сайте	687
Техническая информация	688
Словарь терминов	691
Предметный указатель	712
Часть VIII. Приложения (на компакт-диске)	722
Приложение Г. “Практические задачи для главы 13: анализ классовых сетей IPv4”	724
Приложение Д. “Практические задачи для главы 14: преобразование маски подсети”	727
Приложение Е. “Практические задачи для главы 15: анализ существующих масок подсети”	733
Приложение Ж. “Практические задачи для главы 16: разработка маски подсети”	738
Приложение З. “Практические задачи для главы 17: анализ существующих подсетей”	748
Приложение И. “Практические задачи для главы 18: поиск всех идентификаторов подсети”	785
Приложение К. “Дополнительные сценарии”	795
Приложение Л. “Видеоматериалы”	815
Приложение М. “Таблицы для запоминания материала”	838
Приложение Н. “Таблицы для запоминания материала с ответами”	851
Приложение О. “Дополнительные вопросы ICND1”	862
План изучения лабораторных работ эмулятора Network Simulator	898

Об авторе

Уэнделл Одом (Wendell Odom), сертифицированный эксперт компании Cisco CCIE (Cisco Certified Internetwork Expert — сертифицированный эксперт по сетям компании Cisco) № 1624, в сфере сетевых технологий работает с 1981 года. Уэнделл работал сетевым инженером, консультантом, системным инженером, инструктором и принимал участие в разработке курсов по сетям, а ныне занимается проектированием и разработкой средств сертификации. Он является автором всех предыдущих редакций книги издательства Cisco Press для подготовки к экзаменам CCNA, книг по технологиям Cisco QOS и многих других. Он также поддерживает инструментальные средства обучения, ссылки на свои блоги и другие ресурсы на www.certskills.com.

Технические рецензенты

Элан Бир (Elan Beer) — старший консультант и инструктор Cisco, специализирующийся на проектах многопротокольных сетей, их конфигурации, решении проблем и обслуживании сетей. За последние двадцать лет Элан обучил тысячи экспертов в области маршрутизации, коммутации и архитектур центров обработки и хранения данных. Он принимал участие в крупномасштабных профессиональных проектах по разработке и внедрению объединенных сетей, проведении аудита сетей, а также помогал клиентам с их кратко- и долгосрочными проектами. Благодаря обширной международной клиентуре, Элан обладает глобальной точкой зрения на сетевые архитектуры. Он использовал свой опыт при разработке и настройке сетей в Малайзии, Северной Америке, Европе, Австралии, Африке, Китае и на Ближнем Востоке. в последнее время Элан специализируется на проектах центров обработки и хранения данных, конфигурации и решении сетевых проблем, а также на технологиях провайдера служб.

Элан Бир был одним из первых, кто получил сертификат инструктора Cisco (CCSI) в 1993 году, а в 1996 году он также одним из первых получил наивысший сертификат эксперта компании Cisco (CCIE). с тех пор он участвовал во множестве крупномасштабных международных проектов телекоммуникационных сетей и известен в мире как ведущий специалист по сетевым архитектурам и преподаватель, участвовавший во многих грандиозных проектах, помогая компаниям реализовать передовые технологии в их корпоративной инфраструктуре.

Тери Ку (Teri Cook) — инструктор CCSI (Cisco Systems Certified Instructor — сертифицированный инструктор компании Cisco Systems), специалист CCDP (Cisco Certified Design Professional — сертифицированный профессионал по дизайну сетей Cisco), CCNP (Cisco Certified Network Professional — сертифицированный профессионал по сетям Cisco), CCDA (Cisco Certified Design Associate — сертифицированный специалист по дизайну сетей компании Cisco), CCNA, MCT (Microsoft Certified Trainers — сертифицированный тренер компании Microsoft) и MCSE 2000/2003: Security (Microsoft Certified Systems Engineer — сертифицированный системный инженер компании Microsoft по безопасности). Она имеет более чем десятилетний опыт работы в сфере информационных технологий. Тери работала в разных структурах, начиная от частного бизнеса и до Министерства обороны США, обеспечивая работу сетей высшего уровня, разрабатывая системы безопасности и внедряя слож-

ные компьютерные системы. После получения сертификата специалиста Тери преподавала на курсах по сетевым технологиям как для сетевых специалистов, так и для инструкторов. Она — известный инструктор, использующий накопленный годами опыт для презентации множества сложных сетевых технологий. Более пяти лет Тери обучает специалистов Cisco в качестве IT-инструктора.

Брайан Д'Андреа (Brian D'Andrea) — сертифицированный специалист CCNA, CCDA, MCSE, A+, и Net+, имеет 11-летний опыт работы в сфере информационных технологий в медицинской и финансовой области, где основной его обязанностью было проектирование и поддержка необходимых сетевых технологий. Последние пять лет он занимается технической подготовкой. Большую часть времени Брайан посвящает компании The Training Camp, проводящей тренинги по информационным технологиям. Используя свой опыт и умение объяснять сложные концепции понятным языком, Брайан успешно обучил сотни специалистов для практической работы и подготовил их к сертификационным экзаменам.

Стивен Кальман (Stephen Kalman) — инструктор в области защиты данных. Он является автором или техническим редактором более 20 книг, курсов и компьютерных мультимедийных учебников. Его последняя книга в издательстве Cisco Press — *Web Security Field Guide (Практическое руководство по веб-безопасности)*. Кроме того, он основал консалтинговую компанию, Esquire Micro Consultants, которая специализируется на оценке и анализе безопасности сетей.

Стивен владеет следующими сертификатами: SSCP (Systems Security Certified Practitioner — сертифицированный профессионал по системной безопасности), CISSP (Certified Information Systems Security Professional — сертифицированный профессионал по безопасности информационных систем), ISSMP (Information Systems Security Management Professional — сертифицированный профессионал по управлению системами информационной безопасности), CEH (Certified Ethical Hacker — сертифицированный этичный хакер), CHFI (Computer Hacking Forensic Investigator — исследователь систем взлома компьютерных систем), CCNA (Cisco Certified Network Associate — сертифицированный специалист по сетям компании Cisco), CCSA, (Check Point Certified Security Administrator — сертифицированный администратор по безопасности компании Check Point), A+, Network+ and Security+ certifications, а также является членом ассоциации New York State Bar.

Посвящения

Посвящается Хане Одом (Hannah Odom), лучшей дочери, которую я мог бы вообразить. Я люблю тебя, моя девочка!

Благодарности

Знаете, после тридцати лет написания книг я полагал, что теперь все пройдет нормально, что-то повторится, ведь каждая книга в значительной степени имеет такую же структуру, как и другие. Но теперь мне кажется, что нормальным фактически является аномальность, требующая от всех нестандартности мышления.

Эта книга, вероятно даже более, чем любые другие ее издания, является результатом усилий всей группы. Ее основные нововведения связаны со всеми дополнениями Cisco Press, добавленными в пакет. Благодарю Дэйва, Бретт, Кортни, Сандру

и всех сотрудников издательства Cisco Press за те несколько дополнительных миль, которые пришлось пройти, чтобы сделать возможным это “дополненное” издание и внести в него множество новых дополнительных элементов. Полагаю, читатели оценят значение добавленного. Теперь подробней.

В первую очередь снимаю шляпу перед Дрю Каппом (Drew Cupp). Между прежним изданием этой книгой и нынешним мы с Дрю прошли путь от отсутствия общих книг до работы над тремя совместными, и все это за пять месяцев от начала до конца. Воспоминания об этом причиняют мне головную боль. Помимо той работы, которую предстояло сделать, разносторонние знания Дрю о том, что делать и как, его осведомленность о подробностях печати, создания DVD и сетевых вопросах оказались неоценимы. Эта книга никак не обошлась бы без Дрю. Спасибо, Дрю, ты настоящий друг!

Брайан (Brian), Тери (Teri) и Стив (Steve) — все рецензенты оказали неоценимую помощь в техническом редактировании книги. Помимо помощи в поиске ошибок и обеспечения корректности изложенного материала, каждый технический редактор внес собственный вклад в общий процесс. Надеюсь, мы сможем сотрудничать в будущем. и особая благодарность Элану Биру (Elan Beer), наилучшему техническому редактору в отрасли, за работу над новыми материалами для этого издания.

Знаете, это прекрасно, когда есть человек, на которого вы можете полагаться в любом деле, всегда готового помочь и справиться с любой задачей или проблемой. А когда этот человек фактически работает на партнерскую компанию, это еще более впечатительно. Мне очень повезло иметь такого союзника в лице Брета Барту (Brett Bartow). Большое спасибо за компанию в этом путешествии.

Мэнди Фрэнк (Mandie. Frank) удостоена премии “горячей картошки” (“hot potato”) за работу редактора проекта по этой книге и книге *ICND2*. Характер этого проекта и книги *ICND2* фактически таков, что может возникнуть немало проблем. Мэнди решала их все с изяществом иaplombом, полностью контролировала весь процесс с остальной частью рабочей группы. Спасибо Мэнди и всей группе! и особая благодарность за дополнительное внимание к обзору страниц.

Благодарю Ричарда Беннетта (Richard Bennett), который работал, как раб, по жесткому расписанию над усовершенствованием некоторых рисунков, которые я хотел включить в эту книгу, и за его работу над базой вопросов. Молодец, Робин Уильямс (Robin Williams) гордился бы тобой!

Особая благодарность читателям, которые высказывали свои предложения, находили возможные ошибки, а особенно тем из вас, кто писал сообщения в учебную сеть Cisco (Cisco Learning Network — CLN). Без сомнения, те комментарии, которые я получал лично и читал в сети CLN, сделали это издание лучше.

В заключение хочу поблагодарить мою жену Крис (Kris) за поддержку моих писательских попыток, за ее молитвы и понимание, когда сроки сдачи книги затянулись и пересеклись с нашим запланированным летним отпуском. (Да, это уже второй раз, когда эта книга заставила отказаться от отпуска, — вот такая штука!) Спасибо Иисусу Христу; все мои усилия — лишь движение против ветра без Него.

Условные обозначения сетевых устройств



Соглашения по синтаксису команд

Представленные ниже соглашения по синтаксису команд аналогичны соглашениям, используемым в *Справочнике по командам операционной системы IOS* (IOS Command Reference). В упомянутом справочнике используются следующие соглашения:

- **полужирным** шрифтом выделяются команды и ключевые слова, которые вводятся буквально, как показано; в примерах реальной конфигурации и сообщений системы. Полужирным шрифтом выделяются команды, которые вводятся пользователем вручную (например, команда **show**);
- **курсивом** выделяются аргументы, для которых пользователь указывает реальные значения;
- с помощью вертикальной черты (|) разделяются альтернативные, взаимоисключающие элементы;
- в квадратных скобках ([]) указываются необязательные элементы;
- в фигурных скобках ({ }) указываются необходимые элементы;
- в фигурных скобках, помещенных в квадратные скобки [{ }], указываются необходимые элементы в пределах необязательного элемента.

Введение

Поздравляем! Если вы дочитали эту книгу до введения, то наверняка решили получить сертификат специалиста компании Cisco. Чтобы добиться успеха на поприще технического специалиста в сетевой индустрии, современный сетевой инженер должен быть знаком с оборудованием компании Cisco. Компания имеет невероятно высокую долю на рынке оборудования для маршрутизации и коммутации, в общем — более 80% в некоторых регионах. Во многих странах и на рынке всего мира синонимом слова “сеть” является название компании Cisco. Если читатель хочет, чтобы к нему относились как к серьезному сетевому специалисту, то имеет смысл получить сертификацию компании Cisco.

Исторически сертификатом начального уровня компании Cisco был диплом сертифицированного специалиста по сетям компании Cisco (Cisco Certified Network Associate — CCNA), который появился в 1998 году. Первые три версии сертификации CCNA означали, что специалист сдал один экзамен для получения сертификата. Однако со временем темы экзамена изменялись и расширялись, причем как увеличивалось количество рассматриваемых тем, так и росла сложность вопросов. Поэтому после четвертой генеральной ревизии экзаменов, анонсированной в 2003 году, компания Cisco предложила для начального уровня одну базовую сертификацию (CCNA), но были доступны два варианта экзамена: один общий экзамен CCNA и два экзамена, позволяющих получить тот же сертификат. Возможность получить сертификат, сдав два экзамена, позволила слушателям курсов и специалистам, освоив примерно вдвое меньше материала, сдать один экзамен перед тем, как перейти ко второму.

Структура экзаменов

Для текущего варианта сертификации, анонсированной в июне 2007 года, компания Cisco ввела два экзамена, ICND1 (640-822) и ICND2 (640-816), а также общий экзамен CCNA (640-802). (С 2003 по 2007 год эти экзамены, имея общую структуру, назывались INTRO, ICND и CCNA.) Чтобы получить сертификат CCNA, специалист может сдать или оба экзамена — и ICND1 и ICND2, — или только экзамен CCNA. Экзамен CCNA включает в себя все темы, которые содержатся в экзаменах ICND1 и ICND2. Таким образом, у сетевого специалиста есть две возможности для получения сертификата CCNA. Система из двух экзаменов позволяет сетевым инженерам с меньшим опытом изучать и сдавать сертификационный экзамен по частям, а один общий экзамен позволит сэкономить некоторые финансы на сертификационном тестировании тем, кто может подготовиться к сертификации по всем темам сразу.

Несмотря на то что система двух экзаменов более полезна для части претендентов на сертификацию, компания Cisco разработала экзамен ICND1 с еще одной важной целью. В сертификационном экзамене CCNA тестирование знаний и практических навыков на сегодняшний день уже выходит за рамки общих сведений начального уровня. Компания Cisco нуждается в сертификации, которая бы лучше отображала навыки и знания начального уровня, поэтому был разработан курс под названием *Обединение устройств компании Cisco 1* (Interconnecting Cisco Networking Devices 1 —

ICND1) и соответствующий ему экзамен ICND1. Этот экзамен включает в себя проверку знаний и навыков, необходимых специалисту начального уровня для обеспечения работы сети небольшого предприятия. Чтобы вы могли продемонстрировать владение навыками, требующимися для должностей низшего уровня, компания Cisco создала новую сертификацию CCENT.

На рис. I.1 показана схема сертификации для начальных уровней и указаны экзамены, которые необходимо сдать для получения сертификатов CCENT и CCNA. Обратите внимание: экзамен ICND2 не сопровождается отдельным сертификатом.

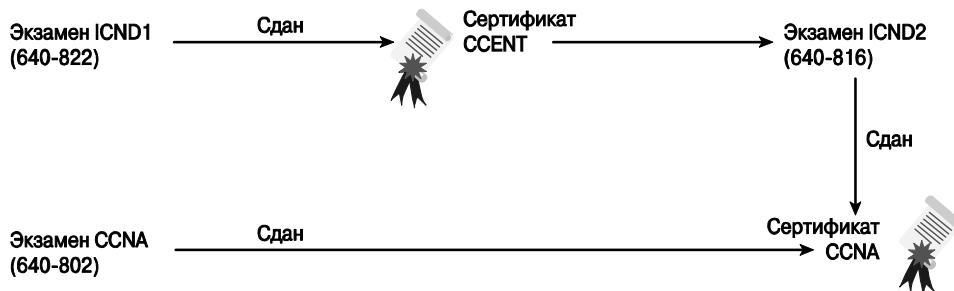


Рис. I.1. Сертификации и экзамены начального уровня компании Cisco

Следовательно, специалист может получить сертификат CCENT, просто сдав экзамен ICND1, но не обязательно сдавать экзамен CCENT, чтобы получить сертификат CCNA. Любой технический специалист может получить сертификат CCNA, не сдавая сертификационный экзамен CCENT.

Экзамены ICND1 и ICND2 включают в себя разные темы, которые изредка пересекаются. Например, тест ICND1 включает в себя такие темы, как IP-адресация и разделение на подсети, а тест ICND2 включает более сложные вопросы по использованию подсетей, которые связаны с масками переменной длины (VLSM). Таким образом, экзамен ICND1 включает только некоторые темы до определенного уровня сложности, экзамен ICND2 содержит более сложные вопросы, экзамен CCNA охватывает все темы, из которых состоят тесты ICND1 и ICND2.

Хотя популярность сертификации CCENT повышается медленно, сертификат CCNA, несомненно, остается наиболее популярным среди программ сертификации в области сетевых технологий начального уровня. Наличие сертификата CCNA у сетевого инженера подтверждает то, что он владеет наиболее полезными базовыми знаниями для работы с наиболее популярными продуктами линейки устройств компании Cisco, а именно маршрутизаторами и коммутаторами. Данный сертификат также доказывает то, что специалист имеет достаточно теоретических знаний в сетевых технологиях и протоколах.

Книги новые, а экзамены Cisco остались старые

В отличие от любых предыдущих изданий этой книги, данное третье издание связано не с пересмотром компанией Cisco экзаменов либо изменением экзаменационных тем или количества экзаменов. Предыдущее второе издание все еще хорошо подходит и включает все содержимое, связанное с текущими экзаменами.

ми 640-822, 640-816 и 640-802. Так зачем было выпускать новое издание, когда содержимое экзамена осталось неизменным и охват тем в предыдущем издании вполне решает поставленную задачу?

Причин две. В первую очередь издатель хотел предоставить больше содержимого, кроме того, что напечатано на страницах книги. Для этого он добавил следующее.

- Бесплатный экземпляр эмулятора CCNA Simulator Lite. Это то же программное обеспечение, что и полная платная версия эмулятора, но с некоторыми заблокированными командами. Это — замечательное добавление, особенно для полных новичков в продуктах Cisco, поскольку оно позволяет получить некоторые навыки работы с пользовательским интерфейсом устройств Cisco, прежде чем приступать к подробному изучению многих возможностей.

Только этих изменений хватило бы для того, чтобы сделать эту новую книгу и новую серию, в которую она входит, намного лучшим выбором, чем прежние книги. Однако книга тоже изменилась, причем не только за счет нового содержимого, но и за счет способа его представления. Я (Уэнделл) переписал и улучшил множество тем, особенно по созданию подсетей, привел к единообразию упражнения, что поможет вам преодолеть более интеллектуальные барьеры. В ходе модернизации книги я также улучшил рисунки и несколько небольших тем, разъяснил некоторые моменты и внес изменения в соответствии с изменением технологий, произошедших за четыре последних года.

Так, если вы сравните новую и старую книги, то увидите полностью реорганизованный раздел по созданию подсетей (семь более коротких глав вместо одной длинной), измененные рисунки в некоторых главах (некоторые были заменены благодаря вашим отзывам!). Чего вы не увидите, так это набора новых тем, поскольку экзамены пока не изменились, а существующие книги уже раскрыли все экзаменационный темы.

Так как же можно быть уверенным, что компания Cisco не изменит экзамены со временем выхода этой книги? Во-первых, игнорируйте слухи в сети, — они не от компании Cisco, просто иногда людям нравится пофантастизировать. Во-вторых, посетите веб-сайт Cisco, в частности страницу www.cisco.com/go/ccna — главную страницу сайта Cisco по сертификации CCNA. Если увидите номера экзаменов, кроме перечисленных на рисунке выше, значит, экзамены изменились. (И если они изменились, посетите сайт www.ciscopress.com, чтобы узнать, как найти новое издание этой книги!)

Формат экзамена CCNA

Экзамены ICND1, ICND2 и CCNA имеют общий формат. Когда претендент приходит в компанию, принимающую сертификационные экзамены, и регистрируется, администратор компании дает ему общие инструкции по сдаче теста, а затем проводит в специализированную комнату с компьютером. Перед тем как начать тестирование, экзаменуемому нужно выполнить еще несколько действий — например, можно пройти пробный тест, только чтобы привыкнуть к компьютеру и программному обеспечению для тестирования. Любой человек, владеющий компьютером на уровне простого пользователя, не будет испытывать проблем с программой тестирования. Дополнительная информация об экзамене приведена в главе 24, в ней также

есть ссылка на страницу веб-сайта компании Cisco, содержащую демонстрационную презентацию экзамена.

- Экзамен состоит из множества вопросов, на которые нужно дать правильные ответы. Программа тестирования работает таким образом, что, только ответив на один вопрос, можно перейти к следующему. *Помните, что экзаменацное программное обеспечение не позволяет вернуться к предыдущему вопросу и изменить свой ответ.* Когда экзаменуемый переходит к следующему вопросу, предыдущий вопрос уже нельзя увидеть.
- Экзаменацные вопросы могут быть в одном из следующих форматов:
 - многовариантный выбор ответа (Multiple choice — MC);
 - тестлет (testlet);
 - вопросы с перетаскиванием правильных ответов (Drag-and-drop — DND);
 - лабораторная работа на эмуляторах оборудования (Simulated lab — Sim);
 - симлет (simlet).

Первые три типа вопросов, вполне очевидно, чаще всего встречаются на экзамене. В вопросах с многовариантным выбором ответа (MC) нужно просто выбрать правильный ответ. В экзаменах компании Cisco обычно указано, сколько ответов нужно выбрать, а тестовое программное обеспечение не позволит выбрать слишком много ответов. Тестлеты — это вопросы с одним общим сценарием и многовариантными вопросами в общем сценарии. Вопросы с перетаскиванием ответов (DND) — это те, в которых с помощью мышки можно переместить объект в другую область и расположить его где-либо, например в списке. Так, например, в некоторых случаях, чтобы дать правильный ответ, экзаменуемый должен расположить 5 объектов в правильном порядке!

В последних двух случаях используется эмулятор сети. Следует отметить, что в действительности эти два типа вопросов позволяют компании Cisco оценивать два совсем разных навыка. В первом типе заданий описывается ошибка и стоит задача настроить один или несколько маршрутизаторов и коммутаторов, чтобы устранить проблему. В экзамене такое задание оценивается по той конфигурации, которая была сделана, или по изменениям, внесенным в существующую конфигурацию. Следует помнить, что за выполнение таких заданий компания Cisco (по крайней мере, на сегодняшний день) выделяет наибольшее количество баллов.

Симлеты — одни из наиболее сложных экзаменацных вопросов. В симлетах также используются эмуляторы сети, но вместо ответа на вопрос или изменения конфигурации в них нужно дать один или несколько многовариантных ответов. В таких вопросах нужно использовать эмулятор для проверки текущего поведения сети, интерпретации информации, выводимой командами группы `show`, которые экзаменуемый сможет вспомнить, чтобы ответить на вопрос. Если вопросы с эмуляцией сети требуют от специалиста умения диагностировать неисправности на основе конфигурации, то симлеты требуют умения проанализировать как исправную сеть, так и неисправную, связать команды группы `show` со знанием сетевой теории и конфигурационные команды.

Как проводится экзамен CCNA

Когда я еще учился в школе, после того, как учитель объявлял о том, что скоро у нас будет тест или контрольная, кто-нибудь всегда спрашивал: “А что это будет за тест?” Даже в колледже студенты всегда хотят иметь больше информации о том, что именно будет на экзамене. Информация в таком случае, главным образом, добывается с вполне практической целью — знать, что нужно учить больше, что меньше, и что можно совсем не учить.

Компания Cisco хочет, чтобы публике были известны и темы экзаменов, и какие именно знания и навыки потребуются для каждой темы при сдаче сертификационных тестов Cisco. Для этого компания Cisco публикует список, содержащий специфические теоретические темы, такие как IP-адресация, протокол RIP и сети VLAN. Кроме того, в описаниях экзаменов также указано, какие знания необходимы для данного теста. Например, одно задание может начинаться со слова “Опишите...” или со слов “Опишите, настройте и устранитне неисправности...”. Из постановки задачи в других заданиях можно четко понять, что необходимо полное понимание темы. Публикуя темы и необходимый уровень навыков для них, компания Cisco помогает специалистам готовиться к экзамену.

Несмотря на то что списки тем для экзаменов весьма полезны, не забывайте, что компания Cisco при публикации списка указывает, что он является *рекомендованным* набором тем для изучения. Компания Cisco стремится в экзаменационных вопросах не выходить за рамки таких тем, и специалисты, занимающиеся разработкой тестов, постоянно анализируют вопросы, обновляют их, чтобы они соответствовали заявленному списку.

Темы экзамена ICND1

В табл. I.1 перечислены темы экзамена ICND1, а список тем экзамена ICND2 представлен в табл. I.2. Несмотря на то что указанные экзаменационные темы не пронумерованы на веб-сайте Cisco.com, компания Cisco Press пронумеровала их для удобства. В табл. I.1 также указаны соответствующие части книги, в которых содержится информация, относящаяся к экзамену. Поскольку экзаменационные темы со временем вполне могут измениться, стоит лишний раз проверить список экзаменационных тем на веб-сайте Cisco.com (www.cisco.com/go/ccna). Если компания Cisco добавила какие-либо новые темы в экзамен, обратитесь к приложению B, в котором рассказано, как получить дополнительную информацию по обновленному экзамену на сайте www.ciscopress.com.

Таблица I.1. Темы экзамена ICND1

№	Часть книги (том ICND1)	Тема экзамена
Принцип работы сетей передачи данных		
1	I	Назначение и функции различных сетевых устройств
2	I	Выбор компонентов сети для определенных задач
3	I, II, III, IV	Использование моделей OSI и TCP/IP, а также связанных с ними протоколов для объяснения принципов передачи потоков данных в сети

Продолжение табл. I.1

№	Часть книги (том ICND1)	Тема экзамена
4	I	Описание наиболее распространенных сетевых утилит, в том числе веб-приложений
5	I	Описание предназначения и основных принципов протоколов в моделях OSI и TCP
6	I	Описание влияния приложений (например, для передачи голоса по сети IP — Voice over IP and Video over IP) на сеть
7	I-V	Интерпретация диаграмм сети
8	I-V	Механизм определения маршрута между двумя хостами в сети
9	I, III, IV	Описание компонентов, необходимых для построения сети и подключения к Интернету
10	I-IV	Идентификация и устранение общих сетевых проблем на уровнях 1, 2, 3 и 7 с использованием подхода на основе многоуровневой модели
11	II, III, IV	Определение и описание отличий между технологиями LAN и WAN и их функциями
Внедрение малых коммутируемых сетей		
12	II	Выбор правильных кабелей, портов и разъемов для подключения коммутаторов к другим сетевым устройствам и узлам
13	II	Объяснение технологии, метода доступа и контроля среды в стандартах Ethernet
14	II	Объяснение принципа сегментации сети и базовых концепций управления трафиком
15	II	Объяснение принципа работы коммутаторов компании Cisco и базовых концепций коммутации
16	II	Создание, сохранение и проверка начальной конфигурации коммутатора, в том числе настройка средств дистанционного доступа к устройству
17	II	Проверка состояния сети и работоспособности коммутатора с помощью базовых сетевых утилит (включая ping, traceroute, Telnet, SSH, arp и ipconfig), а также команд групп show и debug
18	II	Внедрение и проверка базовой безопасности в коммутируемых сетях (режим безопасности портов, выключение неиспользуемых портов и т.п.)
19	II	Идентификация, описание и разрешение основных проблем со средой передачи данных в коммутируемых сетях, проблем с конфигурацией, автосогласованием режима работы портов и аппаратных отказов
Внедрение схемы IP-адресации и IP-служб в небольших сетях филиалов предприятия		
20	I, III	Описание роли и предназначения адресации в сети
21	I, III	Создание и внедрение схемы адресации в сети
22	III, IV	Присвоение и проверка правильности IP-адресов хостам, серверам и сетевым устройствам в локальной сети
23	IV	Описание базовых применений и принципа работы службы NAT в небольших сетях, подключаемых к одному провайдеру
24	I, IV	Описание принципа работы службы DNS
25	III	Описание использования, преимуществ и особенностей частных и открытых зарегистрированных IP-адресов

Продолжение табл. I.1

№	Часть книги (том ICND1)	Тема экзамена
26	III, V	Запуск и конфигурирование службы NAT в сети с одним провайдером служб Интернета, конфигурирование подключения с помощью ПО SDM, а также проверка в интерфейсе командной строки при помощи команды ping
27	IV	Конфигурирование, проверка, поиск и устранение неисправностей в службах DHCP и DNS маршрутизатора (включая CLI/SDM)
28	IV	Внедрение статической адресации и служб динамической адресации для хостов в локальной сети
29	III	Идентификация и устранение проблем в IP-адресации
		Внедрение небольшой маршрутизируемой сети
30	I, III, IV	Описание базовых концепций маршрутизации, в том числе процесса поиска маршрутов и механизмов пересылки пакетов
31	IV	Описание процесса работы маршрутизаторов компании Cisco, в том числе процесса загрузки устройства, процедуры POST и аппаратных компонентов маршрутизатора
32	I, IV	Выбор правильных кабелей, портов и разъемов для подключения маршрутизаторов к другим сетевым устройствам и хостам
33	IV	Конфигурирование, проверка работоспособности, поиск и устранение неисправностей для протокола RIPv2
34	IV	Доступ к интерфейсу командной строки и его использование для настройки базовых параметров устройства
35	IV	Подключение, конфигурирование и проверка работоспособности интерфейсов
36	IV	Проверка конфигурации устройства и наличия связи в сети с помощью утилит ping, traceroute, Telnet, SSH и др.
37	IV	Конфигурирование и проверка статических и стандартных маршрутов
38	IV	Управление конфигурационными файлами операционной системы IOS: сохранение, редактирование, обновление и восстановление
39	IV	Управление операционной системой Cisco IOS
40	IV	Физическая безопасность устройства и внедрение паролей
41	IV	Проверка состояния сети и работоспособности маршрутизатора при помощи стандартных утилит ping, traceroute, Telnet, SSH, arp, ipconfig, а также с помощью команд групп show и debug
		Основы технологии и базовые конфигурации беспроводных локальных сетей (WLAN)
42	II	Описание стандартов беспроводных коммуникаций, в том числе IEEE, Альянса Wi-Fi, Союзов ITU/FCC
43	II	Идентификация и описание назначения устройств небольшой беспроводной сети, а также идентификатора SSID и таких понятий, как BSS и ESS
44	II	Идентификация основных конфигурационных параметров беспроводной сети и организация соединения устройств с определенной точкой доступа
45	II	Сравнение и описание средств безопасности в беспроводных сетях и возможностей технологий безопасности WPA, в том числе стандартов WEP, WPA-1/2 и открытых сетей
46	II	Идентификация основных проблем в беспроводных сетях

Окончание табл. I.1

№	Часть книги (том ICND1)	Тема экзамена
Идентификация брешей в безопасности сетей и описание общих методов их исключения		
47	I	Объяснение современных проблем безопасности, а также почему следует вводить общую политику безопасности в сетях
48	I	Описание общих методов исключения брешей в безопасности систем и сетевых устройств, приложений и операционных систем
49	I	Описание функций основных средств и приложений безопасности
50	I, II, IV	Описание рекомендованных подходов к построению систем безопасности и действий по укреплению защиты сетевых устройств и сетей
Внедрение и проверка работоспособности каналов WAN		
51	V	Описание различных методов подключения к сетям WAN
52	V	Конфигурирование и проверка работоспособности стандартного последовательного канала WAN

Темы экзамена ICND2

В табл. I.2 перечислены темы экзамена ICND2 (код 640-816) и указано, в каких частях второго тома книги описаны соответствующие темы.

Таблица I.2. Темы экзамена ICND2

№	Часть книги (том ICND2)	Тема экзамена
Конфигурирование, проверка работоспособности, а также поиск и устранение неисправностей в коммутаторах с магистральными соединениями и сетями VLAN		
101	I	Описание расширенных технологий коммутируемых сетей и коммутаторов, в том числе VTP, RSTP, VLAN, PVSTP и 802.1q
102	I	Описание того, как сети VLAN создают логически независимые подсети и зачем нужна маршрутизация между ними
103	I	Конфигурирование, проверка работоспособности, поиск и устранение неисправностей в сетях VLAN
104	I	Конфигурирование, проверка работоспособности, поиск и устранение неисправностей в магистральных соединениях (trunking) коммутаторов компании Cisco
105	II	Конфигурирование, проверка работоспособности, поиск и устранение неисправностей в маршрутизации между сетями VLAN
106	I	Конфигурирование, проверка работоспособности, поиск и устранение неисправностей в протоколе VTP
107	I	Конфигурирование, проверка работоспособности, поиск и устранение неисправностей в протоколе RSTP
108	I	Интерпретация вывода команд групп show и debug с целью проверки состояния и работоспособности сети на оборудовании Cisco

Продолжение табл. I.2

№	Часть книги (том ICND2)	Тема экзамена
109	I	Внедрение базовых средств безопасности коммутаторов (безопасный режим порта, неиспользуемые порты, доступ к магистральным соединениям и т.п.) Внедрение схемы IP-адресации в сети и IP-служб для сетей средней величины и крупных филиалов предприятия
110	II	Расчет и применение схемы VLSM IP-адресации в сети
111	II	Определение подходящей бесклассовой адресной схемы для сети по методу VLSM и суммирование маршрутов для обеспечения оптимальной маршрутизации в локальных и распределенных сетях
112	V	Описание технологических требований к внедрению стандарта IPv6: протоколы, двойная адресация, логические тоннели и др.
113	V	Описание IP-адреса стандарта IPv6
114	II, III	Идентификация и устранение наиболее распространенных проблем в IP-адресации и конфигурации окончательных узлов Конфигурирование, а также поиск и устранение неисправностей в протоколах маршрутизации устройств компании Cisco
115	III	Описание и сравнение различных методов маршрутизации и протоколов маршрутизации
116	III	Конфигурирование, проверка работоспособности, поиск и устранение неисправностей в протоколе маршрутизации OSPF
117	III	Конфигурирование, проверка работоспособности, поиск и устранение неисправностей в протоколе маршрутизации EIGRP
118	II, III	Проверка конфигурации и связи в сети с помощью утилит ping, traceroute, Telnet и SSH
119	II, III	Поиск и устранение неисправностей в маршрутизации
120	II, III, IV	Проверка состояния и работоспособности программного и аппаратного обеспечения маршрутизаторов с помощью команд show и debug
121	II	Внедрение базовых средств безопасности в маршрутизаторах Конфигурирование, проверка работоспособности, поиск и устранение неисправностей в службе NAT и списках ACL в сети среднего размера и крупных филиалах предприятий
122	II	Описание и назначение списков управления доступом (ACL)
123	II	Конфигурирование и применение списков управления доступом согласно требованиям фильтрации трафика в сети
124	II	Конфигурирование и применение списков управления доступом для ограничения доступа Telnet и SSH к маршрутизатору
125	II	Проверка списков ACL в сети
126	II	Поиск и устранение неисправностей в списках ACL
127	V	Описание базовых принципов работы службы NAT
128	V	Конфигурирование службы трансляции сетевых адресов (NAT) для заданной сети через интерфейс командной строки
129	V	Поиск и устранение неисправностей в службе NAT

Окончание табл. I.1

№	Часть книги (том ICND2)	Тема экзамена
Внедрение и проверка работоспособности соединений WAN		
130	IV	Конфигурирование и проверка работоспособности соединений Frame-Relay в маршрутизаторах Cisco
131	IV	Поиск и устранение неисправностей в соединениях WAN
132	IV	Описание технологий VPN: их важность, преимущества, роль, влияние на структуру сети, основные компоненты
133	IV	Конфигурирование и проверка соединения PPP между маршрутизаторами компании Cisco

Темы экзамена CCNA 640-802

Экзамен CCNA 640-802 содержит все темы из обоих экзаменов (ICND1 и ICND2), по крайней мере, основан на их опубликованных темах. Опубликованные темы экзамена CCNA включают все темы из табл. I.1 и I.2, кроме тех разделов, которые выделены светло-серым цветом. Обратите внимание на то, что выделенные темы все же присутствуют в экзамене CCNA 640-802, просто они указаны в темах экзамена CCNA, т.е. эти экзаменационные темы практически совпадают. Короче говоря, CCNA = ICND1 + ICND2.

Темы курсов ICND1 и ICND2

Получить представление о темах экзаменов можно также в кратком содержании соответствующих учебных курсов. Компания Cisco предлагает два авторизованных курса, связанных с сертификацией CCNA: объединение устройств компании Cisco 1 (Interconnecting Cisco Network Devices 1 — ICND1) и объединение устройств компании Cisco 2 (Interconnecting Cisco Network Devices 2 — ICND2). Авторизованные партнеры компании Cisco по обучающим программам (Certified Learning Solutions Providers — CLSP) и сертифицированные партнеры по обучению компании Cisco (Certified Learning Partners — CLP) проводят занятия по этим курсам. Такие авторизованные компании могут также создавать свои авторские материалы по курсам и в некоторых случаях выходить за рамки стандартного сертификационного экзамена CCNA.

О книге

Как упоминалось выше, компания Cisco разделила экзамен CCNA на две части: в первую часть были вынесены темы, которые понадобятся инженерам, работающим с небольшими сетями (ICND1), а во вторую, дополнительную, — с сетями среднего размера (ICND2). Аналогично издательство Cisco Press выпустило две книги: одну по экзамену CCENT/CCNA ICND1 и вторую по CCNA ICND2. Эти книги охватывают все темы указанных экзаменов, обычно даже немного более подробно, чем требуется для сдачи сертификационных экзаменов, чтобы подготовить читателя к более сложным вопросам экзамена.

В этом разделе описаны различные особенности обеих книг, поэтому если читатель после прочтения первого тома планирует продолжить изучение материала вто-

рого, то он может не читать введение повторно, так как в этом нет смысла. Если читатель планирует использовать книги для подготовки к сдаче именно экзамена CCNA 640-802, а не к сдаче двух тестов, ему следует прочитать план подготовки к экзамену, который приведен в конце данного раздела.

Цели и методы

Самая важная и вполне очевидная цель этой книги — помочь читателю получить знания и сдать экзамены ICND1 и CCNA. Изначально цель книги была несколько другой, поэтому название книги немного вводит в заблуждение. Тем не менее методы изложения материала, используемые в данной книге, несомненно, существенно помогут в сдаче экзаменов, а также помогут читателю стать высококвалифицированным специалистом в области информационных технологий и сетей.

В этой книге используется несколько ключевых методов, призванных помочь читателю обнаружить те темы, которые следует дополнительно перечитать и изучить, чтобы запомнить концептуальные моменты и дополнительные детали и разобраться в соответствующих технологиях досконально. Задача этой книги состоит не в том, чтобы помочь читателю сдать экзамен за счет зубрежки и хорошей памяти, а в том, чтобы обеспечить изучение и понимание ключевых технологий современных телекоммуникаций. Сертификат CCNA является основой множества профессиональных сертификаций компании Cisco, поэтому книга ориентирована прежде всего на четкое понимание наиболее популярных стандартных технологий и протоколов. Книга поможет успешно сдать сертификационный экзамен CCNA, а также понять, какие темы экзамена следует изучить дополнительно; кроме того, она

- содержит информацию и подробные объяснения, которые помогут заполнить пробелы в знаниях;
- содержит упражнения, которые помогут запомнить материал и дедуктивным методом найти правильные ответы на экзаменационные вопросы;
- и в дополнение ко всему на прилагаемом DVD вы найдете практические примеры и задания по рассматриваемым темам, а также дополнительное тестовое программное обеспечение для подготовки к экзамену.

Особенности книги

Чтобы помочь читателю распланировать свое время в процессе изучения данной книги, в самых важных ее главах есть определенные элементы, указанные ниже, которые помогут упорядочить процесс изучения материала.

- **Контрольные вопросы: знаете ли вы уже темы главы.** Каждая глава начинается с контрольных вопросов, которые помогут определить, сколько времени нужно потратить на изучение данной главы.
- **Основные темы.** В этом разделе описаны протоколы, концепции и конфигурации, рассматриваемые в текущей главе.
- **Подготовка к экзамену.** Этот раздел каждой главы описывает некоторый стандартный план для подготовки к сертификационным экзаменам. В каждой главе есть такой раздел и справочные материалы, связанные с темой главы. Дополнительные материалы включают в себя разделы, перечисленные ниже.

- **Список ключевых тем.** Соответствующая пиктограмма размещена рядом с самыми важными моментами каждой главы, а в конце главы приведена таблица ключевых тем. Несмотря на то что практически любой материал каждой главы может быть в экзамене, ключевые темы нужно знать особенно хорошо.
- **Заполните таблицы и списки по памяти.** Чтобы помочь читателю натренировать память для уверенного запоминания информации и фактов, наиболее важные списки и таблицы вынесены в отдельное приложение на компакт-диске. В другом приложении те же таблицы заполнены только частично, остальные записи читатель должен заполнить самостоятельно.
- **Ключевые термины.** Хотя на экзаменах не попадаются вопросы, в которых нужно просто дать определение какого-либо термина, в экзамене CCNA требуется знание терминологии компьютерных сетей. В этом разделе перечислены основные термины главы, для которых нужно дать развернутые описания и сравнить их со списком терминов, который приведен в конце книги.
- **Таблицы команд.** В некоторых главах описано множество команд конфигурации интерфейса командной строки. В таких таблицах перечислены команды, описанные в главе, наравне с их примерами, которые можно использовать как для запоминания команд, так и для подготовки к сертификационным экзаменам, где самые важные команды нужно помнить на память.

Кроме основного содержимого каждой из глав, есть дополнительные учебные ресурсы, включая следующие.

- **Тренировочные тесты на компакт-диске.** На прилагаемом компакт-диске есть программное обеспечение Pearson IT Certification Practice Test для самотестирования. Имея DVD и код активации (см. ниже), можете запустить специальный экзамен, который очень похож на настоящий, как по курсу ICND1 и CCNA, так и по ICND2.
- **Эмулятор CCNA Simulator Lite.** Эта “облегченная” версия популярного эмулятора CCNA Network Simulator от Pearson позволяет вам прямо сейчас проверить *интерфейс командной строки* (Command-Line Interface — CLI) Cisco. Нет никакой необходимости покупать реальное устройство или полнофункциональный эмулятор, чтобы приступить к изучению CLI. Просто установите его с DVD, прилагаемого к этой книге. (Примечание: чтобы выяснить, когда какую лабораторную работу использовать, обратитесь к веб-странице данной книги (www.ciscopress.com/title/9781587204357 или www.ciscopress.com/title/1587204258) и найдите ссылку на эмулятор.
- **Видеоролики по расчету подсетей.** На компакт-диске также есть специальные видеоролики, помогающие понять принципы IP-адресации и методы расчета подсетей, в частности, как использовать методы расчета, описанные в этой книге.
- **Упражнения по расчету подсетей.** В приложениях на компакт-диске есть большой набор упражнений, соответствующих главам книги. Каждое приложение содержит набор задач по расчету подсетей с решениями для каждого упражнения и объяснениями того, как эти решения найдены. Это отличный ресурс для того, чтобы лучше и быстрее разобраться в принципах и методах расчета подсетей.
- **Практические сценарии на компакт-диске.** В приложении на компакт-диске есть также несколько сценариев событий в компьютерной сети, которые

пригодятся для дополнительной практики. В сценариях описаны некоторые сети и требования к ним, согласно которым нужно разработать дизайн сетей, выполнить конфигурационные настройки и проверить работоспособность. Сценарии нужны для получения практических навыков и помогут даже в том случае, если у читателя нет доступа к лабораторному оборудованию.

- **Дополнительные материалы на веб-сайте.** На веб-сайте www.ciscopress.com/title/1587204258 представлены дополнительные материалы и обновления, которые появились в экзамене с момента выхода книги. Читатель может периодически заходить по указанному адресу и просматривать обновления, которые предоставляет автор книги, а также дополнительные материалы для подготовки к экзамену. Если вы ищете более профессиональный практикум, то можете рассмотреть возможность покупки эмулятора CCNA 640-802 Network Simulator. Вы можете купить экземпляр этого программного обеспечения от Pearson по адресу <http://www.ciscopress.com/series/series.asp?ser=2538752> или в другом месте. Чтобы помочь вам в изучении, я написал руководство, которое со-поставляет каждую из этих 250 лабораторных работ в эмуляторе с определенным разделом данной книги. Вы можете получить это руководство бесплатно на вкладке “Extras” веб-сайта поддержки.
- **Веб-сайт автора и его блоги.** Автор поддерживает веб-сайт, содержащий инструментальные средства и ссылки, полезные при подготовке к экзаменам CCENT и CCNA. Сайт предоставляет информацию, которая поможет вам создать собственную лабораторную работу, исследовать соответствующие страницы по каждой главе этой книги и книги по ICND2, а также блоги автора CCENT Skills и CCNA Skills. Начните с адреса www.certskills.com, а затем переходите на интересующие вас вкладки.

Структура книги

Книга состоит из 24 основных глав, в каждой из которых рассмотрен определенный набор тем экзамена ICND1. В последней главе представлено резюме по материалам книги и даны советы по сдаче сертификационного экзамена. Краткое описание глав приведено ниже.

Часть I “Основы сетей”

- **Глава 1, “Введение в компьютерные сети”,** фактически является простым введением в сетевые технологии для тех, кто никогда с ними не сталкивался.
- **Глава 2, “Сетевые модели TCP/IP и OSI”,** содержит описание двух стандартных сетевых моделей, а именно TCP/IP и OSI.
- **Глава 3, “Основы сетей LAN”,** посвящена концепциям и терминологии наиболее популярной технологии физического и канального уровней локальных сетей — Ethernet.
- **Глава 4, “Основы сетей WAN”,** посвящена концепциям и терминологии наиболее распространенных технологий канального уровня распределенных сетей (WAN), а именно протоколам HDLC, PPP и технологии Frame Relay.
- **Глава 5, “Основы адресации и маршрутизации IPv4”,** посвящена основному протоколу сетевого уровня модели TCP/IP — протоколу Интернета (IP). В ней описаны основы IP-технологий, в частности IP-адресация и маршрутизация.

- Глава 6, “Основы протокола TCP/IP: передача данных, приложения и безопасность”, содержит подробное описание двух основных протоколов транспортного уровня модели TCP/IP — протокола TCP и протокола пересылки дейтаграмм, UDP.

Часть II “Коммутация в локальных сетях”

- Глава 7, “Базовые концепции коммутации Ethernet”, содержит углубленное и расширенное описание технологий локальных сетей, представленных в главе 3, в частности, наиболее подробно рассматриваются сети Ethernet.
- Глава 8, “Работа с коммутаторами компании Cisco”, содержит описание методов подключения, проверки и конфигурирования коммутаторов Catalyst компании Cisco.
- Глава 9, “Настройка коммутаторов Ethernet”, посвящена описанию множества функций коммутаторов: настройкам скорости и дуплексности портов, технологиям режима безопасности порта, методам обеспечения безопасности интерфейса командной строки и настройкам IP-адреса коммутатора.
- Глава 10, “Поиск и устранение неисправностей в коммутаторах Ethernet”, посвящена методам проверки работы коммутирующих устройств, преимущественно с помощью команд группы `show`.
- Глава 11, “Беспроводные локальные сети”, содержит описание базовых концепций беспроводных сетей, а также объяснение наиболее общих проблем безопасности таких сетей.

Часть III “IPv4-адресация и создание подсетей”

- Глава 12, “Перспективы создания подсетей IPv4”, рассматривает все концепции создания подсетей, начиная с классовой (A, B или C) сети и включая анализ требований, выбор, расчет подсети, перенос результата на бумагу, а также всю подготовку к установке, настройку устройств и использование подсети.
- Глава 13, “Анализ классовых сетей IPv4”. Первоначально IPv4-адреса относились к нескольким классам, при одноадресатных IP-адресах, начинающихся с классов A, B и C. Эта глава исследует все связанное с классами адресов и концепции сети IP, порожденные этими классами.
- Глава 14, “Преобразование маски подсети”. Когда речь идет о масках подсети, нужна математика. Маски подсети бывают в трех форматах. В этой главе обсуждается, как быстро и просто осуществлять преобразования между форматами. Так что вы сможете попрактиковаться, прежде чем заняться масками вплотную в следующих двух главах.
- Глава 15, “Анализ существующих масок подсети”. В большинстве случаев кто-то уже успел поработать перед вами и установить в сети маску подсети. Что это означает? Что эта маска дает? Данная глава посвящена тому, как по маске (и сети IP) выяснить такие ключевые факты, как размер подсети (количество хостов) и количество подсетей в сети.
- Глава 16, “Разработка маски подсети”. Подход прямо противоположный главе 15: взгляд на маски подсети с точки зрения проектирования. Если бы вы могли выбрать маску для использования в сети, то какую бы выбрали? Какие во-

просы следует задавать, чтобы сделать хороший выбор? Данная глава исследует эти вопросы и математические подходы для решения подобных проблем.

- **Глава 17, “Анализ существующих подсетей”.** Диагностика большинства проблем подключения начинается с выяснения IP-адреса и маски. Эта глава рассматривает поиск упомянутой пары и демонстрирует, как осматривать и анализировать подсеть, в которой располагается IP-адрес, включая выяснение идентификатора подсети, диапазона адресов в подсети и широковещательного адреса подсети.
- **Глава 18, “Поиск всех идентификаторов подсети”.** В ходе разработки подсети многие выбирают адрес сети и маску, а затем вычисляют и записывают все идентификаторы подсети, вытекающие из сделанного выбора. Данная глава демонстрирует, как сделать то же самое: как выяснить все идентификаторы подсети, присвоенный сети адрес и единую маску, используемую по всей сети.

Часть IV “Маршрутизация IPv4”

- **Глава 19, “Работа с маршрутизаторами компании Cisco”.** Очень похожа на главу 8, но только посвящена маршрутизаторам, а не коммутаторам.
- **Глава 20, “Концепции и конфигурирование протоколов маршрутизации”.** Содержит описание и объяснение процесса маршрутизации, а также алгоритмов поиска оптимального маршрута к каждой подсети. В этой главе описано также конфигурирование IP-адресов, статических маршрутов и один протокол маршрутизации: RIP версии 2.
- **Глава 21, “Поиск и устранение неисправностей маршрутизации”.** Посвящена обсуждению средств поиска и устранения неисправностей и проблем маршрутизации IP. Содержит также сценарии исследования процесса передачи пакетов IP.

Часть V “Распределенные сети”

- **Глава 22, “Базовые концепции распределенных сетей”.** Посвящена технологиям WAN. Она продолжает и расширяет материал главы 4, а также затрагивает такие технологии подключения к Интернету, как каналы DSL и кабельные каналы. В ней также рассмотрена концепция трансляции сетевых адресов (NAT).
- **Глава 23, “Конфигурирование соединений WAN”.** Посвящена техническим деталям конфигурирования каналов WAN. Описана также настройка служб NAT с помощью программного обеспечения SDM компании Cisco.

Часть VI “Подготовка к экзамену”

- **Глава 24, “Подготовка к сертификационному экзамену”.** Содержит план подготовки к сертификационному экзамену, а также некоторые дополнительные материалы и ключевые моменты книги.

Часть VII “Приложения (в книге)”

- **Приложение А, “Ответы на контрольные вопросы”.** Содержит ответы на контрольные вопросы глав 2–23.
- **Приложение Б, “Справочные числовые таблицы”** Состоит из нескольких таблиц с цифровой информацией, включая таблицу преобразования чисел от 0 до 255 в двоичную систему и список степеней числа 2.

- **Приложение В, “Обновление экзамена ICND1: версия 1.0”.** Состоит из небольших тем и блоков материала для повторения пройденных тем. Это приложение время от времени обновляется и размещается по адресу www.ciscopress.com/ccna. Материалы, доступные на момент издания книги, были добавлены в это приложение. Здесь также приведена подробная инструкция о том, как загрузить наиболее свежую версию этого приложения. <http://www.pearsonitcertification.com/title/0132903822>
- **Список терминов,** приведенный в конце книги, понадобится читателю для проверки определений ключевых терминов, которые перечислены в конце каждой главы.

Часть VIII “Приложения (на компакт-диске)”

Перечисленные ниже приложения в формате PDF размещены на прилагаемом к книге компакт-диске.

- **Приложение Г, “Практические задачи для главы 13: анализ классовых сетей IPv4”.** Содержит список практических задач, связанных с материалом главы 13. В частности, задачи о выяснении адреса классовой сети, в которой располагается адрес, и всех других фактов об этой сети.
- **Приложение Д, “Практические задачи для главы 14: преобразование маски подсети”.** Содержит список практических задач, связанных с материалом главы 14. В частности, задачи на преобразование между тремя форматами масок.
- **Приложение Е, “Практические задачи для главы 15: анализ существующих масок подсети”.** Содержит список практических задач, связанных с материалом главы 15. В частности, задачи на исследование существующей маски, выяснение структуры IP-адресов, а также задачи на расчет количества подсетей и хостов.
- **Приложение Ж, “Практические задачи для главы 16: разработка маски подсети”.** Содержит список практических задач, связанных с материалом главы 16. В частности, вопросы на исследование набора требований, определение масок, соответствующих этим требованиям (если нужно), и выбор наилучшей из них на основании предпочтений.
- **Приложение З, “Практические задачи для главы 17: анализ существующих подсетей”.** Содержит список практических задач, связанных с материалом главы 17. В частности, вопросы об определении IP-адреса и маски, идентификатора подсети, широковещательного адреса подсети и диапазона IP-адресов в подсети.
- **Приложение И, “Практические задачи для главы 18: поиск всех идентификаторов подсети”.** Содержит список практических задач, связанных с материалом главы 18. В частности, вопросы о выяснении всех идентификаторов подсети в классовой сети, когда дана единая маска, используемая во всей сети.
- **Приложение К, “Дополнительные сценарии”.** Содержит дополнительные сценарии некоторых типичных ситуаций, решение которых поможет читателю улучшить свои навыки анализа сетей, поиска и устранения неисправностей и решения сложных задач.
- **Приложение Л, “Видеоматериалы”.** Состоит из нескольких видеороликов, иллюстрирующих алгоритмы, представленные в главе 12. В этом приложении представлены ключевые элементы этих видеороликов, которые могут приго-

диться в процессе просмотра последних, чтобы не нужно было перематывать видеофайл назад и просматривать некоторые фрагменты заново.

- **Приложение М, “Таблицы для запоминания материала”.** Содержит ключевые таблицы и списки всех глав, из которых удалена некоторая информация. Эти таблицы можно распечатать и использовать для тренировки памяти — заполнить их, не заглядывая в книгу.
- **Приложение Н, “Таблицы для запоминания материала с ответами”.** Содержит заполненные таблицы (т.е. фактически ответы) к приложению М.
- **Приложение О, “Дополнительные вопросы ICND1”.** Содержит вопросы из экзамена ICND1, которые не вошли в окончательный вариант тестирования или использовались в предыдущем издании книги. Их также можно использовать для подготовки к экзамену.

Как использовать эту книгу для подготовки к экзаменам ICND1 и CCNA

Эта книга преследует две основные цели: помочь читателю подготовиться к экзамену ICND1 и к экзамену CCNA (для последнего понадобятся два тома книги). Подготовка к экзамену по книге достаточно проста: нужно прочитать последовательно всю книгу, выполнить упражнения, ответить на контрольные вопросы и воспользоваться рекомендациями главы 24 для последнего этапа.

Есть несколько вариантов работы с основными главами этой книги (с 1-й по 23-ю). Возможно, читатель уже знает самые важные технологии главы и хорошо ориентируется в ее материале. Чтобы решить, следует ли читать главу или нет, можно сначала ответить на контрольные вопросы в начале главы. Если ответы на все вопросы даны правильно или дан только один неправильный ответ, можно пропустить главу и перейти к ее последнему разделу, посвященному подготовке к экзамену. Общий план работы с материалом представлен на рис. I.2.

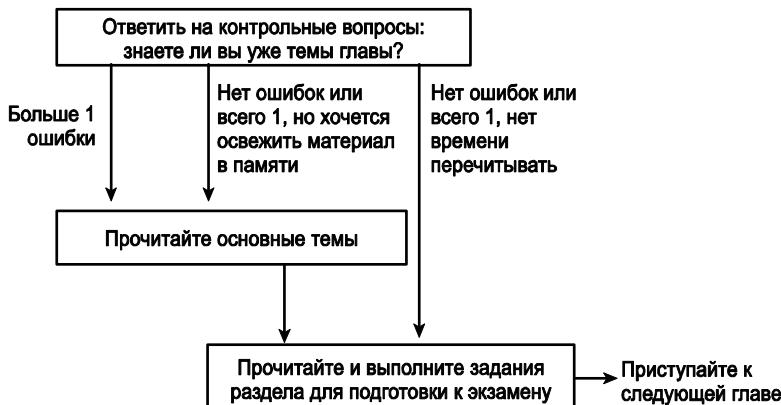


Рис. I.2. Как работать с главами книги

После прочтения глав 1–23 можно воспользоваться рекомендациями по подготовке к экзамену, представленными в главе 24. В последней главе книги вы найдете следующие рекомендации:

- загрузите с веб-сайта свежую копию приложения В, в котором могут быть представлены дополнительные экзаменационные темы и материалы;
- попрактикуйтесь в использовании дополнительных инструментов и заданий, которые размещены на прилагаемом компакт-диске;
- выполните все задания из разделов для подготовки к сертификационному экзамену всех глав;
- выполните задания сценариев, которые размещены на компакт-диске;
- ответьте на контрольные вопросы всех глав, используя экзаменационное программное обеспечение;
- попрактикуйтесь в сдаче тестов на экзаменационном программном обеспечении.

Как использовать эту книгу для подготовки к экзамену CCNA 640-802

Если читатель планирует получить сертификат CCNA, сдав один экзамен CCNA с кодом 640-802, он сможет подготовиться к нему по двум томам книги. Если покупать оба тома книги одновременно, то стоимость будет меньше, чем если покупать каждый том по отдельности.

Два тома книги предназначены для подготовки к полной сертификации CCNA и сдаче соответствующего экзамена. Готовиться к экзамену можно двумя методами. Первый метод достаточно прост и очевиден: сначала следует прочитать первый том (ICND1), потом второй (ICND2). Альтернативный вариант подготовки может быть таким: читатель сначала читает какую-либо тему первого тома (ICND1) и сразу же читает продолжение во втором томе (ICND2), а потом опять возвращается к первому тому книги; т.е. работает одновременно с обоими томами. На рис. I.3 проиллюстрирован возможный план подготовки к экзаменам по двум книгам.

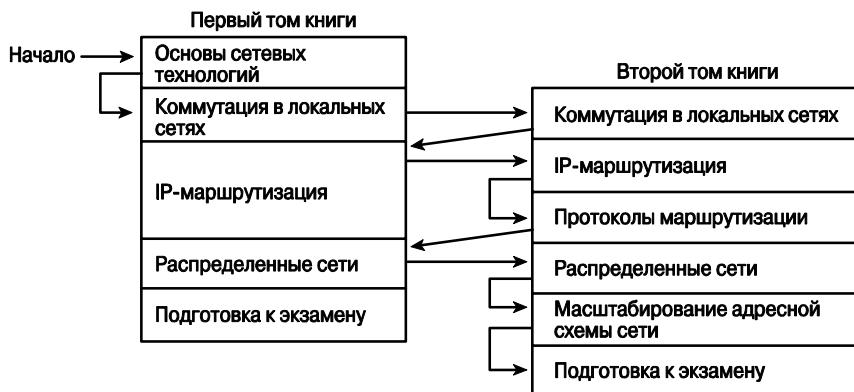


Рис. I.3. Как работать с главами книги при подготовке к экзамену CCNA

Оба возможных плана подготовки имеют свои преимущества. Проработка определенной темы сразу по двум книгам позволит сконцентрироваться на какой-либо одной технологии. Тем не менее материал частично перекрывается в обоих экзаменах, следовательно, он перекрывается и повторяется в книгах. Из комментариев и отзывов читателей о предыдущем издании книги был сделан вывод: те читатели, которые хуже знакомы или совсем незнакомы с сетевыми технологиями и компьютерными сетями, предпочитают полностью прочитать первую книгу и только потом приступать ко второй. Более опытные специалисты, читающие эти книги, предпочтитаю метод, который приведен на рис. I.3.

При подготовке к сдаче экзамена CCNA следует использовать рекомендации последней главы второго тома книги (ICND2), а не первого. В главе 20 второго тома даны те же самые рекомендации и задания, что и в первом томе, а также представлены расширенные задачи, связанные с материалами второго тома.

Еще один небольшой комментарий к плану подготовки к экзамену CCNA, показанному на рис. I.3, — следует очень хорошо изучить и попрактиковаться в IP-адресации, а также в алгоритмах расчета подсетей, прежде чем переходить к IP-маршрутизации и протоколам маршрутизации, которые рассматриваются во втором томе. Вопросы, связанные с подсетями, во втором томе (ICND2) не рассматриваются и не описываются повторно математические операции; предполагается, что читатель уже очень хорошо умеет выполнять нужные расчеты. Главу, посвященную маскам VLSM, будет намного проще понять и легче усвоить, если читатель свободно чувствует себя в расчетах подсетей.

Дополнительная информация

Комментарии и отзывы о книге можно оставить на веб-сайте издательства www.ciscopress.com. На первой странице сайта нужно перейти по ссылке **Contact Us** (Контакты) и отправить сообщение издательству.

Компания Cisco изредка может вносить изменения в программу, которые отражаются и в сертификационном экзамене CCNA. Перед тем как сдавать соответствующие сертификационные экзамены, следует проверить, не изменились ли их темы, по адресам www.cisco.com/go/ccna и www.cisco.com/go/ccent.

Сертификация CCNA фактически является наиболее важным и самым популярным сертификационным экзаменом компании Cisco, хотя новая сертификация CCENT пока медленно набирает популярность. Сертификат CCNA необходим для получения практически любой другой сертификации компании Cisco, поэтому сдача соответствующего экзамена — это первый шаг на пути профессионального развития сетевого специалиста Cisco.

Книга призвана помочь сетевому специалисту в обучении сетевым технологиям и сдаче сертификационных экзаменов CCENT и CCNA. Эта книга — учебник от единственного авторизованного компанией Cisco издательства — Cisco Press. Издательство Cisco Press верит, что эта книга безусловно поможет читателю как в подготовке к экзамену CCNA, так и в практической работе. Мы надеемся, что вы с пользой проведете время за чтением этой книги.

От издательства

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

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

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

E-mail: info@williamspublishing.com
WWW: http://www.williamspublishing.com

Наши почтовые адреса:

в России: 127055, г. Москва, ул. Лесная, д. 43, стр. 1
в Украине: 03150, Киев, а/я 152

Внимание, требуется код активации!

При регистрации ПО Pearson IT Certification Practice Test, находящегося на прилагаемом DVD, нужно ввести код активации, который высылается бесплатно всем, купившим книгу. Пожалуйста, отправьте запрос в произвольной форме по адресу: activation_code@ciscopress.ru, в котором укажите ваши ФИО, ISBN книги, место ее приобретения и цену.

В этой части рассмотрены следующие темы экзамена Cisco ICND1¹...

Принципы работы сетей передачи данных:

- описаны функции различных сетевых устройств;
- рассмотрен процесс выбора компонентов сети для определенных задач;
- описано применение моделей OSI и TCP/IP, а также связанных с ними протоколов для объяснения принципа передачи потоков данных в компьютерных сетях;
- описаны основные сетевые приложения, в том числе веб-службы;
- описаны принципы работы и предназначение протоколов в моделях OSI и TCP/IP;
- описано влияние мультимедийных приложений (передачи голоса по сети IP) на компьютерные сети;
- рассмотрены наиболее важные компоненты сетевых коммуникаций и коммуникаций Интернета;
- описано, как находить и устранять наиболее часто встречающиеся в сетях проблемы на 1, 2, 3 и 7 уровнях с использованием модульного подхода.

Внедрение схемы IP-адресации и служб IP для построения сетей средних и малых офисов:

- описана роль адресов в сети и их назначение;
- приведены примеры расчета и применения схем адресации в сети;
- описаны принцип работы и метод проверки работоспособности службы DNS.

Внедрение малых маршрутизируемых сетей:

- описаны основные концепции маршрутизации, в том числе механизмы перенаправления пакетов, процесс поиска маршрутов;
- рассмотрен процесс выбора среды передачи данных, кабелей, портов и разъемов для соединения маршрутизаторов с другими сетевыми устройствами и узлами.

Угрозы безопасности в сети и общие методы защиты от них:

- приведены описания современных угроз сетевой безопасности и рассказано о том, как создать всестороннюю политику безопасности сети для предотвращения атак;
- разъяснены наиболее распространенные методы защиты от атак на сетевые устройства, хосты и приложения;
- описаны основные функции приложений и устройств обеспечения безопасности;
- рассмотрены наиболее действенные подходы к построению системы безопасности и начальные этапы процесса обеспечения безопасности сетевых устройств.

¹ Текущие темы сертификационного экзамена приведены на сайте <http://www.cisco.com>. — Примеч. авт.

Часть I. Основы сетей

Глава 1. “Введение в компьютерные сети”

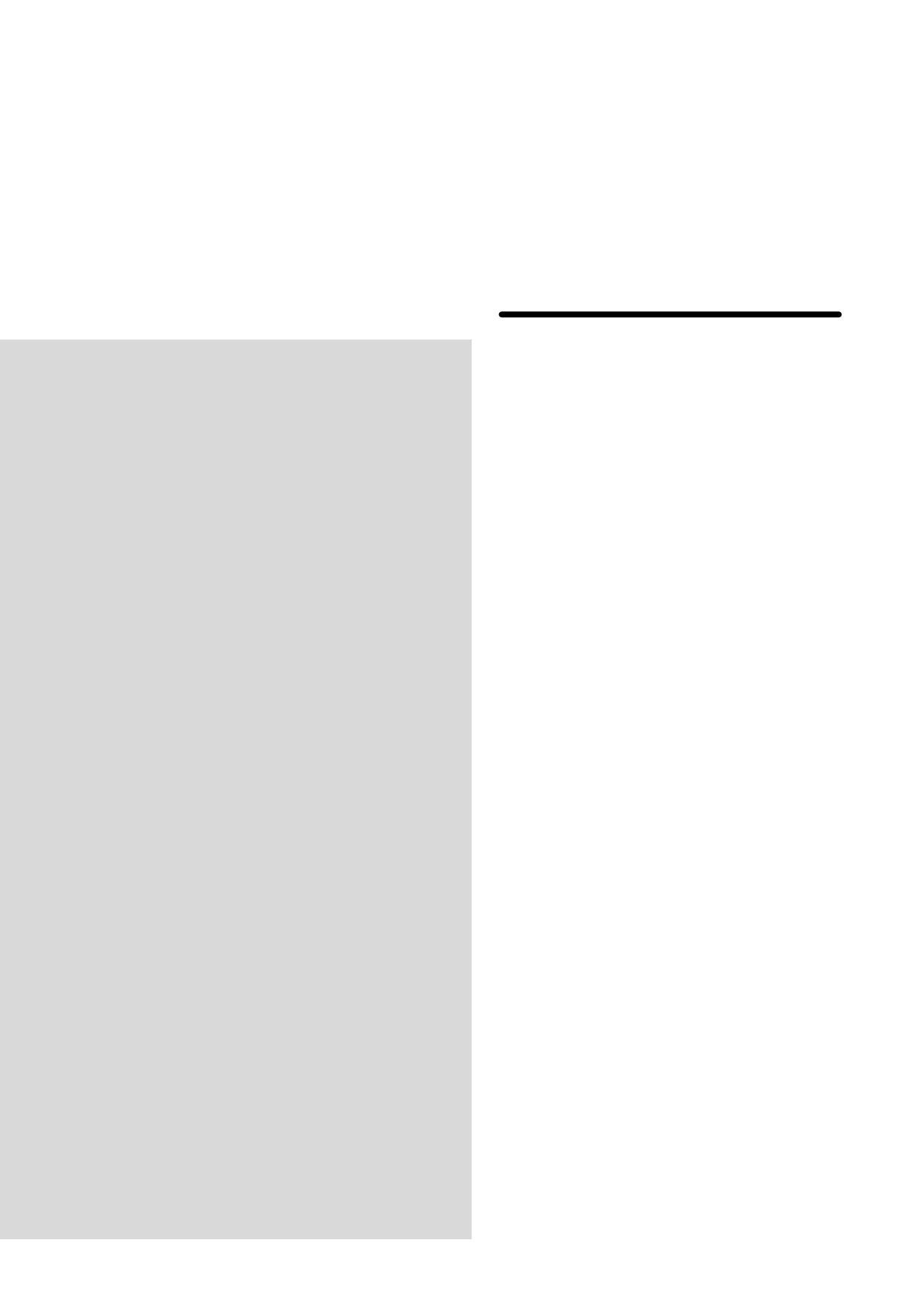
Глава 2. “Сетевые модели TCP/IP и OSI”

Глава 3. “Основы сетей LAN”

Глава 4. “Основы сетей WAN”

Глава 5. “Основы адресации и маршрутизации IPv4”

Глава 6. “Основы протокола TCP/IP: передача данных,
приложения и безопасность”



ГЛАВА 1

Введение в компьютерные сети

В этой главе даны простые описания основных принципов компьютерных сетей, рассказано, как возникли сети, почему они работают так, а не иначе. Несмотря на то что рассматриваемые ниже темы не будут представлены в вопросах сертификационного экзамена CCNA (Cisco Certified Network Associate — сертифицированный специалист компании Cisco), они помогут читателю подготовиться к более сложным вопросам, которые рассматриваются в главе 2. Если читатель практически не знаком с сетевыми технологиями, то главу 1 следует прочитать перед тем, как углубляться в детали технологий, — она поможет разобраться в основах компьютерных сетей. Если же читатель уже достаточно искушен в стеке протоколов TCP/IP, технологии Ethernet, понимает, что такое маршрутизатор, коммутатор, IP-адресация и другие сетевые термины, то эту главу можно пропустить и сразу перейти к следующей.

Что такое современные сети

Итак, вы новичок в компьютерных сетях. Тем не менее вы уже что-то слышали об информационных технологиях и решили серьезно заняться тематикой сетей передачи данных. Ваши представления о телекоммуникационных сетях, как и у большинства людей, основаны на опыте использования сетевых технологий в качестве пользователя, а не на опыте инженера, который строит компьютерные сети. Например, ваши знания, скорее всего, основаны на опыте использования домашнего подключения к Интернету, возможно, даже вполне высокоскоростного. Возможно, вы пользуетесь компьютером на работе или в учебном заведении, опять же используете ресурсы Интернета для выполнения каких-либо задач, и такой компьютер обычно подключен к сети с помощью какого-либо кабеля. Оба варианта подключения к сети показаны на рис. 1.1.

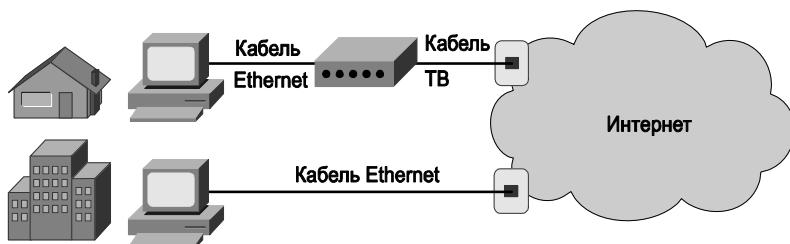


Рис. 1.1. Различные варианты подключения к сети

В верхней части рис. 1.1 показан стандартный метод высокоскоростного кабельного подключения к Интернету. К персональному компьютеру пользователя стандартным кабелем Ethernet подключен кабельный modem. В свою очередь modem под-

ключен к розетке кабельного телевидения (Community Antenna Television — CATV) с помощью коаксиального кабеля; точно такой же кабель используется для подключения телевизора. Поскольку такое кабельное подключение к Интернету работает постоянно, пользователю достаточно включить свой компьютер, и он сразу может отправлять электронную почту, искать информацию на веб-сайтах, осуществлять телефонные звонки через сеть и использовать любые другие сетевые приложения.

Абсолютно аналогично сотрудник компании или студент университета представляет себе всемирную сеть как подключение через настенную розетку (см. рис. 1.1). Обычно в таком подключении используется некоторая *локальная сеть* (LAN — Local Area Network), которую зачастую называют просто сетью Ethernet. Вместо кабельного модема персональный компьютер подключен к разъему Ethernet — настенной розетке (сетевой разъем очень похож на распространенный нынче стандартный четырехконтактный телефонный разъем, но он больше по размеру и отличается по количеству контактов). Точно так же как и в кабельной технологии подключения к Интернету, соединение Ethernet не требует каких-либо дополнительных действий от пользователя при подключении к сети, — нужно просто подключить кабель к телекоммуникационной розетке (как, например, кабель питания компьютера к настенной электрической розетке) и можно начинать работать.

С точки зрения обычного пользователя, вне зависимости, от того, где это происходит — дома, на работе, в университете или школе, — все, что происходит “по ту сторону” телекоммуникационной розетки, относится к разряду магии. Точно так же большинство людей не представляют себе, как работает машина, на которой они ездят, или как работает телевизор и другая бытовая техника. Многие из тех, кто используют в повседневной жизни компьютерные сети, не знают, как они работают. И не хотят знать! Тем не менее раз уж вы взялись за эту книгу и решили начать с первой главы, у вас есть мотивация и желание получить знания, которые будут намного шире, чем у обычного пользователя. После прочтения этой книги у вас будут достаточно обширные знания сетевых технологий, чтобы понимать, что происходит в компьютерной сети для обоих вариантов подключения, которые показаны на рис. 1.1.

В сертификационных экзаменах на звание CCNA (Cisco Certified Network Associate — сертифицированный специалист компании Cisco), в частности в экзамене ICND1 (Interconnecting Cisco Network Devices — объединение сетевых устройств компании Cisco, код 640-822), основной упор делается на две основные сферы применения сетевых технологий, протоколов и устройств. Первая группа технологий связана с построением корпоративных телекоммуникационных сетей (*enterprise networking*). Корпоративная сеть обычно создается и управляется одной организацией (предприятием, корпорацией) с тем, чтобы сотрудники могли легко взаимодействовать, общаться и обмениваться информацией в любой момент времени. Например, на рис. 1.2 показан пользователь (такой же, как и на рис. 1.1), который работает с корпоративным веб-сервером через сеть компании (показанную на рисунке в виде стандартного обозначения сетевой среды — облака). Пользователь через свой компьютер может взаимодействовать с корпоративным веб-сервером для того, чтобы сделать что-то полезное для компании, например, он может общаться с клиентом по телефону, параллельно печатая новый заказ от пользователя в интерактивной системе обработки заказов, которая работает на таком сервере.

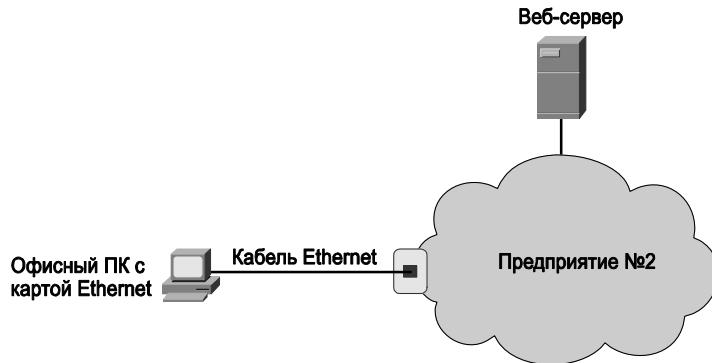


Рис. 1.2. Пример корпоративной сети

ВНИМАНИЕ!

На схемах компьютерных сетей облаком обозначают ту часть сети, детали которой не важны. В рассмотренном выше примере на рис. 1.2 не акцентируется внимание на том, как именно построена или работает корпоративная сеть.

Вторая, не менее важная сфера применения компьютерных сетей, которая рассматривается в экзамене ICND1, — построение компьютерных сетей для *малых и домашних офисов* (Small Office/Home Office — SOHO). В этой сфере используются те же концепции, протоколы и устройства, которые применяются в корпоративных сетях, а также некоторые дополнительные технологии, которые не характерны для корпоративных сетей. В сетях SOHO пользователь подключает компьютер к Интернету через разнообразные телекоммуникационные каналы, например, как показано на рис. 1.1. Поскольку большинство корпоративных сетей также имеет подключение к Интернету, пользователь SOHO может находиться дома, в небольшом офисе, в филиале и тому подобном и работать с серверами и службами корпоративной сети точно так же, как с любыми другими хостами Интернета (рис. 1.3).



Рис. 1.3. Подключение пользователя SOHO к Интернету и корпоративной сети

Фактически Интернет представляет собой объединение корпоративных сетей, различных ресурсов и сотен миллионов сетевых устройств и компьютеров, которые подключены к нему через *провайдеров служб Интернета* (Internet Service Provider — ISP). В действительности сам термин “сеть Интернет” является сокращением от английской фразы “INTERconnected NETworks”, которая переводится как *объединенные сети*. Провайдеры служб Интернета предоставляют доступ к всемирной сети с помощью кабельного телевизионного подключения, цифровой телефонной технологии DSL (Digital Subscriber Line — *цифровой абонентский канал*) или обычной телефонной линии с подключенным к ней модемом. Практически каждое предприятие или компания также подключены как минимум к одному провайдеру ISP с использованием канала *распределенной сети* (Wide Area Network — WAN). В итоге провайдеры во всем мире так или иначе подключены друг к другу. Такие объединенные сети, от наименьшей домашней сети, состоящей из одного или двух компьютеров, мобильных телефонов и портативных устройств, до сетей крупных предприятий и компаний с тысячами компьютеров формируют глобальную сеть Интернет.

Большинство стандартов корпоративных сетей было разработано на протяжении последней четверти XX столетия. Скорее всего, вы начали интересоваться сетевыми технологиями уже после того, как большинство основных соглашений и правил для сетей передачи данных было принято. Тем не менее, если в процессе ознакомления с технологиями попытаться поставить себя на место авторов стандартов и обдумать, что бы вы сделали на их месте и в каком направлении бы двигались при разработке стандартов, многие вещи станут значительно проще и понятней. В следующем разделе представлен простейший и отчасти глупый пример альтернативного подхода к описанию сетей, представляющий собой некоторый вариант воображаемого стандарта доисторических сетей. Однако этот простой пример поможет разобраться в терминологии и базовых концепциях корпоративных сетей, а также в некоторых особенностях дизайна компьютерных сетей и понять, почему некоторые технологии работают именно так, а не иначе.

Сеть Флинстоунов — первая компьютерная сеть?

Флинстоуны — это мультипликационная семейства, которая, согласно сценарию, живет в доисторические времена. Поскольку в дальнейшем предполагается более подробно обсудить процесс разработки воображаемых начальных стандартов компьютерных сетей в шутливой манере, Флинстоуны выглядят как раз подходящим объектом для экспериментов.

Фред (Fred) является президентом компании FredsCo, в которой работают его жена Вилма (Wilma), приятель Барни (Barney) и его жена Бетти (Betty). У них есть телефоны и персональные компьютеры, но нет сети, поскольку идея объединить устройства в сеть еще никому не пришла в голову. Фред замечает, что его работники постоянно отрываются от работы и расхаживают по офису, чтобы обмениваться дисками с информацией, и ему такой подход кажется очень неэффективным. Фред, большой выдумщик, сразу же представляет себе мир, в котором все люди могут соединить свои компьютеры каким-либо образом и обмениваться данными, не вставая со своего рабочего места. Итак, воображаемая первая в истории человечества сеть почти появилась!

Пебблз (Pebbles), дочь Фреда, только что закончила университет Роквилля (Rockville University) и собирается присоединиться к семейному бизнесу. Фред дает ей первое практическое задание и назначает ее первым сетевым инженером в мире. Он говорит ей: “Пебблз, мне нужно, чтобы все работники могли обмениваться файлами, не вставая со своих рабочих мест. Я хочу, чтобы сотрудники могли просто набрать имя файла и имя человека, и оп! Файл появляется на компьютере другого человека. Кроме того, наши сотрудники постоянно переходят из отдела в отдел, поэтому нужно сделать так, чтобы каждый работник мог брать с собой свой компьютер, включать его в настенную розетку и опять же иметь возможность точно так же, как и раньше, отправить или получить файл на новом рабочем месте. Я хочу, чтобы эта сеть была похожа на сеть электропитания, которую разработал для нас год назад твой друг Бамм-Бамм (Bamm-Bamm), т.е. чтобы около каждого рабочего места была настенная розетка, и как только сотрудник подключается к ней, он — в сети!”

Пебблз решает сначала заняться научными исследованиями. Если она сможет заставить два компьютера обмениваться файлами в лабораторных условиях, то потом сможет достичь такого же результата для любого количества компьютеров. Она пишет код программы обмена файлами, которую называет сокращенно FTP, или программой обмена данными Фреда (Fred's Transfer Program)¹, в честь своего отца.

Программа, кроме всего прочего, использует специализированный интерфейсный модуль, который Пебблз разработала и собрала в лаборатории. Такой модуль, называемый платой сетевого интерфейса, подключается к другому модулю кабелем с двумя проводами: один используется для передачи данных, второй — для приема. Пебблз устанавливает по одному модулю в каждый из двух компьютеров в лаборатории и соединяет их двухпроводным кабелем. Используя эти сетевые карты, программа FTP на каждом из компьютеров передает биты данных, из которых состоят файлы. Когда Пебблз вводит команду, например `ftp отправить имя_файла`, программное обеспечение пересыпает файл с указанным именем компьютеру на другом конце кабеля. Схема описанной выше лабораторной сети показана на рис. 1.4.

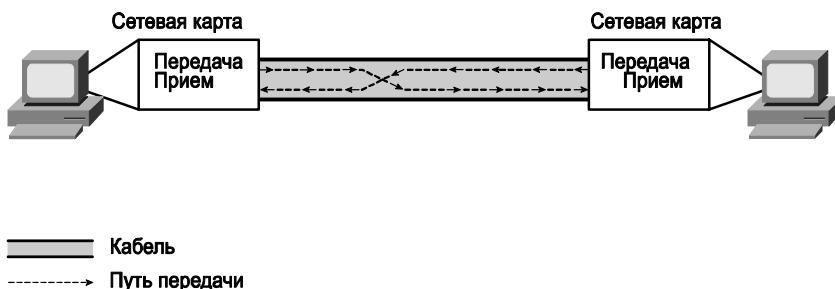


Рис. 1.4. Два компьютера обмениваются файлами в лабораторной сети

Сетевой модуль, который разработала Пебблз, использует первый провод для передачи битов, а второй — для приема, поэтому провод с номером 1 (передача) первого компьютера должен быть подключен к разъему с номером 2 (прием) второго

¹ Игра слов с использованием стандартных аббревиатур: FTP расшифровывается как File Transfer Protocol (протокол передачи файлов), а в данном случае Fred's Transfer Program. — Примеч. ред.

компьютера и аналогично должен быть подключен оставшийся провод. В результате такого подключения обе рабочие станции будут передавать данные через разъем с номером 1 и принимать через разъем с номером 2.

Бамм-Бамм, проходя мимо, замечает, что Пебблз занята какими-то экспериментами, и слышит ее восклицание: “Я готова начать внедрение новой сети!”. Бамм-Бамм, как умудренный опытом ветеран компании FredsCo (а он закончил университет Роквилля на целый год раньше, чем его подруга!), начинает задавать каверзные вопросы. “А что произойдет, если ты захочешь подключить не два, а три персональных компьютера?” — спрашивает он. Пебблз объясняет, что в таком случае она поставит два сетевых модуля в каждый компьютер и соединит их кабелями. “А что произойдет, если ты захочешь соединить вместе десять, нет, сто компьютеров? Просто захочешь подключить друг к другу сто компьютеров в нескольких зданиях?” — ехидно спрашивает Бамм-Бамм. Пебблз понимает, что все не так просто, как ей хотелось, и нужно продолжать исследования дальше. Ей нужно придумать какую-то схему подключения, в которой может быть больше двух-трех пользователей. Неожиданно Бамм-Бамм сам предлагает решение: “Послушай, Пебблз, у меня возникла идея. Возьмем для примера сеть электропитания, провода которой подключены к каждой настенной розетке через распределительные щиты. Тем не менее источник электричества один — генератор. Может, эту идею с одним источником и многими получателями можно взять за основу компьютерной сети?”.

Идея друга вызывает у Пебблз прилив вдохновения, которого ей так не хватало. Вдохновение в немалой степени подкрепляется еще и тем фактом, что она только что создала первую компьютерную сетевую карту, поэтому Пебблз решает разработать устройство, которое позволит использовать схему подключения кабелей, аналогичную предложенной Бамм-Баммом, для сети электропитания. Идея Пебблз выглядит приблизительно так, как показано на рис. 1.5.

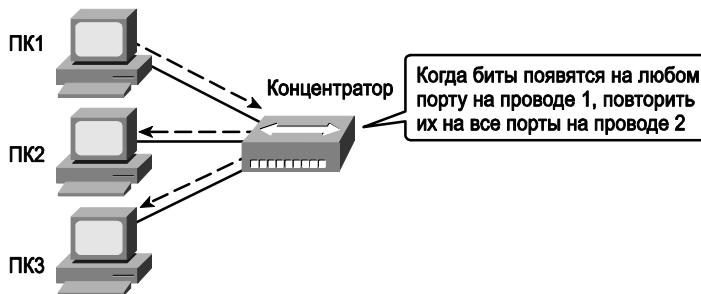


Рис. 1.5. Звездообразная топология с повторителем в центре

Пебблз использует совет Бамм-Бамма, однако ей нужно устройство, в которое можно подключить кабели, т.е. что-то, что сможет принимать биты, которые передает в кабель компьютер и “повторяет” их для всех остальных устройств в компьютерной сети. Поскольку сетевые модули используют для передачи битов разъем (и провод) с номером 1, Пебблз разрабатывает новое устройство таким образом, чтобы оно принимало биты как обычно, но передавало их дальше через разъем с номером 2, и, таким образом, компьютер-получатель получал их через принимающий провод. (Вот почему в такой кабельной схеме не нужно перекрещивать провода с номерами 1 и 2. В новом

устройстве все, что нужно, уже сделано.) Такое устройство стало самым первым сетевым устройством в мире, и ему нужно дать какое-то название. Пебблз решает назвать его *концентратором* (hub).

Перед тем как начать внедрять первый в мире концентратор и прокладывать жгуты проводов, Пебблз решает сделать очень правильный поступок: она сначала проверяет все в лаборатории — подключает три компьютера к концентратору. Она запускает программу FTP на первом персональном компьютере (ПК1) и передает файл с названием *мои_любимые_рецепты.doc*, при этом замечает, что второй компьютер (ПК2) выдал на экран окошко с сообщением об окончании передачи файла, как и раньше (в сети с двумя компьютерами). “Фантастика!” — думает Пебблз и замечает, что компьютер с номером 3 (ПК3) выдал точно такое же сообщение о том, что файл был принят. Таким образом, один и тот же файл был передан одновременно на два компьютера, ПК2 и ПК3. “Логично, — думает Пебблз, — поскольку концентратор просто повторяет все, что попадает ему на входной разъем на всех выходных разъемах; когда программа FTP передает файл, все устройства в сети получат его. Значит, мне нужно придумать способ передачи файла только определенному компьютеру!”

Теперь Пебблз размышляет над несколькими возможными вариантами реализации своей идеи. Сначала она думает о том, что каждому компьютеру можно дать название, которое, например, будет совпадать с именем его владельца. Для этого придется поменять код программы FTP таким образом, чтобы можно было вместе с именем файла в команде использовать имя компьютера. Например, если нужно передать свои рецепты маме, нужно будет ввести команду в виде: **ftp отправить Вилме имя_файла**. Несмотря на то что все компьютеры получат такой файл, поскольку они подключены к концентратору, а он просто повторяет сигнал на всех своих портах, только компьютер, имя которого совпадает с заданным, должен записать такой файл себе. Тем временем ее отец, проходя мимо, спрашивает: “Ну что, Пебблз? Работа уже близка к завершению? Я как раз иду встречаться с нашим новым главой службы безопасности, Барни Файфом (Barney Fife), ему тоже скоро понадобится доступ к компьютерной сети”.

Итак, использовать имена владельцев для названий компьютеров невозможно, поскольку теперь в компании FredsCo работают два человека по имени Барни. Пебблз хорошо подкована в математике, поэтому для разработки оборудования выбирает другой подход. Она восклицает: “Я свяжу с каждым компьютером уникальное число, которое будет использоваться каждой сетевой картой в качестве идентификатора, и пусть такое число состоит из четырех десятичных цифр!” Поскольку именно Пебблз делает все сетевые модули, она вполне может проследить за тем, чтобы номер каждого из них был уникален. Кроме того, используя четырехзначные числа, можно быть вполне уверенным, что их хватит на всех, так как существует $10\ 000$ (10^4) неповторяющихся комбинаций, которых с головой хватит для всех 200 сотрудников компании FredsCo.

К слову, поскольку все описанные методы используются впервые, их можно назвать как душе угодно, поэтому Пебблз решает назвать такие “встроенные” идентификаторы *адресами*. Теперь, когда кто-либо хочет передать файл, он использует ту же самую команду, в которой вместо имени указано число-адрес. Например, команда **ftp 0002 мои_любимые_рецепты.doc** заставит компьютер переслать указанный файл компьютеру, адрес сетевой карты которого равен 0002. На рис. 1.6 показано, как теперь выглядит лабораторная сеть.

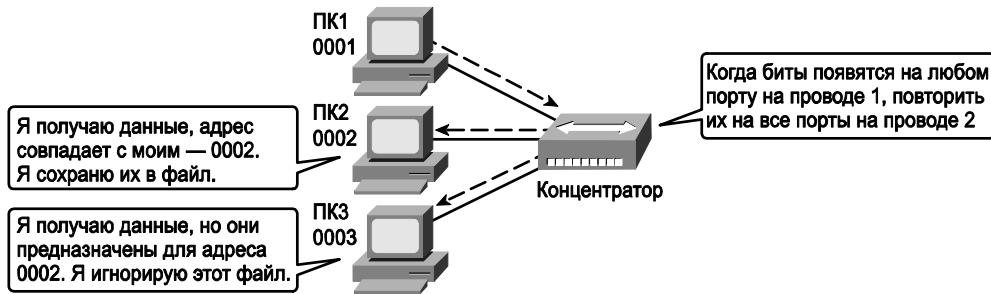


Рис. 1.6. Первое соглашение об адресах компьютеров

Программой FTP (с минимальными изменениями) на данном этапе можно пользоваться точно так же, как и раньше, например, чтобы отправить список рецептов компьютеру с адресом 0002. Пебблз проверяет программное и аппаратное обеспечение сети в лаборатории, как и раньше, и, несмотря на то, что ПК1 передает данные обоим компьютерам в сети, ПК2 и ПК3, только ПК2 обрабатывает то, что передается, и создает копию файла на жестком диске. Аналогично Пебблз проверяет и адрес 0003 — только ПК3 обрабатывает поступающие данные и записывает их. Теперь все готово для того, чтобы создать первую компьютерную сеть.

Теперь задача Пебблз упрощается, ей всего лишь нужно смастерить все требуемое оборудование. Сначала она создает 200 сетевых карт, каждая из которых промаркирована уникальным адресом. Потом Пебблз устанавливает программу на все компьютеры и подключает сетевую карту к каждому персональному компьютеру. После этого она возвращается в лабораторию, чтобы спланировать и рассчитать необходимое количество кабелей и их длину. И тут она понимает, что далеко не все еще учтено: некоторые кабели, например, будут очень длинными. Если поставить концентратор, например, на первом этаже одного здания, а часть компьютеров будет размещена на пятом этаже соседнего здания, то длина кабеля будет невероятной! Кабели стоят денег, причем, чем длиннее кабель, тем больше он стоит. Кроме того, Пебблз еще не проверяла сеть с использованием длинных кабелей, так как в лаборатории (а места там мало) длина кабеля не превышала двух метров.

Как обычно, мимо проходит ее друг Бамм-Бамм и видит, что Пебблз чем-то расстроена. Она начинает причитать: “Ты знаешь, насколько требователен отец, и он хочет, чтобы этот проект был завершен в ближайшее время. А я не подумала над тем, какой длины кабель выбрать, и теперь не вложусь в выделенную сумму. Кроме того, я буду прокладывать эти кабели не одну неделю!” Бамм-Бамм, как человек более хладнокровный, тем более настроенный только что закончившимся обедом на добродушный лад, подозревает, что решение лежит на поверхности, но поскольку Пебблз сильно взволнована, она его просто не видит. Вполне очевидно, что решение не настолько глобально отличается от того, которое Бамм-Бамм использовал для прокладки кабелей сети электропитания год назад. Концентраторы ведь повторяют все, что они получили, правда? Почему бы тогда не сделать эдакие “скопления” из соединенных между собой каким-либо образом концентраторов и соединить их вместе? Можно поставить по одному концентратору на каждом этаже здания и включить в них все компьютеры на этаже. Потом можно будет проложить кабель от каждого концентратора на первый этаж и подключить их к одному концентратору. И в конце концов придется проложить только один кабель между двумя

главными концентраторами в двух зданиях. Поскольку концентратор повторяет принятый сигнал на все свои порты, каждый компьютер получит его, когда один из пользователей сети что-то передает, независимо от того, подключен он к тому же самому концентратору или находится за четырьмя промежуточными устройствами. На рис. 1.7 показан предложенный выше вариант дизайна сети.

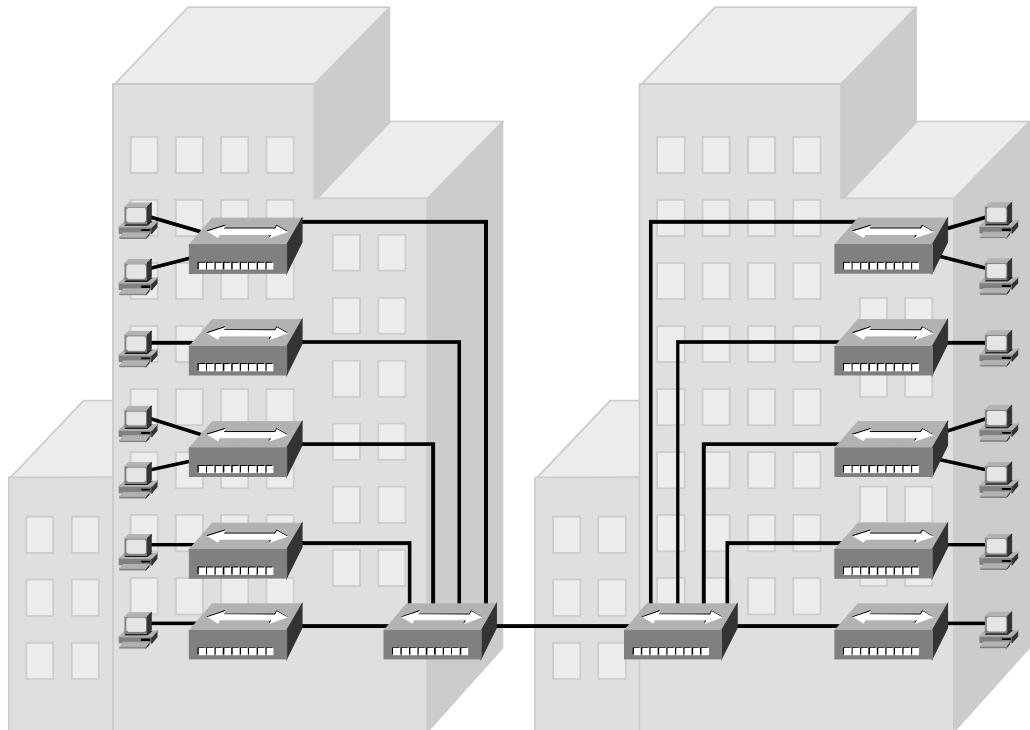


Рис. 1.7. Структурированная сеть с использованием концентраторов

Пебблз безумно понравилась эта идея. Она собирает дополнительные концентраторы, чтобы проверить работоспособность решения. Все работает! Пебблз изготавливает кабели (теперь они значительно короче!), устанавливает концентраторы и начинает проверку. Несколько наугад выбранных компьютеров работают в сети! Первая в мире сеть была успешно внедрена!

Пебблз пишет сообщение всем сотрудникам компании с рассказом о том, как использовать программу передачи данных Фреда, чтобы подготовить небольшой сюрприз любимому папочке. К сообщению она прилагает список имен сотрудников и соответствующие им четырехзначные адреса, чтобы все знали, как отправлять файлы друг другу. Пебблз рассыпает эту информацию всем и с нетерпением ждет результата.

Невероятно, но все работает, как часы. Пользователи сети безмерно счастливы, Фред устраивает для Пебблз и Бамм-Бамма праздничный ужин, вполне очевидно, что он приготовлен его женой Вилмой, а не собственноручно.

Пебблз пребывает в состоянии эйфории, она создала первую в мире компьютерную сеть, все работает без проблем, но проходит несколько недель... “У меня не получается

больше отправлять файлы Фреду, — жалуется Барни Раббл. — С тех пор как у Фреда появился новый компьютер, он настолько занят, что даже не может сходить в боулинг-клуб, а сейчас я даже не могу отправить ему файл, чтобы напомнить, что наша команда по боулингу без него как без рук!” Причина проста — Фред обзавелся новым компьютером, в котором стоит новая сетевая карта, следовательно, его адрес в сети поменялся. Если эта сетевая карта сломается и ее придется заменить, адрес поменяется еще раз.

Приблизительно в это же время Вилма зашла на минутку посплетничать. “Мне так нравится эта новая сеть, которую ты придумал. Я и Бетти теперь в любой момент можем обмениваться сообщениями, просто поместив их в файл и передав друг другу на компьютер. Это настолько удобно, что кажется, будто мы работаем в одном кабинете”, — говорит она. “Правда, есть одна проблема — мне настолько сложно запомнить все эти числа, которые используются в сети, что ты даже себе не представляешь. Можно ли как-то изменить программу FTP так, чтобы вместо этих ужасных чисел я могла писать имя?”

В порыве вдохновения проблема, которую высказала ее мама, наталкивает Пебблз на оригинальную мысль и изящное решение как для задачи мистера Барни, так и для проблемы Вилмы. “Я изменю программу так, чтобы можно было использовать имена вместо адресов. Я переговорю со всеми сотрудниками, чтобы каждый сказал мне, какое имя он будет использовать, например, Барни Раббл может взять себе в сети имя БарниР, а Барни Файф будет называться БарниФ. Программа сможет использовать как числовые адреса, так и имена, и будет искать их соответствие в какой-нибудь таблице, которую можно разместить на всех компьютерах. В будущем, когда придется заменить какую-либо сетевую карту, все, что нужно будет сделать, — это обновить список имен и адресов и разослать его каким-то образом на все компьютеры в сети, причем сделать все можно так, что никто даже не будет об этом знать”. В табл. 1.1 приведен пример списка имен и адресов.

Таблица 1.1. Первая таблица соответствия имен и адресов Пебблз

Имя сотрудника	Название компьютера	Сетевой адрес
Фред Флинтстоун	Фред	0001
Вилма Флинтстоун	Вилма	0002
Барни Раббл	БарниР	0011
Бетти Раббл	Бетти	0012
Барни Файф	БарниФ	0022
Пебблз Флинтстоун	СетеваяГуру	0030
Бамм-Бамм Раббл	ЭлектроВеник	0040

Как обычно, Пебблз сначала проверяет работоспособность новой версии программы FTP в лаборатории, и все работает отлично. Она внедряет новое программное обеспечение в компании, рассыпает всем сотрудникам таблицу названий всех компьютеров и еще одно сообщение. Теперь все изменения в сети проходят гладко, поскольку аппаратные функции, такие как адреса сетевых карт, отделены от логических, которые нужны конечным пользователям.

Точно так же как и Пебблз, любой хороший сетевой инженер должен сначала всесторонне обдумать дизайн сети, проверить возможные варианты в лаборатории

и только потом внедрять сеть в компании. Для проблем, которые можно таким образом предусмотреть, всегда можно придумать некоторый обходной путь их решения.

На этом заканчивается шуточная, возможно, неостроумная история некоторой выдуманной первой в мире компьютерной сети. Для чего же был все-таки нужен этот простой и веселый пример? Прежде всего, читатель теперь имеет представление о том, с какими проблемами и задачами сталкивались люди, разрабатывавшие первые сетевые протоколы и приложения, которые он начнет изучать в процессе подготовки к экзамену CCNA. Несмотря на то что пример Пебблз может быть в достаточной степени смешным, проблемы, с которыми она столкнулась, так же как и проблемы, с которыми столкнулись разработчики сетевых технологий и успешно решили их, — одни и те же.

Второе несомненное достоинство рассказанной истории, особенно важное для читателей, слабо знакомых с сетевыми технологиями, состоит в том, что в ней представлены некоторые основополагающие концепции сетей:

- сети Ethernet требуют установки специальных модулей в каждый компьютер;
- такие модули должны иметь уникальные адреса (похожие на те, что использовались в сетевых картах Пебблз);
- компьютеры подключаются к концентраторам Ethernet с помощью специальных кабелей, сами концентраторы при этом повторяют полученный сигнал на всех портах;
- кабели обычно прокладываются по звездообразной топологии, или, другими словами, прокладываются от распределительного шкафа к кабельным узлам;
- приложения, такие как протокол передачи данных Фреда, или, в обычной жизни, протокол передачи файлов (FTP), используют аппаратное обеспечение для передачи содержимого компьютерных файлов; пользователи могут использовать в приложениях удобочитаемые имена, например, для доступа к веб-сайту вводить в командной строке браузера имя www.certskills.com, такое имя автоматически будет преобразовано в правильный уникальный адрес в сети.

Теперь мы перейдем к более серьезным главам, в которых рассматриваются реальные протоколы и устройства современных компьютерных сетей, а также темы, включенные в экзамен ICND1.

В этой главе...

- **Эталонная модель TCP/IP.** Объясняется терминология и концепции самой популярной во всем мире сетевой модели — TCP/IP, включая некоторые примеры таких протоколов, как HTTP, TCP, IP и Ethernet.
- **Эталонная модель OSI.** Описана терминология и функции модели OSI, а также проведено ее сравнение с моделью TCP/IP.

ГЛАВА 2

Сетевые модели TCP/IP и OSI

Сетевая модель, или сетевая структура, представляет собой упорядоченный набор документации и стандартов. По отдельности такие документы описывают небольшие независимые функции сети. Одни документы могут давать определение какого-либо протокола, т.е. набора логических правил и соглашений, которые должны выполнять сетевые устройства, чтобы взаимодействовать. Другие документы могут стандартизировать некоторые требования к физическим характеристикам сети, например, описывать полярность и величину напряжения на каких-либо контактах кабеля определенного типа. Совместно отдельные документы сетевой модели полностью описывают все элементы какой-либо сети, а также стандартизируют процесс ее разработки, что позволяет получить работоспособную сеть.

Чтобы создать работоспособную сеть, устройства в сети должны соответствовать требованиям и стандартам соответствующей сетевой модели. Если несколько компьютеров и других сетевых устройств используют стандартно реализованные протоколы, спецификации физического уровня и общие правила, а также правильно соединены кабелями, то все устройства в такой сети смогут вполне успешно обмениваться данными.

Сетевую модель можно себе представить как набор архитектурных планов для строительства дома. Очевидно, что дом можно построить и без таких планов, но результат будет намного лучше, если все же использовать чертежи. Если учесть, что обычно над постройкой дома работает много людей — стекольщики, электрики, каменщики, маляры и другие, — то им понадобится некоторый общий план, чтобы успешно завершить начатое дело. Аналогично при построении собственной сети можно написать собственное программное обеспечение, разработать собственные сетевые модули и в итоге построить сеть без использования каких-либо сетевых моделей. Тем не менее намного проще будет купить и внедрить продукты, которые соответствуют какой-либо известной сетевой модели. Производители аппаратного или программного обеспечения используют одни и те же сетевые модели, следовательно, их продукты будут совместимы друг с другом и смогут успешно взаимодействовать.

В экзамене CCNA требуются знания, относящиеся преимущественно к одной модели — TCP/IP (Transmission Control Protocol/Internet Protocol — протокол передачи данных/протокол Интернета). Эта модель активно использовалась на протяжении всей истории развития сетевых технологий, поэтому ее реализацию можно найти практически в каждой существующей на сегодняшний день операционной системе, например, как в мобильных телефонах, так и в высококлассовых мейнфреймах. Все сети, где встречается оборудование компаний Cisco, поддерживают протоколы TCP/IP, поэтому не удивительно, что основное внимание в экзамене уделяется именно этой модели.

В экзамене ICND1, и чуть больше в экзамене ICND2, кроме этого встречаются вопросы по второй распространенной эталонной модели — OSI (Open System Interconnection — модель взаимодействия открытых систем). С исторической точки зрения эталонная модель OSI представляет собой первую попытку создать сетевую модель. Поскольку такая модель была первой и довольно всеобъемлющей, множество терминов в сетевых технологиях взяты из нее или основаны на ее концепциях. Поэтому в данном разделе обсуждаются темы и терминология, связанные с моделью OSI.

Контрольные вопросы: знаете ли вы уже темы главы

Этот раздел предназначен для того, чтобы читатель мог предварительно оценить свои знания и решить, нужно ли ему читать главу целиком. Если ответы на девять из десяти вопросов даны правильно, можно сразу же перейти к последнему разделу “Подготовка к экзамену”. Основные темы этой главы и предварительных контрольных вопросов перечислены в табл. 2.1. Отвечая на контрольные вопросы и используя таблицу, читатель сможет достаточно точно определить свои знания в той или иной области. Ответы на вопросы приведены в приложении А.

Таблица 2.1. Темы контрольных вопросов

Основная тема	Номера вопросов
Эталонная модель TCP/IP	1–6
Эталонная модель OSI	7–10

1. Какой из перечисленных ниже протоколов относится к транспортному (transport) уровню модели TCP/IP? (Выберите несколько ответов.)
 - Ethernet.
 - HTTP.
 - IP.
 - UDP.
 - SMTP.
 - TCP.
2. Какой из перечисленных ниже протоколов относится к уровню доступа к сети (network access) модели TCP/IP? (Выберите несколько ответов.)
 - Ethernet.
 - HTTP.
 - IP.
 - UDP.
 - SMTP.
 - TCP.
 - PPP.
3. Когда протокол HTTP запрашивает протокол TCP о передаче каких-либо данных и контроле доставки, такой процесс будет примером:
 - Взаимодействия двух систем на одинаковом уровне.
 - Взаимодействия двух смежных уровней.

в) Эталонной модели OSI.

г) Все указанные выше ответы верны.

4. Примером какой технологии является процесс, когда протокол TCP передающего узла маркирует сегмент порядковым номером 1, а принимающий узел отправляет в ответ подтверждение приема с порядковым номером 1?
- а) Инкапсуляция данных.
 - б) Взаимодействие двух систем на одинаковом уровне.
 - в) Взаимодействие двух смежных уровней.
 - г) Эталонная модель OSI.
 - д) Все указанные выше ответы верны.
5. Примером какой технологии является процесс, когда служба веб-сервера добавляет к полю данных, в которое помещена веб-страница, заголовок протокола TCP, далее добавляет заголовок протокола IP, а потом заголовок и концевик канального уровня?
- а) Инкапсуляция данных.
 - б) Взаимодействие двух систем на одинаковом уровне.
 - в) Эталонная модель OSI.
 - г) Все указанные выше ответы верны.
6. Каким из перечисленных ниже терминов называют блок данных, когда он помещен между заголовком и концевиком канального уровня?
- а) Данные.
 - б) Цепочка.
 - в) Сегмент.
 - г) Фрейм.
 - д) Пакет.
 - е) Все вышеперечисленные ответы ошибочны, на канальном уровне нет инкапсуляции.
7. Какой из уровней модели OSI отвечает за логическую адресацию в рамках всей сети и маршрутизацию?
- а) Уровень 1.
 - б) Уровень 2.
 - в) Уровень 3.
 - г) Уровень 4.
 - д) Уровень 5.
 - е) Уровень 6.
 - ж) Уровень 7.
8. Какой из уровней модели OSI задает стандарты для кабельной системы и соединений между узлами?
- а) Уровень 1.

- б) Уровень 2.
 - в) Уровень 3.
 - г) Уровень 4.
 - д) Уровень 5.
 - е) Уровень 6.
 - ж) Уровень 7.
9. Какой из уровней модели OSI описывает стандарты форматов данных и шифрование трафика?
- а) Уровень 1.
 - б) Уровень 2.
 - в) Уровень 3.
 - г) Уровень 4.
 - д) Уровень 5.
 - е) Уровень 6.
 - ж) Уровень 7.
10. Какой из перечисленных ниже терминов не является названием уровня в модели OSI? (Выберите несколько ответов.)
- а) Уровень приложений.
 - б) Канальный уровень.
 - в) Уровень передачи.
 - г) Уровень представления.
 - д) Уровень Интернета.
 - е) Сеансовый уровень.

Основные темы

Эталонная модель TCP/IP

Сетевая модель (networking model), называемая также *сетевой архитектурой* (networking architecture), *сетевой схемой* (networking blueprint) или *эталонной моделью*, — это исчерпывающий набор документов. По отдельности каждый документ описывает одну небольшую функцию сети; совместно эти документы определяют все, что необходимо для работы компьютерной сети. Некоторые документы описывают *протокол* (protocol), представляющий собой набор логических правил, которые должны соблюдать коммуникационные устройства. Другие документы определяют некоторые физические требования к сетям. Например, документ может определять уровни напряжения тока, используемые в специфическом кабеле при передаче данных.

Сетевые модели можно считать архитектурными чертежами при строительстве дома. Конечно, дом можно построить и без чертежей. Но чертеж может гарантировать, что дом имеет правильную конструкцию и структуру, поэтому он не завалится и будет иметь соответствующие скрытые пространства для размещения трубопроводов, электрических, газовых магистралей и т.д. Кроме того, благодаря использованию документации множество разных людей, участвующих в строительстве дома (арматурщики, электрики, каменщики, маляры и т.д.), знают, что, следя чертежам при выполнении своей части работы, они не создадут проблем для других рабочих.

Точно так же вы можете построить и собственную сеть — написать собственное программное обеспечение, смастерить собственные сетевые карты и все остальное, чтобы получить рабочую сеть. Однако намного проще купить и использовать готовые продукты, которые уже соответствуют некой стандартной сетевой модели или схеме. Поскольку производители сетевых продуктов создавали свои товары с учетом некой сетевой модели, совместно их изделия должны работать хорошо.

История возникновения сетевой модели TCP/IP

Сегодня в мире компьютерных сетей используется только одна сетевая модель: TCP/IP (Transmission Control Protocol/Internet Protocol — протокол управления передачей/протокол Интернета). Но мир не всегда был настолько прост. Когда-то давным-давно не было никаких сетевых протоколов, в том числе и протокола TCP/IP. Производители создавали первые сетевые протоколы, но эти протоколы поддерживали только компьютеры данного производителя. Например, корпорация IBM выпустила в 1974 году свою сетевую модель системной сетевой архитектуры (Systems Network Architecture — SNA). Другие производители также создавали собственные сетевые модели. В результате, когда компания покупала компьютеры от трех производителей, сетевым инженерам зачастую приходилось создавать три разных сети на базе сетевых моделей, разработанных каждым из производителей, а затем, тем или иным способом, соединять эти сети, получая намного более сложные комбинированные сети. На рис. 2.1, *слева*, приведено общее представление того, как могла выглядеть корпоративная сеть компании в 1980-х годах, до того, как модель TCP/IP получила распространение в объединенных корпоративных сетях.

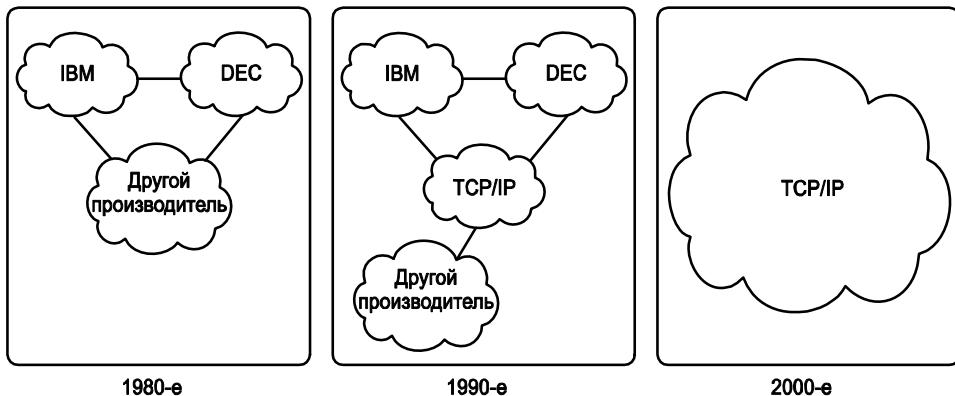


Рис. 2.1. Исторический прогресс: от собственных моделей к открытой модели TCP/IP

Хотя собственные сетевые модели производителей обычно работали хорошо, наличие открытой, независимой от производителя сетевой модели обеспечило бы равенство в конкуренции и уменьшило бы сложность. *Международная организация по стандартизации* (International Organization for Standardization — ISO) взяла на себя эту тяжелую ношу — разработку универсальной модели в конце 1970-х. Таким образом, в начале 80-х появилась сетевая модель, которая известна как эталонная модель взаимодействия открытых систем (Open System Interconnection — OSI). Организация ISO совершила благородный поступок и взяла на себя весь труд по созданию модели ISO: упорядочение и стандартизация существующих на тот момент протоколов и коммуникаций, разработка теоретических основ методов взаимодействия компьютерных систем во всем мире и т.п. Этой благородной цели было посвящено немало времени, кроме того, большинство технологически высокоразвитых стран принимало участие в процессе разработки и стандартизации модели.

Вторая менее формализованная попытка создать открытую, независимую от производителя сетевую модель была предпринята Министерством обороны США в рамках одного оборонного проекта. Множество исследователей, ученых и просто энтузиастов из различных университетов в США принимали участие в разработке и дальнейшем усовершенствовании оригинальной сетевой структуры, которая появилась благодаря Министерству обороны. Попытка создания открытой сетевой модели в конце концов увенчалась успешным набором протоколов, который сегодня известен под названием *стек TCP/IP*.

На протяжении 1990-х годов компании начали внедрять в свои корпоративные сети эталонные модели OSI, TCP/IP или обе вместе. Однако к концу 1990-х модель TCP/IP стала общепринятой, а модель OSI — нет. На рис. 2.1, *посредине*, приведено общее представление корпоративных сетей в это десятилетие, когда сети полагались на несколько сетевых моделей, включая и TCP/IP.

Ныне, в XXI столетии, доминирует модель TCP/IP. Собственные сетевые модели все еще существуют, но от них, по большей части, отказываются в пользу модели TCP/IP. Модель OSI из-за более медленного и чуть более сложного процесса стандартизации, по сравнению с TCP/IP, так никогда и не получила большой популярности на рынке телекоммуникаций. Модель TCP/IP практически полностью (как она сама, так и составляющие протоколы) первоначально была разработана добровольцами и энтузиастами со всего мира, поэтому она содержит больше протоколов

и технологий, чем какая-либо из существовавших и существующих на сегодняшний момент моделей (см. рис. 2.1, *справа*).

В этой главе будут описаны некоторые базовые принципы стандартной модели стека TCP/IP. Некоторые интересные факты, связанные со стеком TCP/IP, могут пригодиться в практической работе, тем не менее основная цель изложенного ниже материала — помочь читателю разобраться в том, что такая сетевая модель, сетевая структура и как в действительности они работают.

В этой главе также рассмотрены некоторые из наиболее распространенных терминов модели OSI. Видели ли вы когда-либо или работали за компьютером под управлением полного стека протоколов модели OSI, а не протоколов стека TCP/IP? Вероятно, нет, поскольку она очень мало распространена. Тем не менее с терминологией OSI приходится сталкиваться каждый день. В экзамене ICND1 (Interconnecting Cisco Network Devices 1 — Объединение устройств компании Cisco, часть 1) встречаются вопросы по основам модели OSI, поэтому можно сказать, что данная глава также поможет читателю подготовиться к соответствующему экзамену.

Структура протоколов стека TCP/IP

Модель TCP/IP описывает множество протоколов, позволяющих взаимодействовать компьютерам. Подробное описание протоколов, входящих в стандартный набор TCP/IP, представлено в документах, которые называются *запросами на комментарии* (Requests for Comments — RFC). (Вы можете найти документы RFC, используя любой сетевой поисковый механизм.) Модель TCP/IP не дублирует работу, уже проделанную некоторыми другими организациями по стандартизации или консорциумом производителей, просто ссылаясь на соответствующий стандарт или протокол, созданный этими группами. Например, *Институт инженеров по электротехнике и электронике* (Institute of Electrical and Electronic Engineers — IEEE) определяет локальные сети Ethernet; поэтому модель TCP/IP не определяет сети Ethernet в своих запросах на комментарии, а ссылается на документы IEEE Ethernet.

Компьютер, использующий протоколы TCP/IP, можно сравнить с обычным телефоном. Можно пойти в магазин, торгующий бытовой техникой, и купить телефонный аппарат какой угодно модели и производителя. Тем не менее, если принести его домой и включить в телефонную розетку тем же самым кабелем, каким был подключен старый аппарат, новый телефон будет работать. Производители телефонов знают стандарты телефонии для своей страны и производят телефоны в соответствии с ними.

Аналогично, когда вы сейчас покупаете новый компьютер, он, по сути, уже реализует модель TCP/IP, чтобы вы могли взять соответствующие кабели и подключить компьютер к сети. Теперь вы можете использовать веб-браузер для просмотра своего любимого веб-сайта. Почему? Операционная система на компьютере реализует части модели TCP/IP. Встроенная в компьютер плата Ethernet или плата беспроводной сети реализует некоторые стандарты LAN, используемые моделью TCP/IP. Короче говоря, производители, которые создали аппаратные средства и программное обеспечение, реализовали модель TCP/IP.

Чтобы упростить изучение сетевых моделей, каждая из них разделена на несколько функциональных разделов, называемых *уровнями* (layer). Каждый уровень включает протоколы и стандарты, относящиеся к данному функциональному разделу. Фактически есть две альтернативные модели TCP/IP, как показано на рис. 2.2.



Рис. 2.2. Две сетевые модели TCP/IP

Модель, показанная слева, исходная модель TCP/IP, разделена на четыре уровня. Верхние уровни сосредоточиваются на приложениях, которые должны передавать и получать данные, тогда как нижние уровни больше сосредоточиваются на средствах передачи битов между устройствами. Справа представлена более новая версия модели, сформированная за счет расширения уровня доступа к сети (слева) на два отдельных уровня: канального и физического. Обратите внимание на то, что модель, представленная справа, ныне используется чаще.

Большинство из вас уже слышали о некоторых протоколах TCP/IP, таких как перечисленные в табл. 2.2. Более подробная информация о большинстве протоколов и стандартов, перечисленных в этой таблице, приведена далее в книге. Ниже уровни модели TCP/IP рассматриваются подробнее.

Таблица 2.2. Структурная модель TCP/IP и примеры протоколов

Уровень модели TCP/IP	Примеры протоколов
Приложений	HTTP, POP3, SMTP
Транспортный	TCP, UDP
Интернет	IP
Доступа к сети	Ethernet, Point-to-Point Protocol (PPP), T/1

Уровень приложений TCP/IP

Уровень приложений стека TCP/IP предоставляет службы приложениям и программному обеспечению, работающему на компьютере. Сам он не определяет требования непосредственно к приложениям, а стандартизирует службы, которые могут понадобиться приложениям. Например, протокол уровня приложений HTTP (Hypertext Transfer Protocol — протокол передачи гипертекста) определяет, как веб-браузер может запрашивать содержимое веб-страницы с веб-сервера. Другими словами, уровень приложений представляет собой интерфейс между программным обеспечением компьютера и сетью.

Вероятно, наиболее популярным приложением TCP/IP на сегодняшний день является веб-браузер. Многие компании уже поменяли или как раз меняют свое программное обеспечение таким образом, чтобы с ним можно было работать через веб-браузер. К счастью, работать с браузером исключительно просто — нужно всего

лишь запустить его на компьютере, потом набрать адрес веб-сайта в строке ввода адреса, и в окне программы появится ожидаемая веб-страница.

Краткий обзор протокола HTTP

Что же в действительности происходит, когда веб-страница появляется в окне браузера?

Предположим, Боб запустил на своем компьютере веб-браузер. Браузер настроен таким образом, что он сразу обращается к стандартной странице веб-сервера его друга Ларри, или, другими словами, к его *домашней странице*. Схема работы браузера и сервера приведена на рис. 2.3.



Рис. 2.3. Схема работы приложения с веб-сервером

Итак, что же происходит? Первоначальный запрос от программного обеспечения компьютера Боба запрашивает сервер Ларри об отправке домашней страницы браузеру Боба. Веб-сервер Ларри настроен таким образом, что страница `home.html` является стандартной и в ней содержится домашняя страница Ларри. Программное обеспечение компьютера Боба получает файл страницы от сервера Ларри, и браузер корректно отображает его в своем окне.

Механизмы протокола HTTP

Этот пример демонстрирует, как приложения конечной точки (а именно приложение веб-браузера и приложение веб-сервера) используют уровень приложений протокола TCP/IP. Чтобы запросить веб-страницу и возвратить ее содержимое, приложения используют *протокол передачи гипертекста* (Hypertext Transfer Protocol — HTTP).

Протокол HTTP появился в начале 1990-х годов, когда Тим Бернерс-Ли (Tim Berners-Lee) создал первый веб-браузер и веб-сервер. Бернерс-Ли придал протоколу HTTP возможность запрашивать содержимое веб-страниц, а именно способность веб-браузера запрашивать файлы у сервера, и предоставил серверу возможность возвращать содержимое этих файлов. Общая логика соответствует тому, что изображено на рис. 2.3; а рис. 2.4 демонстрирует ту же идею, но с подробностями, специфическими для протокола HTTP.

ПРИМЕЧАНИЕ АВТОРА

Полная версия большинства веб-адресов, называемых также *универсальными локаторами ресурсов* (Universal Resource Locators — URL), начинаются с символов `http`, что означает использование протокола HTTP для передачи веб-страницы.

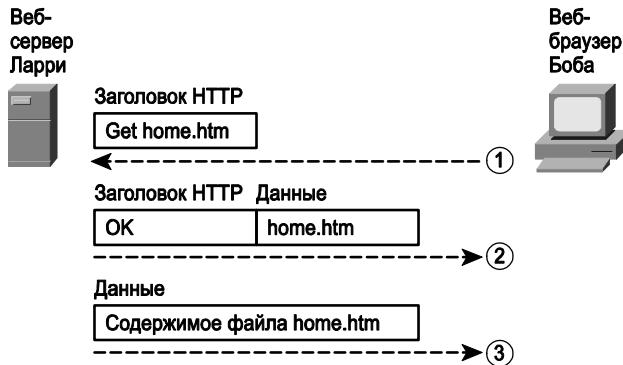


Рис. 2.4. Запрос HTTP GET, ответ HTTP и сообщение с данными

Чтобы получить веб-страницу от сервера Ларри (этап 1), Боб пересыпает сообщение с заголовком HTTP. Как правило, протоколы используют заголовки как место для размещения используемой ими служебной информации. Этот заголовок HTTP содержит запрос `get` (получить) на получение нужного файла. Обычно такой запрос содержит также имя файла (в данном случае `home.htm`), а если имя файла отсутствует, то веб-сервер предполагает, что запрашивается веб-страница по умолчанию.

Этап 2 на рис. 2.4 демонстрирует ответ веб-сервера Ларри. Сообщение начинается с заголовка HTTP с кодом возврата (200), означающим нечто столь же простое, как “OK”. Протокол HTTP определяет также другие коды возврата, таким образом, сервер может указать браузеру, сработал запрос или нет. (Еще один пример: при обращении к веб-странице, которая была не найдена, получаешь ошибку HTTP 404 “not found”, т.е. передается код возврата HTTP 404.) Второе сообщение включает также первую часть затребованного файла.

Ответ от сервера Ларри также содержит инструкцию HTTP, в заголовке которой написано что-то вроде “OK”. Ответ всегда содержит код в заголовке, который указывает запрашивающей стороне, может ли быть выполнен запрос. Например, если серверу приходит запрос на страницу, которая не существует, браузер получит сообщение HTTP с кодом ошибки 404, “страница не найдена”. Если же запрашиваемый файл был найден, то в ответ сервер передаст сообщение с кодом 200, который свидетельствует о том, что все в порядке и выполняется дальнейшая обработка запроса.

Этап 3 на рис. 2.4 демонстрирует еще одно сообщение веб-сервера Лэрри веб-браузеру Боб, но на сей раз без заголовка HTTP. Данные по протоколу HTTP передаются при посылке нескольких сообщений, каждое с частью файла. Чтобы не тратить впустую пространство при повторной посылке заголовков HTTP, содержащих ту же информацию, эти последующие сообщения просто опускают заголовок.

Транспортный уровень TCP/IP

Хотя в модели TCP/IP существует множество протоколов уровня приложений, его транспортный уровень содержит меньше протоколов. Двумя наиболее популярными протоколами транспортного уровня модели TCP/IP являются *протокол управления передачей* (Transmission Control Protocol — TCP) и *протокол пользовательских дейтаграмм* (User Datagram Protocol — UDP).

Протоколы транспортного уровня предоставляют службы протоколам уровня приложений, которые в модели TCP/IP располагаются на один уровень выше. Как протокол транспортного уровня предоставляет службы протоколу более высокого уровня? В этом разделе рассматриваются общие концепции на примере одной из служб, предоставляемой протоколом TCP: восстановление при ошибках. В последующих главах транспортный уровень исследуется более подробно и рассматривается куда больше его функций.

Основы восстановления при ошибках протокола TCP

Чтобы представить себе, что именно делает транспортный уровень, нужно сначала обратиться к верхнему уровню, а именно к уровню приложений. Зачем? Каждый уровень многоуровневой модели предоставляет некоторые службы вышестоящему уровню, — так протокол TCP уровня приложений предоставляет службу восстановления при ошибках.

Например, как показано на рис. 2.3, Боб и Ларри используют протокол HTTP для пересылки веб-страницы с веб-сервера на веб-браузер. А что произойдет, если, например, запрос на получение страницы от Боба где-то “потеряется” по пути? Или ответ от сервера Ларри, содержащий текст веб-страницы, не будет получен? В любом из указанных случаев информация не появится в браузере Боба.

Итак, стеку TCP/IP нужен механизм гарантированной доставки данных в компьютерной сети. Поскольку многим приложениям потребуется такая возможность, создатели протокола TCP включили в него возможность восстановления при ошибках. Для восстановления после ошибок протокол TCP использует концепцию подтверждений. На рис. 2.5 показана основная идея того, как протокол TCP замечает потерю данных и запрашивает у отправителя их повторную передачу.

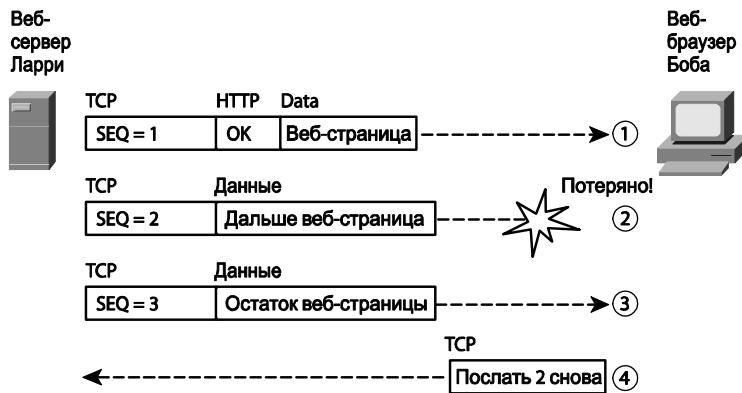


Рис. 2.5. Служба восстановления при ошибках протокола TCP, предоставляемая протоколу HTTP

Как показано на рис. 2.5, веб-сервер Ларри посыпает веб-страницу на веб-браузер Боба, используя три отдельных сообщения. Обратите внимание: здесь представлены те же заголовки HTTP, что и на рис. 2.4, а также заголовок TCP. Заголовок TCP демонстрирует порядковый номер (SEQ) каждого сообщения. На этом примере показано: в сети есть некая проблема, не позволившая доставить сегмент с порядко-

вым номером 2. Когда Боб получает сообщения с порядковыми номерами 1 и 3, но не получает сообщения с порядковым номером 2, он понимает, что сообщение 2 было потеряно. Согласно этой логике реализации протокола TCP, он запрашивает у сервера Ларри повторную передачу сообщения 2.

Взаимодействие на смежных и равноправных уровнях

Пример на рис. 2.4 демонстрирует также функцию *взаимодействия на смежных уровнях* (adjacent-layer interaction), которая описывает концепцию взаимодействия смежных уровней сетевой модели на том же компьютере. В этом примере протоколу более высокого уровня (HTTP) нужно сделать нечто, на что он неспособен (восстановление при ошибках). Он просит об этом протокол следующего, нижнего уровня (TCP), и протокол нижнего уровня предоставляет службу уровню выше него.

Рис. 2.4 демонстрирует также пример подобной функции *взаимодействия на равноправных уровнях* (same-layer interaction). Когда определенные слои одного компьютера хотят взаимодействовать с равноправным уровнем на другом компьютере, для хранения информации, которой они хотят обмениваться, эти два компьютера используют заголовки. Например, на рис. 2.4 компьютер Ларри установил порядковые номера 1, 2 и 3, чтобы компьютер Боба мог заметить отсутствие некоторых данных. Процесс передачи на компьютере Ларри создал заголовки TCP с последовательными номерами; процесс на компьютере Боба получает и реагирует на сегменты TCP. Этот процесс, в ходе которого два компьютера передают и интерпретируют информацию в заголовке, используемом тем же уровнем, называется *взаимодействием на равноправном уровне*.

В табл. 2.3 кратко описаны ключевые моменты взаимодействия смежных уровней на одном и том же компьютере и механизм взаимодействия равноправных уровней на разных компьютерах в сети.



Таблица 2.3. Взаимодействие на смежных и равноправных уровнях

Концепция	Описание
Взаимодействие на равноправных уровнях между разными компьютерами	Два компьютера используют для взаимодействия протокол. Протоколом называют формальный набор правил, соглашений и форматов, в котором также используются заголовки для упорядоченного обмена информацией между компьютерами
Взаимодействие на смежных уровнях в одном компьютере	В одном компьютере один уровень может предоставлять некоторые службы другому компьютеру. Программное или аппаратное обеспечение, в котором реализованы процедуры верхнего уровня, запрашивает нижний уровень о выполнении некоторой функции

Уровень Интернета модели TCP/IP

Уровень приложений включает множество протоколов, а транспортный уровень — существенно меньше, а именно два: TCP и UDP. Основным протоколом уровня Интернета модели TCP/IP является *протокол Интернета* (Internet Protocol — IP). Фактически название *TCP/IP* — это просто названия двух наиболее распространенных протоколов (TCP и IP), разделенные косой чертой.

Протокол IP предоставляет несколько средств, наиболее важными из которых являются адресация и маршрутизация. Этот раздел начинается со сравнения адресации и маршрутизации протокола IP с другой общеизвестной системой почтовой

службы, которая использует адресацию и маршрутизацию. Далее в этом разделе содержится введение в IP-адресацию и маршрутизацию. (Более подробная информация по этой теме приведена в главе 5.)

Протокол Интернета и почтовая служба

Предположим, вы написали два письма: одно другу на другой стороне страны и одно другу на другой стороне города. Вы написали адреса на конвертах, наклеили марки и подготовили оба письма к отправке по почте. Есть ли разница в том, как вы готовили каждое письмо? Никакой. Обычно вы просто бросаете их в тот же почтовый ящик, и ожидаете, что почтовая служба доставит оба письма.

Однако почтовая служба должна позаботиться о каждом письме индивидуально и принять решение о том, куда послать каждое письмо, чтобы оно дошло до адресата. Письмо, посланное в пределах города, сотрудникам почтового отделения достаточно поместить в соответствующий грузовик.

Письмо, которое должно пересечь всю страну, почта посыпает другому почтовому отделению, затем другое почтовое отделение пересыпает его следующему и так далее, пока оно не будет доставлено через всю страну. В каждом почтовом отделении сотрудники должны обработать письмо и решить, куда его послать далее.

Чтобы все это работало, у почтовой службы есть регулярные маршруты для маленьких и больших грузовиков, самолетов, судов и так далее, по которым перевозятся письма между почтовыми отделениями. Служба способна получать и передавать письма, при этом она должна принимать правильное решение о том, куда именно послать каждое письмо далее (рис. 2.6).

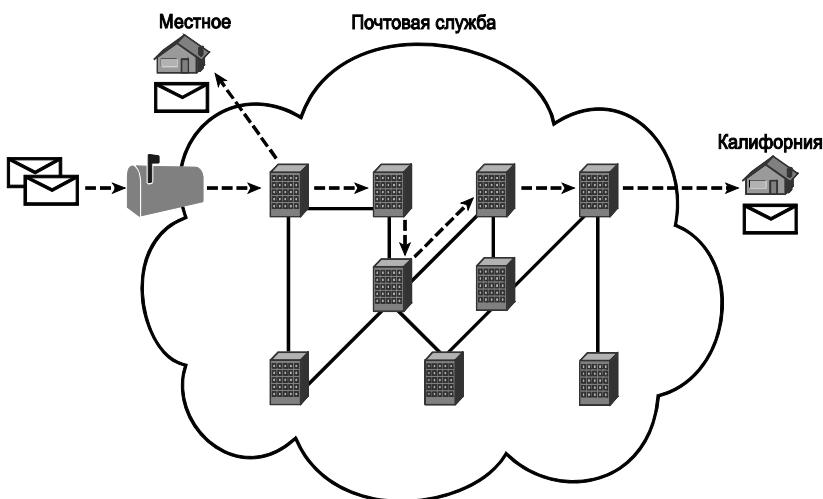


Рис. 2.6. Почтовая служба доставляет письма

Рассмотрим в контексте почтовой службы, в чем разница между человеком, посыпающим письмо, и сотрудником почты. Отправитель письма ожидает, что почтовая служба доставит письмо куда нужно, однако он не обязан знать точный путь следования письма. Сотрудник почтовой службы, напротив, не пишет письмо, а принимает его от клиента. Но чтобы иметь возможность доставить письмо, он должен быть подробно осведомлен об адресах и почтовых кодах, группирующих адреса в большие группы.

Уровни приложений и транспортные уровни модели TCP/IP выступают в роли человека, посылающего письма через почтовую службу. Эти верхние уровни работают точно так же, независимо от того, находятся ли компьютеры назначения в той же локальной сети или их разделяет Интернет. Посылая сообщение, эти верхние уровни полагаются на уровень, расположенный ниже их, на уровень Интернета, который должен доставить сообщение.

Нижние уровни модели TCP/IP, Интернета и доступа к сети выступают в роли почтовой службы, которая правильно доставит сообщения соответствующим получателям. Для этого нижние уровни должны понимать основы физической сети, поскольку они должны выбрать, как лучше доставить данные от одного хоста на другой.

“Так какое же отношение имеет почта к сетевым технологиям?” — спросит читатель. Протокол Интернета (Internet Protocol — IP), протокол уровня Интернета модели TCP/IP работает по тому же принципу, что и почта. Протокол IP определяет адреса для каждого компьютера или хоста в сети, причем каждый хост должен иметь собственный уникальный IP-адрес, точно так же, как и в обычной почте у каждого получателя должен быть свой адрес (город, улица, дом, квартира). На уровне Интернета происходит выбор наилучшего маршрута и пересылка пакета, которую выполняют специализированные устройства — маршрутизаторы. Точно так же как в почтовой службе есть специализированная инфраструктура, состоящая из почтовых отделений, сортировочных машин, грузовиков, самолетов и обученного персонала, данный уровень модели определяет, какая именно инфраструктура нужна, как она должна быть построена и как сеть может доставить данные нужным компьютерам в сети.

Основы адресации протокола Интернета

Протокол IP определяет адреса по нескольким важным причинам. В первую очередь потому, что каждому устройству, которое использует модель TCP/IP (*хосту* (host) TCP/IP), требуется уникальный адрес, чтобы его можно было идентифицировать в сети. Протокол IP определяет также группировку адресов, аналогично группам в почтовом индексе, используемом почтовой службой США.

Чтобы понять основы, рассмотрим рис. 2.7, на котором показаны знакомый веб-сервер Ларри и веб-браузер Боб; но теперь уже без игнорирования сетевой инфраструктуры между ними.

В первую очередь обратите внимание на примеры IP-адресов. Каждый IP-адрес содержит четыре числа, разделенных точками. В данном случае для Ларри использован IP-адрес 1.1.1.1, а для Боба — 2.2.2.2. Этот стиль чисел называется *десятичным представлением с разделительными точками* (Dotted Decimal Notation — DDN).

На рис. 2.7 представлены также три группы адресов. В этом примере все IP-адреса, начинающиеся с 1, должны располагаться в области слева вверху, как показано на рисунке, все адреса, начинающиеся с 2, — справа вверху, а начинающиеся с 3 — внизу.

Кроме того, на рис. 2.7 представлены пиктограммы, которые представляют IP-маршрутизаторы. *Маршрутизатор* (router) — это сетевое устройство, соединяющее вместе части сети TCP/IP в целях маршрутизации (пересылки) пакетов IP соответствующему получателю. Маршрутизаторы выполняют работу, аналогичную той, которую выполняют сотрудники почтового отделения: они получают пакеты IP на различных физических интерфейсах и на основании IP-адреса, присвоенного пакету, принимают решение об их пересылке некоторому другому сетевому интерфейсу.

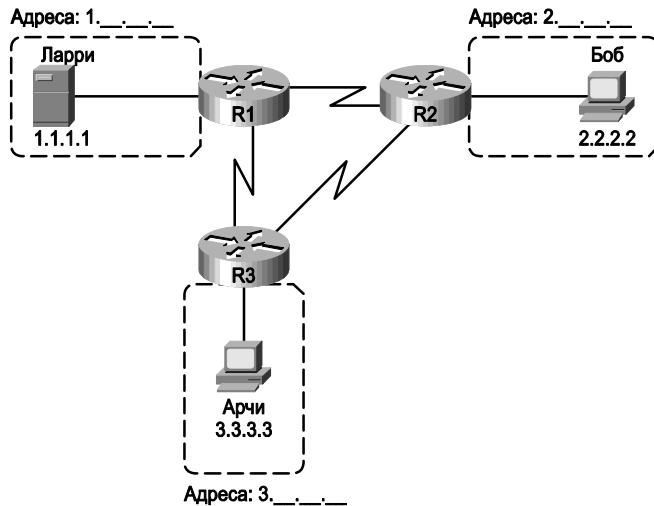


Рис. 2.7. Простая сеть TCP/IP: три маршрутизатора со группированными IP-адресами

Основы маршрутизации протокола Интернета

Уровень Интернета модели TCP/IP использует протокол IP, предоставляющий службы пересылки пакетов IP от одного устройства другому. Любое обладающее IP-адресом устройство может подключиться к сети TCP/IP и передавать пакеты. В этом разделе представлен простой пример маршрутизации IP.

ВНИМАНИЕ!

Термин *хост IP* (IP host) относится к любому устройству, независимо от его размера или мощности, которое имеет IP-адрес и подключено к любой сети TCP/IP.

На рис. 2.8 повторяется знакомый случай, когда веб-сервер Ларри передает часть веб-страницы браузеру Боба, но теперь с подробностями IP. Обратите внимание: внизу слева у сервера Ларри есть знакомые данные приложения, заголовки HTTP и TCP. Кроме того, сообщение теперь содержит также заголовок IP, который включает IP-адрес отправителя (адрес Ларри 1.1.1.1) и IP-адрес получателя (адрес Боба 2.2.2.2).

Первый этап (рис. 2.8, слева) начинается с того, что Ларри готов послать пакет IP. Процесс на компьютере Ларри решает послать пакет некоему маршрутизатору (ближайшему маршрутизатору в той же сети LAN), рассчитывая, что он знает, как переслать пакет дальше. (Эта логика очень похожа на нас, когда мы, посылая свои письма, бросаем их в ближайший почтовый ящик.) Ларри не обязан ничего знать ни о топологии, ни о других маршрутизаторах.

На втором этапе маршрутизатор R1 получает пакет IP, и его процесс IP принимает решение. Маршрутизатор R1 исследует адрес получателя (2.2.2.2), сравнивая его с известными ему маршрутами IP, и решает переслать пакет маршрутизатору R2. Этот процесс пересылки пакета IP называется *маршрутизацией IP* (IP routing), или просто *маршрутизацией* (routing).

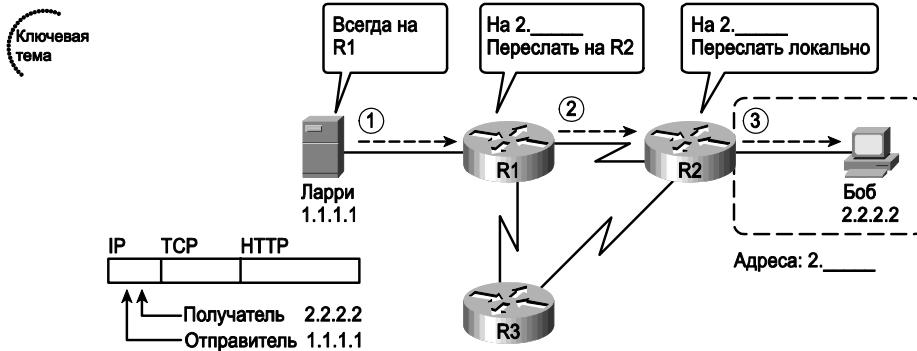


Рис. 2.8. Простой пример маршрутизации

На третьем этапе маршрутизатор R2 следует той же логике, что и маршрутизатор R1. Его процесс IP сравнивает IP-адрес получателя пакета (2.2.2.2) с известными ему маршрутами IP и решает переслать пакет непосредственно Бобу.

Все экзамены CCNA требуют глубоких знаний протокола IP. Фактически в половине глав этой книги рассматривается некоторое средство, имеющее непосредственное отношение к адресации, маршрутизации IP и тому, как маршрутизаторы осуществляют маршрутизацию.

Уровень доступа к сети TCP/IP

Уровень доступа к сети модели TCP/IP называют еще уровнем соединения хоста и сети. Он стандартизирует аппаратное обеспечение и протоколы, используемые для передачи данных по разным физическим сетям. Термин *доступ к сети* (network access) отражает тот факт, что этот уровень определяет, как именно осуществляется доступ или использование физической среды передачи, поверх которой передаются данные.

Точно так же как и любой другой уровень в сетевой модели, уровень доступа к сети TCP/IP предоставляет службы вышестоящим уровням. Когда процесс хоста или маршрутизатора IP решает послать пакет IP на другой маршрутизатор или хост, он использует возможности уровня доступа к сети для передачи этого пакета следующему хосту или маршрутизатору.

Поскольку каждый уровень предоставляет службы уровню выше его, уделим мимо размышлений о логике IP, связанной с происходящим на рис. 2.8. В том примере логика IP хоста Ларри принимает решение передать пакет IP на ближайший маршрутизатор (R1), без упоминания о лежащей в основе сети Ethernet. На самом деле для доставки этого пакета с хоста Ларри на маршрутизатор R1 должна использоваться сеть Ethernet, которая реализует протоколы уровня доступа. На рис. 2.9 демонстрируются четыре этапа процесса, происходящего на уровне доступа к сети, позволяющего Ларри передать пакет IP маршрутизатору R1.

ВНИМАНИЕ!

На рис. 2.9 сеть Ethernet изображена как серия линий. Сетевые диаграммы зачастую используют это соглашение при изображении локальных сетей Ethernet в случаях, когда фактическая кабельная проводка и устройства LAN не важны для текущего обсуждения, как в данном случае. У реальной сети LAN были бы кабели и такие устройства, как коммутаторы LAN, которые не представлены на этом рисунке.

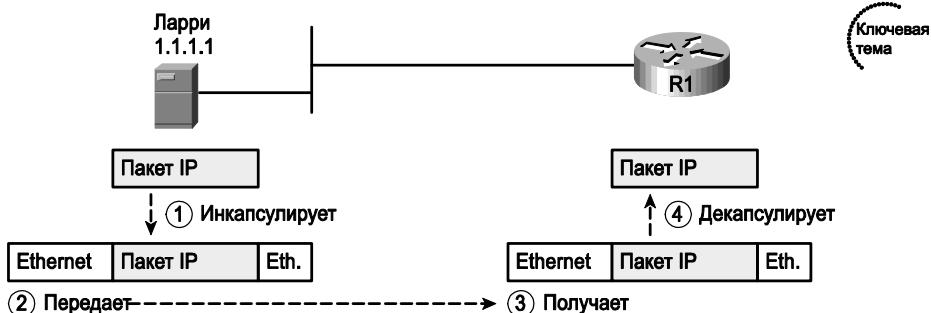


Рис. 2.9. Для пересылки пакета IP маршрутизатору R1 Ларри использует Ethernet

На рис. 2.9 показаны четыре этапа. Первые два происходят на сервере Ларри, а последние два — на маршрутизаторе R1.

- Этап 1** Сервер Ларри инкапсулирует пакет IP между заголовком и концевиком Ethernet, создавая фрейм (frame) Ethernet.
- Этап 2** Сервер Ларри физически передает биты этого фрейма Ethernet, используя электрический ток в кабеле Ethernet.
- Этап 3** Маршрутизатор R1 физически получает электрический сигнал по кабелю и восстанавливает те же биты, интерпретируя значения электрических сигналов.
- Этап 4** Маршрутизатор R1 деинкапсулирует пакет IP из фрейма Ethernet, удаляя и отбрасывая заголовок и концевик Ethernet.

Таким образом, совместная работа процессов доступа к сети на сервере Ларри и маршрутизаторе R1 позволила доставить пакет с хоста Ларри на маршрутизатор R1.

ВНИМАНИЕ!

Протоколы определяют **заголовки** (header) и **концевики** (trailer) по той же причине, но заголовки располагаются в начале сообщения, а концевики — в конце.

Уровень доступа к сети содержит множество протоколов и стандартов. Например, уровень доступа к сети включает все варианты протоколов Ethernet наряду с несколькими другими стандартами LAN, которые были популярны в прошедшем десятилетии. Уровень доступа к сети включает стандарты WAN для различных физических сред, которые значительно отличаются от стандартов LAN в связи с большей длиной дистанций, задействованных при передаче данных. Этот уровень включает также популярные стандарты WAN, которые добавляют свои заголовки и концевики, как показано в общем на рис. 2.7, а также такие протоколы, как *протокол двухточечного соединения* (Point-to-Point Protocol — PPP) и Frame Relay. Более подробная информация по этой теме для сетей LAN и WAN приведена в главах 3 и 4 соответственно.

Таким образом, уровень доступа к сети TCP/IP включает две разные функции: физическая передача данных, а также протоколы и правила, контролирующие использование физической среды. Чтобы соответствовать этой логике, пятиуровневая модель TCP/IP просто разделяет уровень доступа к сети на два уровня (канальный и физический).

Терминология модели TCP/IP

Прежде чем закончить это введение в модель TCP/IP, рассмотрим некоторые оставшиеся подробности модели и связанную с ней терминологию.

Сравнение двух моделей TCP/IP

Функции, определенные в уровне доступа к сети, могут быть разделены на две основные категории: функции, связанные с физической передачей данных непосредственно, и таковые, связанные с ней косвенно. Например, в четырех этапах, представленных на рис. 2.9, этапы 2 и 3 специфичны именно для передачи данных, а этапы 1 и 4 (инкапсуляции и деинкапсуляция) связаны с ней только косвенно. Это разделение станет понятней по мере изучения дополнительных подробностей каждого протокола и стандарта.

Существуют две альтернативные модели TCP/IP, верхние уровни у них идентичны, а нижние отличаются. Уровень доступа к сети одной модели разделен во второй на два уровня, чтобы отделить физические подробности передачи от других функций. На рис. 2.10 снова представлены эти две модели, но с акцентом на различия.

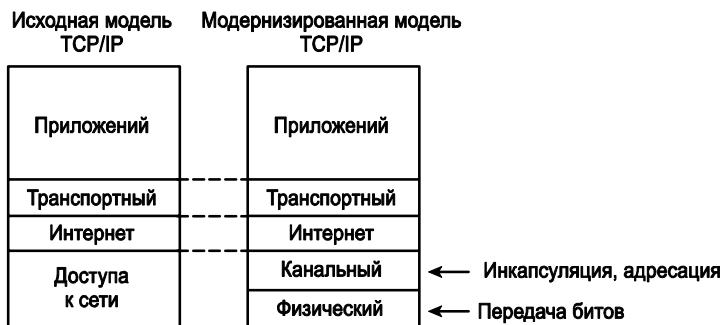


Рис. 2.10. Уровень доступа к сети по сравнению с канальным и физическим уровнями

Терминология инкапсуляции данных

Выше были рассмотрены принципы работы разных протоколов, HTTP, TCP, IP и Ethernet. Из приведенного описания можно заметить, что каждый из них добавляет собственный заголовок (а иногда и контрольную сумму в конце) к каждому блоку данных от вышестоящих уровней. *Инкапсуляция* (encapsulation) описывает процесс добавления заголовка (и иногда концевика) к некоторому блоку данных.

Большинство примеров этой главы демонстрируют процесс инкапсуляции. Так, например, протокол HTTP инкапсулирует веб-страницу в заголовок HTTP (см. рис. 2.4). Далее протокол TCP инкапсулирует данные и заголовок протокола HTTP в собственный заголовок (см. рис. 2.5), а протокол IP инкапсулирует все вместе в свой заголовок IP (см. рис. 2.7). В итоге блок данных от уровня Интернета (IP) инкапсулируется в заголовок и концевик протокола уровня доступа к сети Ethernet (см. рис. 2.9).

Таким образом, процесс отправки информации хостом TCP/IP состоит из пяти этапов. Первые четыре этапа выполняются четырьмя уровнями набора TCP/IP, а последний этап описывает передачу данных хостом в реальной физической среде сети. Факти-

чески, если вы используете модель TCP/IP с пятью уровнями, каждый этап совпадает с соответствующим уровнем. Кратко этапы передачи потока данных описаны ниже.

- Этап 1** Создание и инкапсуляция данных уровня приложений в заголовки нужного протокола уровня приложений. Например, сообщение “HTTP OK” может быть помещено в заголовок HTTP и добавлено к блоку данных, содержащему веб-страницу.
- Этап 2** Инкапсуляция блока данных от уровня приложений в заголовок транспортного уровня. Для пользовательских приложений может быть использован протокол TCP или UDP.
- Этап 3** Инкапсуляция блока данных от транспортного уровня в заголовок уровня Интернета (т.е. заголовок IP). Протокол IP определяет IP-адреса, уникально идентифицирующие каждый компьютер.
- Этап 4** Инкапсуляция блока данных от уровня Интернета в заголовок и концевик уровня доступа к сети. Это единственный уровень, использующий как добавление заголовка, так и концевика с контрольной суммой.
- Этап 5** Передача битов. На физическом уровне информация кодируется в специальный сигнал, который зависит от среды и технологии передачи фреймов.

На рис. 2.11 показана описанная выше концепция; номера слева соответствуют перечисленным этапам передачи информации. Поскольку на уровне приложений далеко не всегда к блоку данных добавляется заголовок, на этом рисунке у уровня приложений отсутствует какой-либо заголовок.

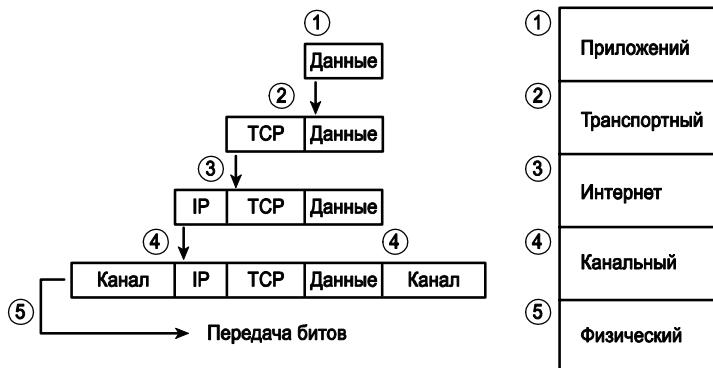


Рис. 2.11. Пять этапов инкапсуляции данных в модели TCP/IP

Названия сообщений TCP/IP

Следует также обратить пристальное внимание на такие термины, как *сегмент* (segment), *пакет* (packet) и *фрейм* (frame), а также на смысловую нагрузку каждого из них. Каждый из перечисленных терминов описывает инкапсуляцию данных на соответствующем уровне, т.е. добавление заголовка нужного уровня и, возможно, концевика. Каждое из приведенных определений относится к своему собственному уровню: сегмент связан с транспортным уровнем, пакет относится к уровню Интернета, фрейм — к уровню доступа к сети. На рис. 2.12¹ показаны уровни и соответствующие им блоки данных.

¹ Как LH обозначен заголовок уровня доступа к сети, а как LT — концевик — Примеч. ред.



Рис. 2.12. Блоки данных разных уровней и инкапсуляция

На рис. 2.12 инкапсулированные данные помечены просто словом “данные”. Если сосредоточиться на функциях какого-либо из уровней, то, что находится в поле данных, не представляет для уровня никакого интереса, это просто какой-то блок информации, не имеющий отношения к текущему уровню. Например, в пакете IP может после его заголовка идти заголовок TCP, за ним — заголовок протокола HTTP, дальше будут присутствовать данные какой-либо веб-страницы в поле данных. Однако для протокола IP все, что идет за его собственным заголовком, представляет собой просто некоторые “данные”. Поэтому на многих схемах, когда иллюстрируют поля пакета IP, все, что идет после заголовка уровня Интернета, называют “данными” и не обращают на них ни малейшего внимания.

Эталонная модель OSI

Когда-то многие полагали, что модель OSI выиграет сражение сетевых моделей, обсуждавшихся ранее. Если бы это произошло, то вместо модели TCP/IP на каждом компьютере в мире выполнялась бы модель OSI.

Однако модель OSI не выиграла это сражение. Фактически модель OSI больше не существует как сетевая модель, которая применялась бы вместо модели TCP/IP, хотя некоторые из первоначальных протоколов, на которых была основана модель OSI, все еще существуют.

Так почему же модель OSI рассматривается в этой книге? Дело в терминологии. На протяжении тех лет, когда многие были уверены, что модель OSI станет общепринятой во всем мире (главным образом в конце 1980–начале 1990-х), многие производители оборудования и издаваемая документация протоколов начали использовать терминологию из модели OSI. Сегодня эта терминология осталась. Поэтому, хотя работать с компьютером, использующем модель OSI, вероятно, никогда и не придется, чтобы понять современную сетевую терминологию, необходимо узнать кое-что о модели OSI.

Сравнение моделей OSI и TCP/IP

С точки зрения фундаментальных концепций эталонная модель OSI очень похожа на эталонную модель TCP/IP. Она содержит семь уровней, каждый из которых выполняет свои особые функции в сети. Как и уровни модели TCP/IP, каждый из уровней модели OSI ссылается на несколько протоколов и стандартов, которые реализуют функции, определенные каждым уровнем. Для уже существующих протоколов, например стека TCP/IP, новые протоколы и стандарты не разрабатывались, существующие разработки просто были стандартизированы в рамках модели OSI. Например, IEEE к тому времени уже выпустил все необходимые спецификации технологии Ethernet, поэтому комитеты OSI не тратили время и ресурсы на то, чтобы выпустить новые стандарты или новый тип технологии Ethernet, они просто ссылались на существовавшие на тот момент стандарты IEEE.

На сегодняшний день модель OSI используется в качестве эталона для сравнения с другими моделями. На рис. 2.13 приведено сравнение семи уровней модели OSI и модели TCP/IP для четырех и пяти уровней.



Рис. 2.13. Модель OSI по сравнению с двумя моделями TCP/IP

Далее в этом разделе рассматриваются две области применения терминологии OSI в настоящее время: описание других протоколов и описание процесса инкапсуляции. При этом в тексте кратко описывается каждый уровень модели OSI.

Описание протоколов со ссылками на уровни модели OSI

Даже сейчас сетевые документы зачастую описывают протоколы и стандарты TCP/IP, ссылаясь на уровни модели OSI как по номерам уровней, так и по их названиям. Например, обычное описание коммутатора LAN — “коммутатор второго уровня”, где часть “второго уровня” относится к уровню 2 модели OSI. Поскольку у модели OSI был действительно четкий набор функций, связанных с каждым из его семи уровней, зная эти функции, можно легко понять, что подразумеваю люди, когда называют продукт или функции по имени уровня модели OSI.

Так, например, уровень Интернета модели TCP/IP, единственным протоколом которого является IP, соответствует третьему уровню модели OSI. Поэтому многие специалисты используют терминологию уровней модели OSI и говорят, что протокол IP является протоколом сетевого уровня, или протоколом третьего уровня. В действительности, если использовать нумерацию модели TCP/IP и в общепринятом стиле начинать отсчет уровней снизу, протокол IP относится ко второму или третьему уровню модели в зависимости от используемой версии модели TCP/IP. Но даже при том, что протокол IP относится к протоколу TCP/IP, все используют названия уровней модели OSI и их номера при описании протокола IP и, собственно говоря, любого другого протокола.

Посмотрев на рис. 2.13, можно вполне обоснованно сказать, что сетевой уровень и уровень Интернета очень схожи, однако объяснить, почему — невозможно. Чтобы понять, почему тот или иной уровень модели TCP/IP соответствует уровню модели OSI, необходимо владеть более глубокими знаниями об уровнях OSI. Так, например, как сетевой, так и уровень Интернета задают логическую адресацию и правила маршрутизации в сети. Хотя детали процессов и спецификаций обеих моделей могут немного отличаться, но функции и цели обоих уровней вполне одинаковы.

В качестве другого примера можете припомнить, что транспортный уровень модели TCP/IP определяет много функций, включая восстановление при ошибках.

Транспортный уровень модели OSI также определяет те же функции, хоть и с другими деталями и специфическими протоколами. В результате сетевая индустрия имеет протокол TCP как протокол уровня 4 или как протокол транспортного уровня, опять-таки на основании номера уровня модели OSI и его названия.

Функции уровней модели OSI

Компания Cisco требует от специалистов уровня CCNA, чтобы они понимали на базовом уровне функции каждого из семи уровней модели OSI, а также помнили названия всех уровней и порядок их следования. Не менее полезно будет также знать, функциям какого уровня модели OSI наиболее близко соответствует каждое упомянутое в данной книге устройство или протокол.

Ныне, поскольку большинство людей намного лучше знакомы с функциями модели TCP/IP, чем с функциями модели OSI, один из лучших способов узнать о некой функции уровня модели OSI — это подумать о функциях в модели TCP/IP и соотнести их с уровнями модели OSI. Если вы используете модель TCP/IP с пятью уровнями, четыре основных уровня модели OSI практически совпадают с таковыми у модели TCP/IP. Единственное различие в четырех верхних уровнях — это название уровня 3, в модели OSI — это сеть, а в TCP/IP — Интернет. Три верхних уровня эталонной модели OSI (уровень приложений, представления данных и сеансовый, т.е. уровни 7, 6 и 5) задают те функции, которые относятся к уровню приложений TCP/IP. В табл. 2.4 описаны основные функции всех семи уровней модели OSI.

Таблица 2.4. Функции уровней эталонной модели OSI

Уровень	Описание функций
7	Уровень приложений (application layer) является ближайшим к пользователю и предоставляет службы его приложениям. Он является интерфейсом между приложениями и коммуникационным программным обеспечением. Данный уровень также определяет процесс аутентификации пользователя
6	Уровень представления (presentation layer) преобразует данные в один из многочисленных существующих форматов, который поддерживается обеими системами и отвечает за согласование формата передачи данных, например, будет это текст в кодировке ASCII ² или EBCDIC ³ , или бинарный файл, или формат BCD ⁴ , или изображение JPEG ⁵ . Шифрование информации относится к данному уровню и является его службой
5	Как понятно из названия, сеансовый уровень (session layer) устанавливает сеансы связи между двумя рабочими станциями, управляет ими и разрывает их. Он также синхронизирует диалог между уровнями представления двух систем и управляет двунаправленным обменом данными так, что приложения верхних уровней уведомляются о получении некоторого завершенного набора сообщений. Этот уровень передает уровню представления данных непрерывный поток данных

² Сокращение от American standard code for information interchange — Американский стандартный код обмена информацией. — Примеч. ред.

³ Сокращение от Extended Binary Coded Decimal Interchange Code — расширенный двоично-десятичный код обмена информацией. — Примеч. ред.

⁴ Сокращение от Binary Coded Decimal — двоично-десятичное число. — Примеч. ред.

⁵ Сокращение от Joint Photographic Experts Group — объединенная группа экспертов по машинной обработке фотографических изображений, алгоритм сжатия неподвижного изображения. — Примеч. ред.

Окончание табл. 2.4

Уровень	Описание функций
4	<i>Транспортный уровень</i> (transport layer) сегментирует данные передающей станции и вновь собирает их в единое целое на принимающей стороне. Протоколы этого уровня предоставляют множество служб, которые подробно рассмотрены в главе 6. Уровни 5–7 модели OSI сфокусированы на проблемах приложений, а четвертый уровень связан с проблемами доставки данных дистанционному компьютеру, например, с коррекцией ошибок и контролем потока данных
3	<i>Сетевой уровень</i> (network layer) является комплексным уровнем, обеспечивающим выбор маршрута и соединение между собой двух рабочих станций, которые могут быть расположены в географически удаленных друг от друга сетях. Он решает три основные задачи: логическая адресация, маршрутизация (перенаправление пакетов) и определение маршрутов в сети. Концепция маршрутизации определяет, как именно специализированные устройства (обычно это маршрутизаторы) перенаправляют пакеты к конечному получателю. Логическая адресация указывает, как именно должен быть сформирован адрес устройства в сети и как такой адрес будет использоваться в маршрутизации. Механизм определения маршрутов указывает, как именно протоколы маршрутизации способны выяснить абсолютно все маршруты в сети и как выбрать наилучший из них
2	<i>Канальный уровень</i> (data link layer) обеспечивает надежную передачу данных по физическому каналу. Он задает правила, определяющие, как именно устройство может переслать данные в определенной среде передачи. Протоколы канального уровня также задают формат заголовков и концевиков второго уровня, которые позволяют успешно передавать данные устройствам в какой-либо среде
1	<i>Физический уровень</i> (physical layer) определяет электрические, процедурные и функциональные спецификации для среды передачи данных, в том числе стандартные разъемы, схемы расположения выводов и назначение контактов, уровни напряжений, синхронизацию изменений напряжения, кодирование сигнала в среде, метод модуляции световых сигналов и правила активации и деактивации физической среды передачи

В табл. 2.5 перечислены основные устройства и протоколы, наиболее часто встречающиеся в экзамене CCNA и этой книге, а также указана их привязка к уровням модели OSI. Следует заметить, что в действительности большинство из приведенных сетевых устройств работает сразу с несколькими уровнями модели OSI. Указанный в табл. 2.5 уровень является самым верхним, с которым может работать устройство в процессе выполнения своих основных задач. В эталонной модели OSI, если протокол или служба работает на нескольких уровнях, принято указывать самый верхний из них. Например, маршрутизаторы всегда относят к уровню 3 эталонной модели, хотя, вполне очевидно, они содержат функции уровней 1 и 2.

Таблица 2.5. Эталонная модель OSI: примеры устройств и протоколов

Название уровня	Протоколы и спецификации	Устройства
Уровни приложений, представления данных и сеансовый (с 5 по 7)	Telnet, HTTP, FTP, SMTP, POP3, VoIP, SNMP	Хосты, брандмауэр, система обнаружения вторжений
Транспортный (4)	TCP, UDP	Хосты, брандмауэры
Сетевой (3)	IP	Маршрутизатор
Канальный (2)	Ethernet (IEEE 802.3), HDLC, Frame Relay, PPP	Коммутатор локальной сети, беспроводная точка доступа, кабельный modem, modem DSL
Физический (1)	RJ-45, EIA/TIA-232, V.35, Ethernet (IEEE 802.3)	Концентратор LAN, повторитель LAN, кабеля

Кроме того, что на экзамене нужно четко представлять себе основные функции всех уровней модели OSI (см. табл. 2.4) и помнить примеры устройств и протоколов для каждого уровня (см. табл. 2.5), следует также запомнить названия всех уровней. Можно просто выписать их, но многие предпочитают использовать некоторые мнемонические правила, чтобы упростить запоминание. Мы предлагаем использовать одну из следующих ниже фраз, в которых первая буква слова соответствует англоязычному названию соответствующего уровня модели OSI. Уровни в такой схеме запоминания идут в правильном порядке, порядок следования указан в скобках.

- All People Seem To Need Data Processing⁶ (слева направо: с 7 по 1).
- Please Do Not Take Sausage Pizzas Away (слева направо: с 1 по 7).
- Pew! Dead Ninja Turtles Smell Particularly Awful (слева направо: с 1 по 7).

Концепции и преимущества многоуровневой структуры модели OSI

Хотя сетевые модели используют уровни, чтобы классифицировать сетевые функции и помочь людям понять их, для этого есть и другие причины. Рассмотрим, например, еще одну аналогию с почтой. Человек, пишущий письмо, может не думать о том, как почтовая служба доставит письмо через всю страну. Сотрудник почты, на полпути следования письма, может не задумываться о содержимом письма. Аналогично сетевые модели, которые делят функции на различные уровни, позволяют программным пакетам и аппаратным устройствам реализовать функции определенного уровня и подразумевать, что другое программное обеспечение и аппаратные средства выполняют функции, определенные другими уровнями.



Преимущества многоуровневых сетевых моделей

- **Упрощение решаемых задач.** Многоуровневая модель позволяет разделить задачу на меньшие и более простые этапы.
- **Стандартизация интерфейсов** взаимодействия уровней позволяет разным производителям создавать устройства, ориентированные на выполнение какой-либо определенной функции, а конкуренция в рамках открытых моделей ведет к значительному улучшению продукта.
- **Упрощение процесса обучения.** Людям намного проще изучать детали отдельных протоколов и уровней.
- **Упрощение процесса разработки новых устройств.** Чем проще продукты и устройства, тем проще и быстрее можно внести в них какие-либо изменения, а также разработать новые продукты.
- **Совместимость устройств разных производителей.** Если устройства отвечают одним и тем же стандартам, это означает, что компьютеры и сетевое оборудование от разных производителей будет работать корректно.

⁶ В переводе фразы не помогут запомнить названия и порядок следования уровней, следует запоминать их в английском варианте. Первая фраза: *всем людям, несомненно, нужна обработка данных*. Вторая фраза: *пожалуйста, не уносите с собой пиццу с сосисками*. Третья фраза: *Уф! Мертвые черепашки-ниндзя пахнут исключительно ужасно*. — Примеч. ред.

- Модульные разработки.** Один производитель может написать программное обеспечение, работающее на верхних уровнях, например веб-браузер компании Opera, а другой разработчик может написать программное обеспечение нижних уровней, например реализацию стека протоколов TCP/IP в операционной системе компании Microsoft, и в рамках стандартов программное обеспечение будет успешно работать с сетью.

Терминология инкапсуляции модели OSI

Подобно модели TCP/IP, модель OSI стандартизирует процесс получения служб верхними уровнями от нижних. Чтобы предоставить службы, каждый уровень использует заголовок, а возможно, и концевик. Нижние уровни модели инкапсируют данные верхних уровней в заголовок определенного формата. Последний раздел этой главы посвящен терминологии и концепциям инкапсуляции в модели OSI.

В модели TCP/IP используются такие термины, как *сегмент* (segment), *пакет* (packet) и *фрейм* (frame), для описания инкапсулированных данных разных уровней (см. Рис. 2.11). В модели OSI используется более общий термин — *блок данных протокола* (Protocol Data Unit — PDU).

Под блоком PDU понимают как биты заголовка и концевика соответствующего уровня, так и сами инкапсулированные данные. Например, пакет IP, который показан на рис. 2.10, согласно терминологии модели OSI, является блоком PDU. Зачастую говорят, что пакет IP является блоком PDU третьего уровня (сокращенно L3PDU), поскольку протокол IP относится к третьему уровню (Layer 3 — L3) модели OSI. Таким образом, вместо терминов *сегмент*, *пакет*, *фрейм* в модели OSI используется обозначение PDU уровня x (L_xPDU), где символом x обозначается обсуждаемый в данный момент уровень.

На рис. 2.14 показан типичный процесс инкапсуляции. Вверху показаны данные уровня приложений и его заголовок, в самом низу — блок L2PDU, который передается уже непосредственно в физический канал.

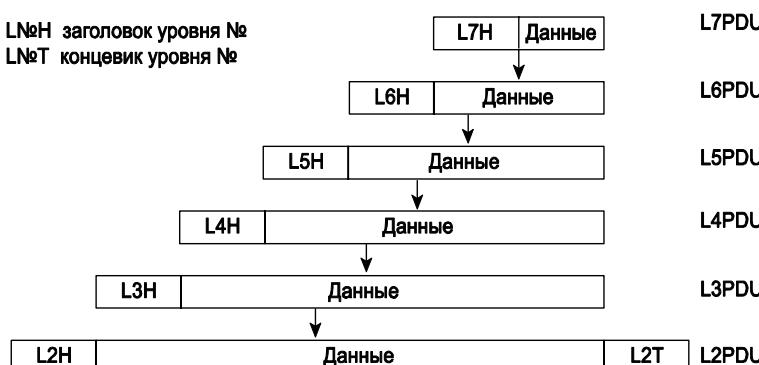


Рис. 2.14. Инкапсуляция и блоки PDU в модели OSI

Подготовка к экзамену

Повторите все ключевые темы

Повторите все ключевые темы данной главы, отмеченные пиктограммой “Ключевая тема”. Ключевые темы и соответствующие им страницы перечислены в табл. 2.6.

Таблица 2.6. Ключевые темы главы 2

Элемент	Описание	Страница
Табл. 2.3	Взаимодействие на смежных и равноправных уровнях	64
Рис. 2.8	Простой пример маршрутизации	68
Рис. 2.9	Для пересылки пакета IP маршрутизатору R1 Ларри использует Ethernet	69
Рис. 2.12	Блоки данных разных уровней и инкапсуляция	72
Рис. 2.13	Модель OSI по сравнению с двумя моделями TCP/IP	73
Список	Преимущества многоуровневых сетевых моделей	76

Заполните таблицы и списки по памяти

Распечатайте приложение М (Appendix L) с компакт-диска или его раздел, относящийся к этой главе, и заполните таблицы и списки по памяти. В приложении Н (Appendix M) приведены заполненные таблицы и списки для самоконтроля.

Ключевые термины

Дайте определения перечисленным ниже терминам и проверьте правильность их написания в списке терминов:

взаимодействие на смежных уровнях (adjacent-layer interaction), деинкапсуляция (decapsulation), инкапсуляция (encapsulation), фрейм (frame), сетевая модель (networking model), пакет (packet), блок данных протокола (Protocol Data Unit — PDU), взаимодействие на равноправном уровне (same-layer interaction), сегмент (segment).

Эталонная модель OSI

В табл. 2.7 перечислены все уровни модели OSI и кратко описаны функции каждого уровня. Эту таблицу нужно знать на память.

Таблица 2.7. Краткое описание модели OSI

Уровень	Функции
Приложений (7)	Является интерфейсом между сетевыми службами и приложениями. Отвечает также за аутентификацию пользователей
Представления (6)	Задает формат и организацию данных. Отвечает также за шифрование
Сеансовый (5)	Устанавливает и управляет сквозными сессиями между двумя конечными точками в сети. Включает в себя средства управления потоками данных

Окончание табл. 2.7

Уровень	Функции
Транспортный (4)	Предлагает множество методов взаимодействия двух компьютеров, в том числе процедуры установления и окончания соединения, контроль потоков данных, контроль и восстановление ошибок, сегментацию больших блоков данных на мелкие и др.
Сетевой (3)	Задает логическую адресацию в сети и отвечает за маршрутизацию
Канальный (2)	Создает фреймы из данных верхних уровней в формате, приемлемом для используемой физической среды. Задает также правила использования среды. Стандартизирует механизмы обнаружения ошибок передачи данных
Физический (1)	Задает электрические, оптические характеристики, стандартизирует кабели, разъемы и процедурные тонкости передачи битов, которые представляют собой некую форму энергии, передаваемой по физической среде

В этой главе...

- **Обзор современных локальных сетей Ethernet.** Кратко описаны перспективы использования технологии Ethernet в офисе или школе.
- **Краткая история технологии Ethernet.** Рассматриваются и сравниваются с современными некоторые устаревшие разновидности технологии Ethernet, а также описаны современные кабельные системы, их терминология и устройства.
- **Витая пара в сетях Ethernet.** Описаны различные типы кабелей и разъемов.
- **Использование коммутаторов вместо концентраторов для повышения производительности сети.** Подробно объясняется, какое влияние на производительность сети оказывает замена старых концентраторов Ethernet коммутаторами.
- **Средства канального уровня Ethernet.** Описаны поля в заголовках и концевиках фреймов Ethernet.

ГЛАВА 3

Основы сетей LAN

За счет взаимодействия стандартов физического и канального уровней компьютеры могут передавать друг другу биты через различные сетевые среды передачи данных. Физический (первый) уровень модели OSI определяет, как физически передаются биты через среду передачи данных. Канальный (второй) уровень определяет правила, используемые при физической передаче данных, например, правила адресации, которые указывают на отправителя и получателя информации, когда устройство может начинать передачу и когда необходимо отложить пересылку.

В этой главе описаны основы локальных сетей. Под термином *локальная сеть* обычно подразумевается набор стандартов первого и второго уровней модели OSI, используемых для взаимодействия устройств и обеспечения работы сети в географически ограниченном пространстве. В главе рассмотрены основные принципы работы локальных сетей, а именно локальных сетей Ethernet. Более детальная информация о локальных сетях приведена в части II книги (главы 7–11).

Контрольные вопросы: знаете ли вы уже темы главы

Этот раздел предназначен для того, чтобы читатель мог предварительно оценить свои знания и решить, нужно ли ему читать главу целиком. Если ответы на десять из одиннадцати вопросов даны правильно, можно сразу же перейти к последнему разделу “Подготовка к экзамену”. Основные темы этой главы и предварительных контрольных вопросов перечислены в табл. 3.1. Отвечая на контрольные вопросы и используя таблицу, читатель сможет достаточно точно определить свои знания в той или иной области. Ответы на вопросы приведены в приложении А.

Таблица 3.1. Темы контрольных вопросов

Основная тема	Номера вопросов
Обзор современных локальных сетей Ethernet	1
Краткая история технологии Ethernet	2
Витая пара в сетях Ethernet	3, 4
Использование коммутаторов вместо концентраторов для повышения производительности сети	5–7
Средства канального уровня Ethernet	8–11

1. Какое из перечисленных ниже утверждений наиболее верно описывает современные локальные сети Ethernet?
 - а) Каждое устройство подключается последовательно с использованием коаксиального кабеля.
 - б) Каждое устройство подключается последовательно с использованием неэкранированной витой пары.
 - в) Каждое устройство подключается к центральному концентратору локальной сети с использованием неэкранированной витой пары.
 - г) Каждое устройство подключается к центральному коммутатору локальной сети с использованием неэкранированной витой пары.
2. Какое из перечисленных ниже утверждений верно относительно кабельной системы локальной сети Ethernet на основе стандарта 10BASE2?
 - а) Каждое устройство подключается последовательно с использованием коаксиального кабеля.
 - б) Каждое устройство подключается последовательно с использованием неэкранированной витой пары.
 - в) Каждое устройство подключается к центральному концентратору локальной сети с использованием неэкранированной витой пары.
 - г) Каждое устройство подключается к центральному коммутатору локальной сети с использованием неэкранированной витой пары.
3. Какое из перечисленных ниже утверждений о перекрещенном (crossover) кабеле Ethernet верно?
 - а) Контакты 1 и 2 меняются местами на втором конце кабеля.
 - б) Контакты 1 и 2 на одном конце кабеля соединяются с контактами 3 и 6 на втором конце кабеля.
 - в) Контакты 1 и 2 на одном конце кабеля соединяются с контактами 3 и 4 на втором конце кабеля.
 - г) Длина кабеля может достигать 1000 метров в каналах между зданиями.
 - д) Ни один из указанных выше ответов не верен.
4. Каждый вариант ответа описывает два различных устройства в сети, соединяемых кабелем 100BASE-TX. Если эти устройства подключаются с помощью кабеля UTP, какие пары устройств требуют использования прямого кабеля? (Выберите три ответа.)
 - а) Персональный компьютер и маршрутизатор.
 - б) Персональный компьютер и коммутатор.
 - в) Коммутатор и концентратор.
 - г) Маршрутизатор и концентратор.
 - д) Беспроводная точка доступа (порт Ethernet) и коммутатор.

5. Какое из перечисленных ниже утверждений верно об алгоритме CSMA/CD?
 - а) Алгоритм предупреждает коллизии.
 - б) Коллизия может произойти, но алгоритм определяет процесс уведомления компьютеров о возникновении коллизии и восстановления после нее.
 - в) Алгоритм рассчитан только на два устройства в одном сегменте Ethernet.
 - г) Все перечисленные выше ответы ошибочны.
6. Какое из указанных ниже утверждений описывает домен коллизий?
 - а) Все устройства, подключенные к концентратору Ethernet.
 - б) Все устройства, подключенные к коммутатору Ethernet.
 - в) Два компьютера, один из которых подключен к порту Ethernet маршрутизатора с использованием перекрещенного кабеля, а второй подключен к другому порту Ethernet того же самого маршрутизатора с помощью перекрещенного кабеля.
 - г) Все перечисленные выше ответы ошибочны.
7. Что из перечисленного ниже является недостатком концентратора, который отсутствует в коммутаторе? (Выберите несколько ответов.)
 - а) Концентратор представляет собой единую электрическую шину, к которой подключаются все устройства, в результате полоса пропускания сети разделяется между устройствами в ней.
 - б) Концентраторы обеспечивают меньшую длину отдельных кабелей по сравнению с коммутатором.
 - в) При использовании концентраторов, если два устройства одновременно передают данные, возникает коллизия.
 - г) В концентраторе может быть не более восьми портов.
8. Какой из приведенных ниже терминов описывает адрес Ethernet, используемый для взаимодействия с более чем одним устройством в сети? (Выберите несколько ответов.)
 - а) Прошивочный адрес (burned-in).
 - б) Одноадресатный (unicast).
 - в) Широковещательный (broadcast).
 - г) Многоадресатный (multicast).
9. Что из перечисленного ниже является одной из функций протоколов канального уровня модели OSI?
 - а) Фреймирование.
 - б) Доставка битов от одного устройства к другому.
 - в) Коррекция ошибок.
 - г) Стандартизация размера и формы плат Ethernet.

10. Что из перечисленного ниже верно о формате адреса Ethernet? (Выберите три ответа.)
- а) Каждый производитель помещает уникальный код в первые 2 байта адреса.
 - б) Каждый производитель помещает уникальный код в первых 3 байта адреса.
 - в) Каждый производитель помещает уникальный код в первой половине адреса.
 - г) Часть адреса, содержащая код производителя платы, называется MAC.
 - д) Часть адреса, содержащая код производителя платы, называется OUI.
 - е) Часть адреса, содержащая код производителя платы, не имеет определенного названия.
11. Что из перечисленного ниже верно о поле контрольной суммы во фрейме Ethernet?
- а) Это поле используется для восстановления информации при ошибках.
 - б) Длина этого поля равна 2 байтам.
 - в) Это поле относится к концевику фрейма, а не заголовку.
 - г) Это поле используется для шифрования данных.
 - е) Все перечисленные выше ответы ошибочны.

Основные темы

Типичная корпоративная сеть состоит из множества площадок, соединенных между собой. Устройства конечных пользователей подключаются к локальной сети, позволяющей им обмениваться информацией. Кроме того, на каждой площадке сети находится маршрутизатор, используемый для подключения локальной сети к распределенной, которая обеспечивает передачу информации между разными площадками. Таким образом, с использованием маршрутизаторов и распределенной сети возможна передача информации между компьютерами, которые находятся в географически удаленных точках и зачастую далеко друг от друга.

В этой главе описано, как создать современную локальную сеть, а в главе 4 — как создаются распределенные сети. На текущий момент технология Ethernet является безоговорочным лидером среди стандартов локальных сетей, а другие, использовавшиеся в прошлом технологии построения локальных сетей, такие как среда Token Ring, интерфейс FDDI, уже практически не используются. Технология Ethernet победила в “соревновании стандартов”, и когда сегодня говорят о локальной сети, то никто и не задумывается о типе локальной сети, по сути подразумевая сеть Ethernet.

Обзор современных локальных сетей Ethernet

Ethernet — наиболее популярное во всем мире семейство стандартов для локальных сетей, которое охватывает физический и канальный уровень модели OSI. Стандарты Ethernet отличаются поддерживаемой скоростью; широко распространены на сегодняшний день скорости 10, 100 и 1000 Мбит/с (т.е. 1 Гбит/с). Различные варианты технологии также отличаются типом используемой среды передачи данных, например, в наиболее популярных стандартах Ethernet используется недорогой тип кабеля, а именно *незакрепленная витая пара* (Unshielded Twisted Pair — UTP), в то время как в других — более дорогой оптоволоконный кабель. Использование оптоволоконного кабеля оправдано в том случае, если нужно подключить устройства, которые находятся на большом расстоянии друг от друга, или в случае повышенных требований к безопасности сети. Для обеспечения различных потребностей при создании локальных сетей и были разработаны различные стандарты, работающие на разных скоростях, разном типе среды передачи данных (чем больше расстояние, тем дороже технология) и т.п.

Институт инженеров по электротехнике и электронике (IEEE) опубликовал множество стандартов Ethernet, после того, как в начале 1980-х он возглавил процесс стандартизации локальных сетей. Большинство стандартов по-разному реализовано на физическом уровне, работает с различными скоростями и типами кабелей. В стандартах IEEE канальный уровень разделен на два подуровня:

- IEEE 802.3 — подуровень контроля доступа к среде передачи данных (подуровень MAC);
- IEEE 802.2 — подуровень управления логическим каналом (подуровень LLC).

Фактически MAC-адрес получил свое название от названия нижнего подуровня канального уровня Ethernet.

Каждый новый стандарт физического уровня, публикуемый IEEE, содержит достаточно много отличий от предшествующих, но при этом использует тот же заголовок формата 802.3 и подуровень LLC в качестве верхнего уровня.

В табл. 3.2 перечислены наиболее часто используемые стандарты Ethernet IEEE для физического уровня.

Ключевая тема

Таблица 3.2. Наиболее распространенные разновидности технологии Ethernet

Общеизвестно е название	Скорость (Мбит/с)	Альтернативное название	Стандарт IEEE	Тип кабеля, максимальная длина (м)
Ethernet	10	10BASE-T	IEEE 802.3	Медный, 100
Fast Ethernet	100	100BASE-TX	IEEE 802.3u	Медный, 100
Gigabit Ethernet	1000	1000BASE-LX, 1000BASE-SX	IEEE 802.3z	Оптический, 550 для SX, 5000 для LX
Gigabit Ethernet	1000	1000BASE-T	IEEE 802.3ab	Медный, 100

Эта таблица достаточно простая, но все же некоторые термины требуют дополнительных пояснений. Во-первых, термин *Ethernet* часто используют в значении “любой тип технологии Ethernet”. (Чтобы избежать путаницы, в данной книге используется термин 10BASE-T для обозначения стандарта Ethernet со скоростью 10 Мбит/с в тех случаях, когда тип имеет значение.) Во-вторых, альтернативное название для каждого типа среды Ethernet содержит значение скорости (10, 100, 1000 Мбит/с), а буква “T” обозначает использование неэкранированной витой пары в качестве среды передачи данных (буква “T” имеется в словосочетании *twisted pair* — витая пара).

Для создания современной локальной сети с использованием неэкранированной витой пары необходимы следующие компоненты:

- компьютеры с установленными адаптерами (т.е. платами или сетевыми картами) Ethernet;
- концентратор или коммутатор Ethernet;
- кабель неэкранированной витой пары, соединяющий каждый компьютер с коммутатором или концентратором.

На рис. 3.1 показана схема типичной локальной сети. Здесь не показаны сетевые адAPTERы, поскольку они считаются частью компьютера или принтера, прямые линии соответствуют кабелям неэкранированной витой пары, а пиктограмма в центре — коммутатор Ethernet.

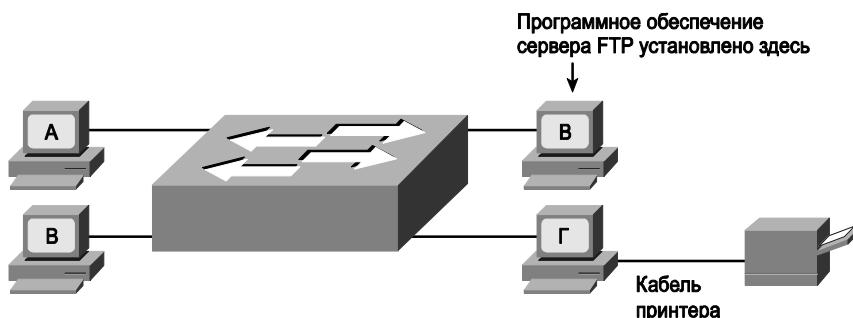


Рис. 3.1. Типичная небольшая современная локальная сеть

ВНИМАНИЕ!

Схема на рис. 3.1 подходит для любой из распространенных на сегодняшний день сетей Ethernet. Один и тот же базовый дизайн и топология используются вне зависимости от скорости передачи данных и типа кабелей.

Большинство пользователей могут создать локальную сеть, подобную той, которая показана на рисунке, при этом не имея даже базовых знаний о том, как работают локальные сети. Большинство персональных компьютеров поставляется с установленными в них адаптерами Ethernet. Коммутаторы не нужно настраивать для передачи информации между компьютерами. Все, что необходимо сделать, — подключить питание коммутатора и подсоединить к нему компьютеры с помощью кабелей неэкранированной витой пары; после этого компьютеры смогут пересыпать фреймы друг другу.

Даже без подключения к распределенной сети такие небольшие локальные сети являются неплохим решением с ограниченным масштабированием для нескольких типов задач, перечисленных ниже.

- **Совместный доступ к файлам.** На каждом компьютере можно настроить совместный доступ ко всей файловой системе или ее части, в результате с других компьютеров возможно чтение или запись файлов в такую систему. Данная функция обычно заложена в операционную систему.
- **Совместное использование принтера.** Компьютеры могут совместно использовать один принтер. Например, компьютеры А, Б, В (см. рис. 3.1) могут печатать документы на принтере, подключенном к компьютеру Г. Эта функция тоже обычно реализуется средствами операционной системы.
- **Передача файлов.** На компьютер можно установить сервер передачи файлов, что позволит соседним компьютерам принимать и пересыпать файлы на этот компьютер. Например, на компьютере В можно установить программное обеспечение сервера FTP (File Transfer Protocol — протокол передачи файлов), что позволит другим компьютерам с установленным клиентским программным обеспечением для протокола FTP подключаться к компьютеру В и передавать файлы.
- **Игры.** На компьютеры можно установить игровое программное обеспечение, и несколько игроков смогут играть в одну и ту же игру. Игровое ПО будет обмениваться информацией непосредственно по сети Ethernet.

Целью первой части главы было помочь читателю понять, что за простой локальной сетью (например, как на рис. 3.1) скрывается множество теоретических и практических знаний. Чтобы досконально разобраться в современных локальных сетях, будет полезно изучить историю технологий Ethernet, которая описывается в следующей части главы. После краткого экскурса в историю рассматриваются физические аспекты (первый уровень модели OSI) простой локальной сети на основе неэкранированной витой пары. Ниже в главе сравниваются прежние (и более медленные) *концентраторы* (hub) Ethernet и более новые устройства (и более быстрые) — *коммутаторы* (switch) Ethernet. В заключительной части главы описаны функции канального уровня (второй уровень модели OSI) в среде Ethernet.

Краткая история технологии Ethernet

Как и множество других ранних сетевых протоколов, протокол Ethernet начинал свое существование внутри корпораций, которые решали свои специфические задачи. Компании Xerox требовался эффективный способ, который позволил бы интегрировать в работу своих офисов новое изобретение — персональный компьютер. Этот момент и считается рождением протокола Ethernet. (На странице <http://inventors.about.com/library/weekly/aa111598.htm> размещен интересный рассказ о возникновении технологии Ethernet.) Чуть позже компания Xerox в сотрудничестве с компаниями Intel и DEC (Digital Equipment Corp.) продолжила разработку технологии, и сеть Ethernet стали называть технологией DIX Ethernet (DIX — первые буквы в названиях компаний DEC, Intel, Xerox).

Три компании в начале 1980-х охотно передали разработку стандартов Ethernet Институту инженеров по электротехнике и электронике (IEEE). Институт создал два комитета, которые работали (и работают по сей день) непосредственно над разработкой спецификаций Ethernet: комитет IEEE 802.3 и комитет IEEE 802.2. Комитет IEEE 802.3 работал над физическим уровнем стандарта и частью канального уровня, которая получила название *подуровень контроля доступа к среде передачи данных* (Media Access Control — MAC). Остальные функции канального уровня были переданы комитету IEEE 802.2, и эта часть канального уровня получила название *подуровень управления логическим каналом* (Logical Link Control — LLC). При этом стандарт 802.2 используется не только для технологии Ethernet, но и для других стандартов построения локальных сетей, таких как Token Ring.

Первые стандарты Ethernet: 10BASE2 и 10BASE5

Понять принципы работы технологии Ethernet проще на примере двух ранних спецификаций Ethernet: 10BASE5 и 10BASE2. Эти две спецификации определяют принципы работы физического и канального уровней первых сетей Ethernet. (Стандарты 10BASE2 и 10BASE5 отличаются характеристиками кабельной системы, но для простоты пока их можно считать идентичными.) Для построения сети с использованием одного из двух указанных стандартов используется коаксиальный кабель. Единый кабель, который образует шину, подводится к каждому устройству в сети, без использования концентраторов, коммутаторов или коммутационных панелей. Шина Ethernet совместно используется всеми устройствами. Когда устройству в сети Ethernet необходимо переслать несколько битов другому устройству, оно генерирует в коаксиальном кабеле сигнал, который доставляется ко всем устройствам, подключенным к шине.

На рис. 3.2 показан основной принцип работы сети Ethernet стандарта 10BASE2, в которой используется общая электрическая шина, созданная с использованием коаксиального кабеля и плат Ethernet компьютеров.

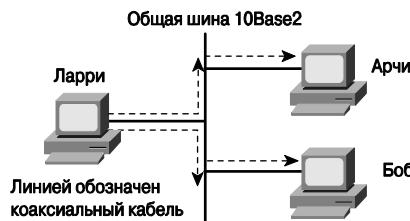


Рис. 3.2. Небольшая сеть Ethernet 10BASE2

Прямыми линиями на рис. 3.2 показаны коаксиальные кабели сети, пунктирными линиями показан маршрут передачи фрейма от компьютера Ларри. Сетевой адаптер компьютера Ларри генерирует электрический сигнал, а компьютеры Боба и Арчи принимают такой сигнал. Коаксиальные кабели образуют электрическую шину, поэтому передаваемый сигнал принимается всеми станциями в локальной сети.

Поскольку в сети используется общая шина, то если два или более электрических сигнала будут передаваться одновременно, они будут накладываться и “столкнуться” (коллизия) — исходные сигналы при наложении станут нераспознаваемыми. Вполне очевидно, что в стандарте Ethernet алгоритм работы сети разрешает только одному устройству одновременно пересыпать данные в сеть, иначе среди Ethernet нельзя было бы использовать для передачи данных. Такой алгоритм работы был назван *множественным доступом с контролем несущей и обнаружением коллизий* (Carrier Sense Multiple Access With Collision Detection — CSMA/CD), и именно он определяет, как осуществляется доступ к общейшине в среде Ethernet.

Аналогией в повседневной жизни алгоритму CSMA/CD может служить комната переговоров, в которой присутствует много человек. Тяжело разобрать, когда два человека говорят одновременно, следовательно, большую часть времени говорит кто-то один, а остальные слушают. Представьте себе, что и Боб, и Ларри одновременно хотят прокомментировать последнее высказывание рассказчика. Как только рассказчик делает паузу, Боб и Ларри одновременно пытаются что-то сказать. Если Ларри услышит голос Боба прежде, чем начать разговор, то он остановится и позволит Бобу высказаться. Если же они начнут говорить практически одновременно, перебивая друг друга, то никто не сможет понять, о чем они говорят. В обычной жизни традиционно говорят: “Извините, что я вас перебил”, — и замолкают. В итоге Ларри или Боб говорят по очереди. Или, возможно, другой человек берет слово и говорит о чем-то, в то время как Боб и Ларри уступают друг другу право высказаться. Такие правила основаны на общечеловеческой культуре; алгоритм CSMA/CD основывается на спецификациях технологии Ethernet, культурном багаже человечества и преследует те же цели.

Информацию об алгоритме CSMA/CD можно вкратце подытожить так.

Обобщение алгоритма CSMA/CD



- Устройство, которое хочет передать фрейм, ожидает отсутствия передачи в локальной сети. Другими словами, пересылка фрейма не выполняется до тех пор, пока присутствует электрический сигнал в общей шине.
- При возникновении коллизии (“столкновении” двух сигналов) устройства, которые создали коллизию, ожидают в течение случайного интервала времени, а затем пробуют повторить передачу.

В локальных сетях 10BASE5 и 10BASE2 коллизия возникает из-за того, что сигнал распространяется по всей протяженности шины. Когда две станции одновременно пересыпают информацию, два электрических сигнала накладываются, что приводит к коллизии. Следовательно, все устройства, использующие стандарт 10BASE5 или 10BASE2 технологии Ethernet, должны использовать алгоритм CSMA/CD для контроля коллизий.

Повторители

Как и любой другой стандарт локальной сети 10BASE5 и 10BASE2, Ethernet задает ограничение на общую длину кабеля. Максимальная длина сегмента для стандарта 10BASE5 равна 500 м, а для 10BASE2 — 185 м. Цифры 2 и 5 в спецификации стандарта соответствуют максимальной длине кабеля, где 2 соответствует 200 метрам, что очень близко к реальному значению в 185 метров.

В некоторых случаях максимальной длины кабеля недостаточно для подключения устройств. В таких случаях используется устройство, которое называется *повторителем* (repeater). Одна из причин, по которой ограничивается длина кабеля, заключается в том, что сигнал, переданный одним устройством, может очень сильно ослабнуть, затухнуть, если длина кабеля превышает 185 или 500 м. Затухание — процесс ослабления сигнала при прохождении через проводники; чем длиннее кабель, тем большее затухание испытывает сигнал. В качестве аналогии вспомним, что можно достаточно хорошо слышать человека, который находится недалеко, но если тот же человек говорит с той же громкостью издалека, то его речь разобрать очень трудно.

Повторители соединяют несколько кабельных сегментов, получают электрический сигнал из одного порта, интерпретируют биты как нули и единицы, а затем генерируют новый очищенный от шумов и усиленный сигнал в другие свои порты. Повторители не просто усиливают сигнал, потому что простое усиление сигнала также увеличит уровень шума, который бы появился при передаче сигнала через среду.

ВНИМАНИЕ!

Поскольку повторители не интерпретируют значение битов, а только детектируют и генерируют электрические сигналы, они относятся к первому уровню модели OSI.

Читателью, скорее всего, не понадобится создавать локальную сеть Ethernet на основе стандарта 10BASE5 или 10BASE2, но для понимания основ технологии все-таки следует выделить несколько ключевых моментов, прежде чем переходить к рассмотрению концепций построения современных локальных сетей.

- Первоначально сеть Ethernet представляла собой электрическую шину, к которой подключались все устройства.
- При использовании общей шины возникают коллизии, поэтому в технологии Ethernet используется алгоритм CSMA/CD, который определяет как метод предотвращения коллизий, так и действия, предпринимаемые в случае их возникновения.
- Повторители увеличивают длину сегментов локальной сети, очищая и регенерируя электрический сигнал без интерпретации его значения, т.е. работают на первом уровне модели OSI.

Построение сети 10BASE-T на концентраторах

IEEE не ограничивается только стандартами 10BASE2 и 10BASE5, он создает новые: в 1990 году вышел стандарт 10BASE-T, в 1995 году — 100BASE-TX, а в 1999 году — 1000BASE-T. Для обеспечения работы сетей в рамках новых стандартов создаются новые сетевые устройства: концентраторы и коммутаторы. В данном разделе описано, как работают эти три популярных типа сетей Ethernet, а также рассмотрены базовые принципы работы коммутаторов и концентраторов.

Стандарт 10BASE-T решает несколько проблем, присущих более ранним стандартам 10BASE2 и 10BASE5. Он позволяет использовать существующие кабели витой пары, используемые для телефонии. Даже при необходимости прокладки новых кабелей недорогой и легкий в прокладке кабель витой пары предпочтительнее старого, более дорогого и более сложного в установке коаксиального кабеля.

Еще одно важное преимущество, появившееся в стандарте 10BASE-T, которое и по сегодняшний день остается ключевым отличием новых локальных сетей, — это принцип подключения каждого устройства к централизованной точке. В первых реализациях 10BASE-T в качестве такой централизованной точки использовалось устройство, называемое концентратором Ethernet (рис. 3.3).

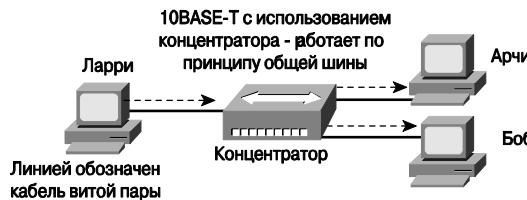


Рис. 3.3. Небольшая сеть Ethernet стандарта 10BASE-T с использованием концентратора

При построении современной локальной сети в качестве центрального устройства, к которому подключаются все остальные, может использоваться или концентратор, или коммутатор. Несмотря на то что в большинстве современных локальных сетей используется именно коммутатор, понимание принципов работы концентраторов позволяет лучше понять терминологию, используемую при описании работы коммутаторов, в том числе и их преимущества для локальных сетей.

Концентратор (hub) — это, по сути, многопортовый повторитель. Такое утверждение означает, что концентраторы просто повторяют электрический сигнал, который приходит на один порт через все другие порты. Работая таким образом, концентраторы фактически создают электрическую шину, в частности как в стандарте 10BASE2 или 10BASE5. Следовательно, в таких сетях возможно возникновение коллизий и необходимо использовать алгоритм CSMA/CD.

Сети стандарта 10BASE-T с использованием концентраторов решили несколько серьезных проблем, существовавших в сетях 10BASE2 и 10BASE5. Во-первых, существенно повысилась надежность работы сети. Повреждение одного кабеля или соединения могло привести и, как правило, приводило к неработоспособности всей сети на основе стандартов 10BASE2 и 10BASE5. В стандарте 10BASE-T устройства подключаются отдельными кабелями к концентратору, следовательно, проблема одного кабеля затрагивает только одно устройство. Как уже отмечалось выше, использование кабеля витой пары в звездообразной топологии (все кабели подключаются к центральному устройству) снижает стоимость самих кабелей и их прокладки.

В современных сетях, возможно, читатель встретит концентраторы, но предпочтительнее использовать вместо них коммутаторы. Коммутаторы работают много лучше, чем концентраторы, обеспечивают большую функциональность и, как правило, их стоимость не сильно превышает стоимость концентратора. Тем не менее все же следует отметить несколько ключевых принципов из истории технологии Ethernet, прежде чем переходить к вопросам, связанным с современными локальными сетями.

- Первоначально среда Ethernet представляла собой электрическую шину, к которой подключались все устройства.
- Повторители увеличивают длину сегментов локальной сети, очищая и регенерируя сигнал, без интерпретации значения электрического сигнала, т.е. работают на первом уровне модели OSI.
- Концентраторы — это повторители, которые обеспечивают централизованную точку включения кабелей витой пары, но все еще образуют общую электрическую шину, используемую различными устройствами, так же как в стандартах 10BASE2 и 10BASE5.
- Коллизии возникают в любом из указанных выше случаев, и в технологии Ethernet используется алгоритм CSMA/CD, который указывает устройствам, как избежать коллизий и какие действия предпринимать в случае их возникновения.

Ниже рассматривается использование кабелей неэкранированной витой пары — наиболее распространенной на сегодняшний день среды передачи данных.

Витая пара в сетях Ethernet

Три наиболее распространенных на сегодняшний день стандарта Ethernet — 10BASE-T (или просто Ethernet), 100BASE-TX (FastEthernet, или “быстрый” Ethernet), 1000BASE-T (Gigabit Ethernet, или гигабитовый Ethernet) — используют кабель неэкранированной витой пары. Кабели, используемые в стандартах, отличаются количеством используемых пар, категорией кабеля и некоторыми другими характеристиками. В этой части главы рассматриваются общие для всех трех стандартов параметры кабелей неэкранированной витой пары, в частности тип используемых разъемов, а также проводники для приема и передачи данных; здесь также описана схема расположения контактов разъема.

Кабель UTP и разъемы RJ-45

Кабель неэкранированной витой пары (UTP), который используется в популярных стандартах Ethernet, состоит из двух или четырех пар проводников. Проводники внутри кабеля тонкие и ломкие, поэтому они помещаются во внешнюю пластиковую оболочку. Каждый медный проводник имеет также собственную пластиковую оболочку, которая предохраняет его от переломов. Пластиковая оболочка разных проводников имеет разную цветовую маркировку, что позволяет легко идентифицировать проводники на концах кабеля. На конце кабеля, как правило, устанавливается специализированный разъем (обычно это разъем RJ-45), при этом концы проводников вставляются в специальные желобки разъема. В разъеме есть восемь контактов (pin), к которым подводятся отдельные проводники. Когда на конец кабеля устанавливается стандартный разъем, концы проводников должны подключаться в правильном порядке.

ВНИМАНИЕ!

Если у читателя есть под рукой кабель неэкранированной витой пары с установленным разъемом, он может прямо сейчас тщательно осмотреть его и записать порядок подключения проводников.

Когда на каждом конце кабеля установлен разъем, его включают в гнездо стандарта RJ-45, которое часто называют портом RJ-45. На рис. 3.4 показаны кабели разъемов и портов.

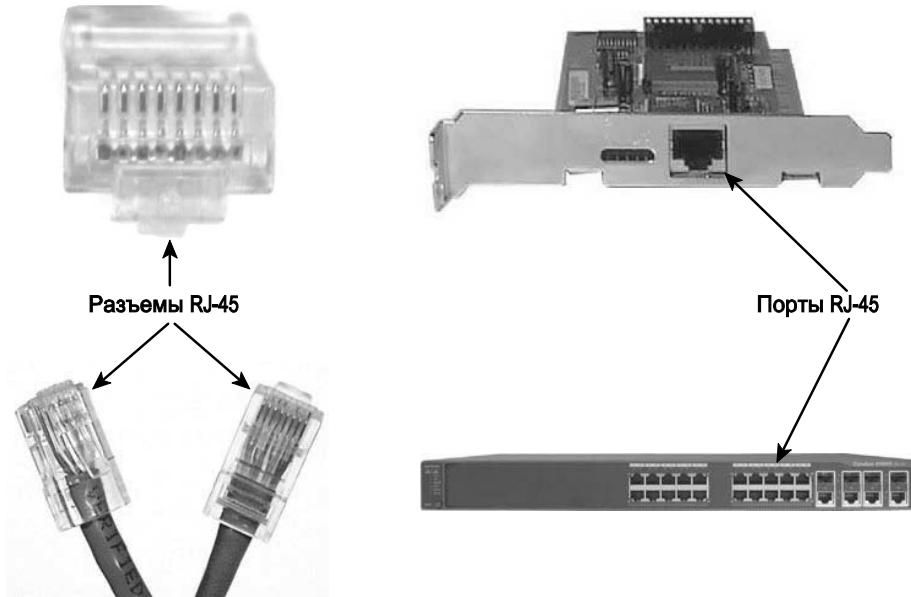


Рис. 3.4. Разъемы и гнезда RJ-45

ВНИМАНИЕ!

Разъем RJ-45 чуть шире, но в остальном похож на разъем RJ-11, который часто используется для телефонных кабелей.

На рис. 3.4, слева, показан разъем RJ-45 в трех разных положениях. В верхнем левом углу показан вид разъема с торца, на котором можно увидеть проводники кабеля, зафиксированные контактами разъема. Справа вверху показан не установленный в компьютер адаптер Ethernet. Порт RJ-45 сетевого адаптера после установки в компьютер будет находиться на задней панели в легкодоступном для подключения кабеля месте. Снизу справа показан коммутатор Catalyst 2960 компании Cisco со множеством портов RJ-45, через которые можно подключить к сети несколько устройств.

Несмотря на то что разъемы стандарта RJ-45 распространены, зачастую у сетевых инженеров возникает необходимость в замене нескольких физических портов без замены всего коммутатора. Многие коммутаторы компании Cisco имеют несколько заменяемых портов, выполненных или в виде разъемов *гигабитового конвертора интерфейса* (Gigabit Interface Convertor — GBIC), или *малоформатного модульного разъема* (SFP — Small-Form Pluggables). Оба разъема используются для установки заменяемых модулей для любого из стандартов сети Ethernet. Просто установив другой тип модуля GBIC или SFP, коммутатор можно использовать для подключения других типов кабелей и разъемов. На рис. 3.5 показана установка модуля GBIC стандарта 1000BASE-T.

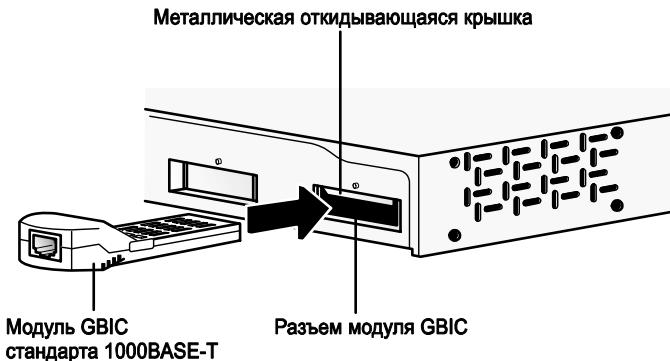


Рис. 3.5. Модуль GBIC стандарта 1000BASE-T с разъемом RJ-45

Если сетевому инженеру понадобится использовать существующий коммутатор в другой роли в локальной сети, он может просто приобрести новый модуль GBIC 1000BASE-LX, заменить старый стандарта 1000BASE-T и не приобретать полностью новый коммутатор. Например, когда коммутатор используется только для подключения устройств и других коммутаторов в том же здании, в нем может использоваться модуль GBIC 1000BASE-T и медные кабели. Если же компания переедет в другое здание, коммутатор может быть переоснащен другим модулем для подключения оптоволоконного канала, который работает на больших расстояниях в стандарте 1000BASE-LX.

Передача данных по витой паре

Кабель неэкранированной витой пары состоит из спаренных и свитых между собой проводников, что и дало название этому типу кабеля *витая пара* (twisted pair). Устройства на концах кабеля создают замкнутую электрическую цепь за счет пары проводников и передачи по ним электрического тока. При этом электрический ток в одной паре проводников течет в разных направлениях по каждому из проводов. Когда ток протекает через любой проводник, вокруг него образуется электромагнитное поле, которое может вызывать наводки на других проводниках в кабеле. Из-за того что проводники в одной паре перевиты и ток в них течет в противоположных направлениях, электромагнитное поле, созданное вторым проводником пары, почти полностью подавляется. Данный эффект используется в большинстве сетевых кабелей на основе медных проводников.

Для передачи данных с помощью электрического тока, генерируемого в паре проводников устройства, используют *схемы кодирования* (encoding scheme), в которых указано, каким должен быть электрический сигнал, чтобы передавать двоичные 0 или 1. Например, в стандарте 10BASE-T используется схема кодирования, в которой битовому 0 соответствует переход сигнала с высокого уровня напряжения на низкий. Электротехнические подробности механизмов кодирования несущественны в рамках данной книги, но важно понимать, что сетевые устройства создают электрический ток, используя сразу пару проводников и определенную схему кодирования для передачи битов.

Схема расположения контактов кабеля UTP для стандартов 10BASE-T и 100BASE-TX

Проводники кабеля витой пары должны быть подключены к правильным контактам разъема RJ-45. Как упоминалось выше, разъем RJ-45 содержит восемь контактов (pin), к которым подключаются медные проводники. Схема подключения контактов — это соответствие проводника определенного цвета в кабеле контакту в разъеме, она должна удовлетворять определенным требованиям стандарта Ethernet, описанным в этой части главы.

Интересный факт: IEEE официально не указал стандарты для кабелей, разъемов и точную схему подключения контактов в разъеме. Ассоциация телекоммуникационной промышленности (Telecommunication Industry Association — TIA) определяет стандарт для кабельной системы на основе витой пары, цветовой схемы проводников и стандартную схему подключения контактов (см. <http://www.tiaonline.org>). На рис. 3.6 показаны две разработанные организациями TIA стандартные схемы подключения проводников с указанием цветов и номеров пар.

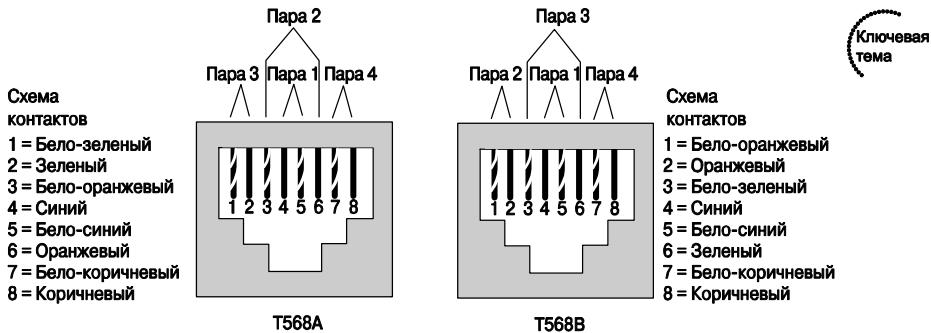


Рис. 3.6. Стандартные схемы расположения выводов кабелей TIA

Обратите внимание на то, что в кабеле неэкранированной витой пары используются четыре цвета для маркировки проводников (оранжевый, зеленый, синий, коричневый) в виде сплошной или чередующейся с белыми полосами окраски. Кабели одной пары свитых проводников имеют один цвет и отличаются методом окраски (сплошная или полосатая), при этом кабели полосатой окраски обычно называют с указанием белого цвета и основного, например бело-оранжевый.

ВНИМАНИЕ!

В кабеле неэкранированной витой пары используются две пары проводников в стандартах 10BASE-T и 100BASE-TX и четыре пары проводников в стандартах 1000BASE-T. В данной части рассматривается двухпарное подключение кабеля, а четырехпарное рассматривается ниже.

Для построения рабочей сети Ethernet необходимо выбирать кабели с правильным подключением контактов на концах кабеля. В стандартах 10BASE-T и 100BASE-TX указано, что одна пара проводников используется для передачи данных в одном направлении, а вторая пара — в обратном направлении. В частности, сетевой адаптер среды Ethernet пересыпает данные, используя контакты 1 и 2, или третью пару, согласно спецификации T568A (см. рис. 3.6). Одновременно сетевой адаптер ожидает входя-

щие данные на контактах 3 и 6 — пара 2 по спецификации T568A. В концентраторах и коммутаторах, соответственно, пары используются наоборот: прием данных осуществляется на контактах 1 и 2, а передача — на контактах 3 и 6.

На рис. 3.7 показано подключение компьютера Ларри к концентратору. Обратите внимание на то, что на рисунке показаны две пары свитых кабелей внутри кабеля, чтобы подчеркнуть, что в кабеле используются только эти две пары.

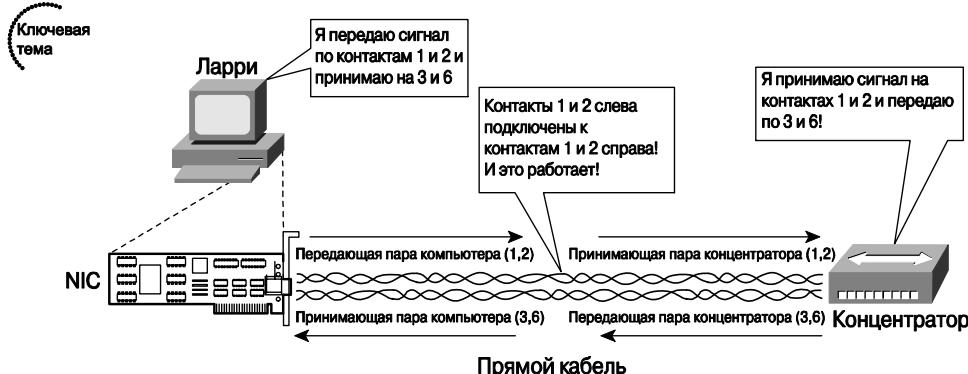


Рис. 3.7. Принцип работы прямого кабеля

В схеме на рис. 3.7 используется *прямой* (straight-through) тип кабеля. В прямом типе кабеля контакт 1 одного конца подключается к контакту 1 противоположного, контакт 2 — к контакту 2, контакт 3 — к контакту 3 и т.д. (При этом на обоих концах кабеля используется одна и та же спецификация EIA/TIA.)

Прямой кабель применяется в тех случаях, когда устройства на его противоположных концах используют разные номера контактов для приема и передачи информации. Для подключения друг к другу устройств, использующих одинаковые номера контактов для приема и одинаковые номера контактов для передачи, в самом кабеле необходимо поменять местами пары проводников. Такой кабель называется *перекрещенным* (crossover). Например, в большой корпоративной сети используется несколько коммутаторов, соединенных кабелем неэкранированной витой пары. Поскольку все коммутаторы передают данные на контактах 3 и 6, а принимают по контактам 1 и 2, в кабеле необходимо поменять эти пары проводников местами. На рис. 3.8 показана принципиальная схема расположения контактов перекрещенного кабеля.

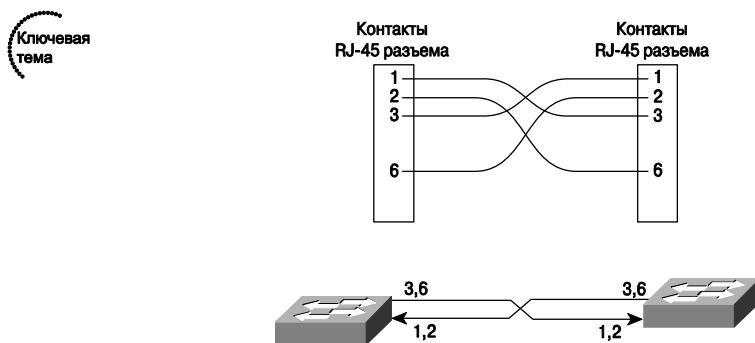


Рис. 3.8. Перекрещенный кабель

В верхней части рисунка показаны контакты с подключенными проводниками. Проводник, подключенный к первому контакту разъема слева, подключается к третьему контакту разъема справа, второй слева — к шестому контакту справа, третий контакт слева — к первому справа, шестой слева — ко второму контакту справа. В нижней части рисунка показана пара, подключенная к передающим контактам 3 и 6 коммутатора слева, которая подключается к принимающим контактам 1 и 2 коммутатора справа, и наоборот.

Для уверенной сдачи экзамена необходимо правильно выбирать тип кабеля (прямой или перекрещенный) для подключения различных устройств. Можно запомнить такую краткую схему: если устройства на разных концах кабеля передают сигнал по одной и той же паре, то необходим перекрещенный кабель; если по разным — то прямой. В табл. 3.3 приведены устройства, которые упоминаются в книге, и номера пар контактов, которые используются для передачи при использовании стандартов 10BASE-T и 100BASE-TX.

Таблица 3.3. Использование контактов в стандартах 10BASE-T и 100BASE-TX



Устройства, которые передают по паре 1,2 и принимают по паре 3,6	Устройства, которые передают по паре 3,6 и принимают по паре 1,2
Сетевые адAPTERы персонального компьютера	Концентраторы
Маршрутизаторы	Коммутаторы
Беспроводные точки доступа (интерфейс Ethernet)	—
Сетевые принтеры (которые непосредственно подключаются к сети Ethernet)	—

Например, на рис. 3.9 показана схема локальной сети одного здания. Несколько прямых кабелей используется для подключения персональных компьютеров к коммутаторам, а для соединения коммутаторов используются перекрещенные кабели.

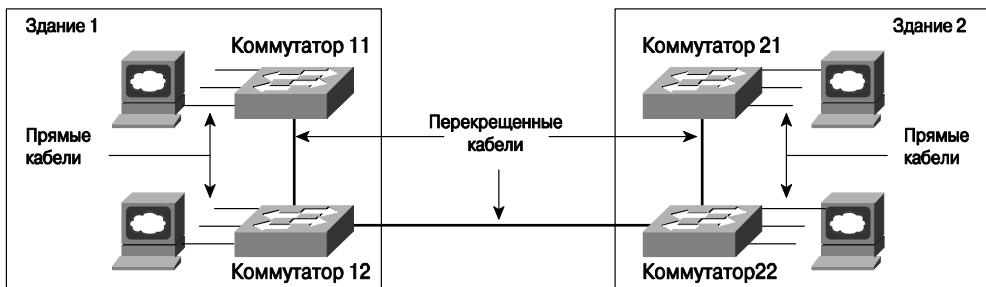


Рис. 3.9. Использование прямых и перекрещенных кабелей

Кабели стандарта 1000BASE-T

Как упоминалось выше, стандарт 1000BASE-T отличается от других по требованиям к кабелю и назначением контактов. Во-первых, в стандарте используются все четыре пары проводников, во-вторых, гигабитовая технология Ethernet позволяет принимать и передавать данные одновременно по всем четырем парам.

Тем не менее в гигабитовой технологии Ethernet присутствуют такие понятия, как прямой и перекрещенный кабель, но с небольшими отличиями от более ранних стандартов. Схема подключения для прямого кабеля точно такая же: первый контакт разъема подключается к первому, второй — ко второму и т.д. В перекрещенном кабеле точно так же меняются местами пары на контактах 1,2 и 3,6, но кроме этого также меняются местами две другие пары — на контактах 4,5 и 7,8.

ВНИМАНИЕ!

Если у читателя есть некоторый опыт в создании локальных сетей, может возникнуть мысль, что он где-то использовал неправильный кабель, но сеть все же работала. В коммутаторах компании Cisco реализована функция *автоопределения типа кабеля* (auto-mdix), за счет которой устройство само обнаруживает, какой тип кабеля включен в порт. Эта функция перенастраивает коммутирующие микросхемы под установленный кабель. Для сдачи экзамена необходимо идентифицировать правильный тип кабеля так, как показано на рис. 3.9.

Использование коммутаторов вместо концентраторов для повышения производительности сети

В этом разделе описаны некоторые проблемы с производительностью сети, построенной на концентраторах, и показано, как коммутаторы помогают решить две наиболее существенные проблемы концентраторов. Для лучшего понимания проблемы обратимся к рис. 3.10, на котором показано, что происходит, когда одно устройство пересыпает данные через концентратор.

ВНИМАНИЕ!

Схема и принцип работы на рисунке применимы как для стандарта 10BASE-T, так и для технологий 100BASE-TX и даже для 1000BASE-T.

На рис. 3.10 видно, что концентратор создает общую электрическую шину. Этапы работы устройства описаны ниже.

- Этап 1** Сетевой адаптер пересыпает фрейм.
- Этап 2** Сетевой адаптер через внутреннюю петлю осуществляет передачу фрейма на пару для приема данных.
- Этап 3** Концентратор принимает электрический сигнал и распознает его как последовательность битов.
- Этап 4** Концентратор повторяет полученную последовательность битов на всех портах, кроме того, с которого был получен фрейм.
- Этап 5** Концентратор повторяет сигнал на принимающих парах для всех устройств в соответствующих портах.

Обратите внимание: концентратор всегда повторяет электрический сигнал на всех портах, кроме того, с которого этот сигнал был получен. Так же на рис. 3.10 не показаны коллизии, однако если компьютер 1 и компьютер 2 начнут передавать сигнал одновременно, то на 4 этапе два сигнала перекроются, фреймы попадут в коллизию и их невозможно будет распознать или фреймы будут содержать большое количество ошибок.

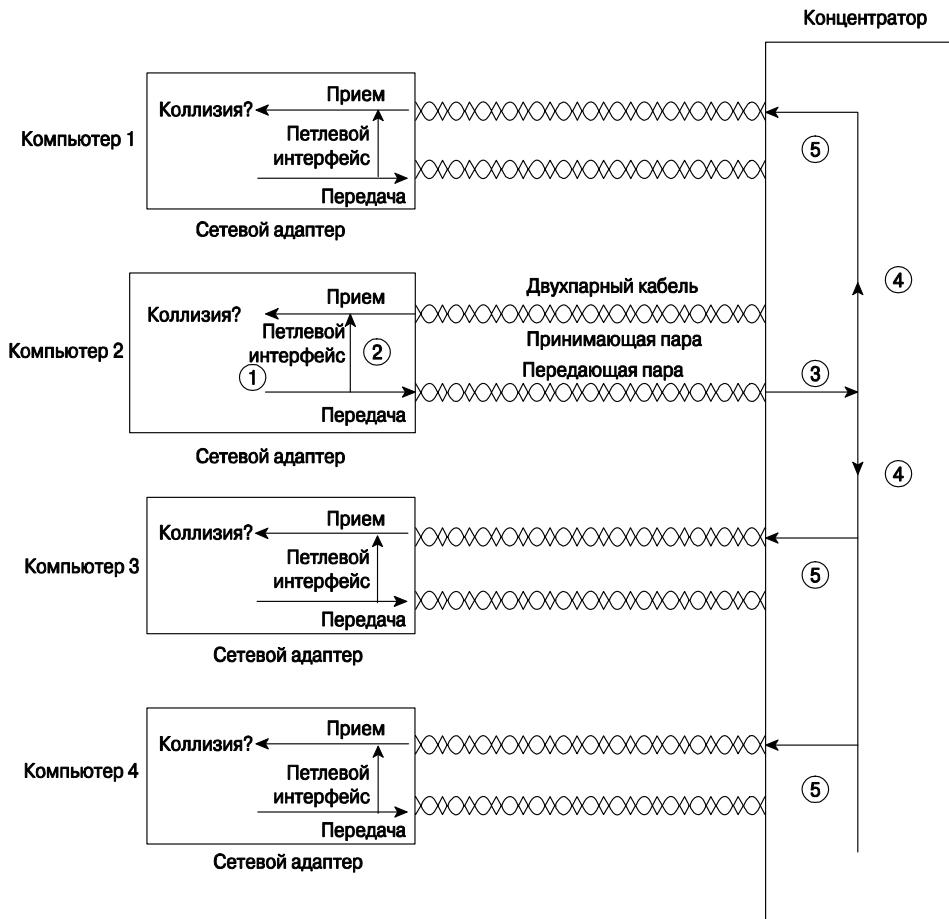


Рис. 3.10. Концентратор образует общую электрическую шину

Алгоритм CSMA/CD

Ключевая тема

Алгоритм CSMA/CD позволяет предотвратить коллизии и задает порядок действий при их возникновении, этапы которого описаны ниже.

- Этап 1** Устройство, пересылающее фрейм, ожидает, пока не освободится среда Ethernet.
- Этап 2** Когда среда Ethernet свободна, отправитель (или отправители) начинает отправку фрейма.
- Этап 3** Отправитель (или отправители) прослушивает среду на предмет возникновения коллизии.
- Этап 4** Если происходит коллизия, устройства, которые отправляли фреймы, генерируют сигнал оповещения о коллизии (jamming signal), чтобы все станции были уведомлены о возникновении коллизии.
- Этап 5** После получения сигнала о коллизии каждый отправитель ожидает в течение случайного интервала времени, прежде чем начать повторную попытку передачи попавшего в коллизию фрейма.
- Этап 6** Когда истекает случайный интервал, процесс начинается с этапа 1.

Алгоритм CSMA/CD не предотвращает коллизии полностью, но позволяет продолжить работу даже в случае их возникновения. Когда происходит коллизия, алгоритм CSMA/CD обязывает устройства, вовлеченные в коллизию, отложить передачу данных на случайный интервал, а затем повторить попытку. Такой подход позволяет локальной сети функционировать, но негативно сказывается на ее производительности. Следует запомнить два ключевых момента. Во-первых, алгоритм CSMA/CD обязывает устройства ожидать освобождения среды передачи, прежде чем начать передачу. Такое требование помогает избежать коллизий, но также означает, что в каждый момент времени вести передачу информации может только одно устройство. В результате устройства, подключенные к одному концентратору, делят между собой общую полосу пропускания. Режим работы, в котором передача возможна только при отсутствии сигнала на принимающей паре, называется *полудуплексным* (half duplex). Такое утверждение, по сути, означает, что устройство может только или принимать, или передавать фрейм в каждый произвольный момент времени.

Вторая основная особенность алгоритма CSMA/CD — это метод обработки коллизий. Когда происходит коллизия, алгоритм обязывает вовлеченные в нее устройства отложить передачу на случайный период времени. Такое требование позволяет работать локальной сети, но в то же время понижает ее производительность. Во время коллизии полезные данные не передаются через сеть, кроме того, устройства, ожидающие истечения случайного интервала, дольше ожидают возможности повторной передачи, чем в среде без коллизий. Следует отметить, что при увеличении нагрузки на сеть Ethernet увеличивается вероятность возникновения коллизий. До тех пор, пока коммутаторы не стали доступными и не решили многие проблемы с производительностью, выработалось правило, что производительность сети Ethernet начинает ухудшаться при загрузке выше 30%, преимущественно за счет увеличения числа коллизий.

Увеличение производительности сети с помощью коммутаторов

Термином *домен коллизий* (collision domain) описывают набор устройств, фреймы которых могут создать коллизию. Все устройства в сетях 10BASE2, 10BASE5 или любой сети с концентраторами могут испытывать коллизии, следовательно, все устройства в таких сетях находятся в одном домене коллизий. Например, все устройства, подключенные к концентратору (рис. 3.10), находятся в одном домене коллизий. Для избежания коллизий и их обработки в таких сетях используется алгоритм CSMA/CD.

Коммутаторы для локальных сетей значительно сокращают или даже полностью устраниют коллизии в сети. В отличие от концентраторов, коммутаторы не образуют общую электрическую шину и пересыпают полученный сигнал на все свои порты. Они работают следующим образом:

- коммутаторы интерпретируют последовательность битов как фрейм и в большинстве случаев пересыпают такой фрейм только на один порт, а не на все;
- если коммутатору необходимо переслать больше чем один фрейм на один и тот же порт, он буферизирует фреймы в памяти и пересыпает их последовательно один за другим, что позволяет избежать коллизий.

Например, на рис. 3.11 показано, как коммутатор пересыпает два фрейма одновременно, не создавая при этом коллизию. На этом рисунке компьютер 1 и компью-

тер 3 одновременно передают фреймы. Компьютер 1 отправляет фрейм с адресом получателя, соответствующим адресу компьютера 2, а компьютер 3 — с адресом получателя, соответствующим адресу компьютера 4, в заголовках фрейма. (Более подробно об адресации в сети Ethernet рассказано далее в главе.) Коммутатор проверяет адрес получателя в заголовке фрейма Ethernet и пересыпает фрейм от компьютера 1 компьютеру 2 и одновременно пересыпает фрейм от компьютера 3 компьютеру 4. Если в сети используется концентратор, то в такой ситуации возникает коллизия, но поскольку коммутатор не пересыпает фрейм через все свои порты, он позволяет избежать столкновения.

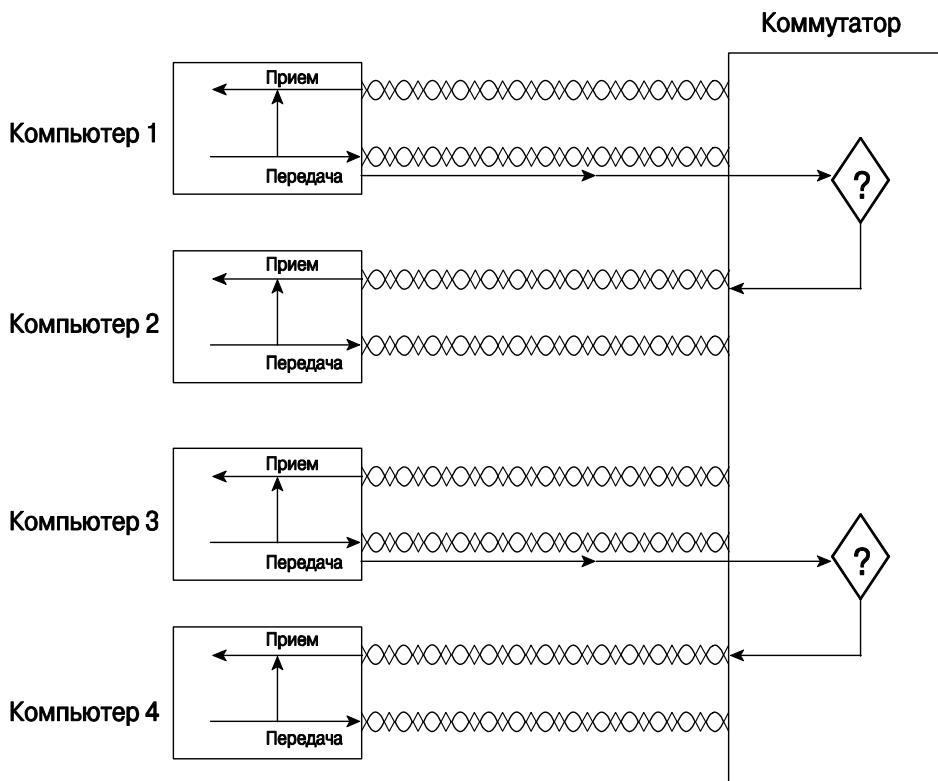


Рис. 3.11. Принцип работы коммутатора

ВНИМАНИЕ!

Коммутатор использует информацию из заголовка фрейма Ethernet, т.е. выполняет функцию второго уровня модели OSI, следовательно, коммутатор считается устройством второго уровня, в то время как концентратор относится к первому уровню модели OSI.

Буферизация также позволяет избежать коллизий. Представьте, что компьютеры 1 и 3 одновременно пересыпают фреймы компьютеру 4. Коммутатор знает, что одновременная передача этих фреймов приведет к коллизии, буферизирует один из них (другими словами, временно сохраняет его в памяти устройства) до тех пор, пока второй не будет целиком отправлен компьютеру 4.

Описанные выше принципы работы коммутаторов позволяют существенно повысить производительность сети по сравнению с концентраторами за счет следующих особенностей:

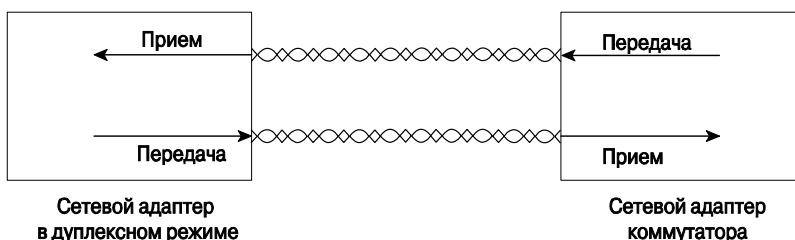
- если каждое устройство подключено к отдельному порту коммутатора, то коллизии не возникают;
- устройства, подключенные к одному порту коммутатора, не делят полосу пропускания с устройствами, подключенными к другим портам. Каждое устройство использует выделенную полосу пропускания, на практике коммутатор на 100 Мбит/с обеспечивает около 100 Мбит/с полосы пропускания на каждый порт.

Второе утверждение относится к понятиям совместно используемой среды Ethernet и коммутируемой среды Ethernet. Как уже упоминалось выше, совместно используемая среда Ethernet подразумевает, что полоса пропускания локальной сети делится между всеми устройствами, потому что они должны ожидать освобождения общей шины, прежде чем начать передачу информации. Термин *коммутируемая среда Ethernet* подчеркивает тот факт, что при использовании коммутаторов полоса пропускания не делится между устройствами, что приводит к значительному увеличению производительности сети. Например, концентратор, к которому подключено двадцать четыре устройства, на скорости 100 Мбит/с обеспечивает теоретически до 100 Мбит/с полосы пропускания в общем. При использовании коммутатора вместо концентратора обеспечивается до 100 Мбит/с на каждый порт, что в сумме дает до 2,4 Гбит/с полосы пропускания.

Увеличение вдвое производительности при использовании дуплексного режима

Любая сеть Ethernet на концентраторах требует использования алгоритма CSMA/CD для корректной работы. Этот алгоритм требует полудуплексного режима работы, и соответственно только одно устройство может передавать информацию в каждый момент времени. Поскольку коммутаторы буферизируют фреймы в памяти, они могут полностью исключить коллизии в своих портах для одного устройства. В результате коммутаторы с единственным подключенным к порту устройством могут работать в **дуплексном (full-duplex) режиме**. Дуплексный режим означает, что сетевой адаптер может одновременно и принимать, и передавать информацию.

На рис. 3.12 показано, почему нет коллизии в дуплексном режиме и как обеспечивается дуплексное подключение единственного компьютера к порту коммутатора.



Rис. 3.12. Дуплексный режим работы коммутатора

Коллизия не может произойти между коммутатором и компьютером в ситуации, показанной на рис. 3.12. Когда используется дуплексный режим работы, в портах фактически отключается алгоритм CSMA/CD на обоих концах кабеля; ни одно устройство не ожидает отсутствия сигнала в принимающей паре перед передачей данных. В результате такого подхода производительность сегмента Ethernet удваивается за счет одновременного обмена информацией в обоих направлениях.

Резюме: первый уровень технологии Ethernet

Выше были рассмотрены принципы работы и методы построения сети Ethernet с использованием концентраторов и коммутаторов в рамках первого уровня модели OSI и правила использования кабелей витой пары при подключении устройств к коммутаторам или концентраторам. Была описана обобщенная теория передачи информации устройствами — передача данных с помощью электрических сигналов через электрические цепи, образованные парой проводников в кабеле. Важной информацией является также описание того, какие пары проводников используются для приема и передачи информации, а также принцип работы коммутаторов, методы устранения коллизий в них, которые существенно повышают производительность по сравнению с концентраторами.

Средства канального уровня Ethernet

Одним из наиболее важных преимуществ семейства протоколов Ethernet является то, что в них используется один и тот же стандарт канального уровня. Адресация в протоколах Ethernet не менялась начиная со стандарта 10BASE5 и заканчивая наиболее современными реализациями 10-гигабитовой среды Ethernet, включая те, которые используют отличную от медной среду передачи данных. Больше того, алгоритм CSMA/CD, который, по сути, является частью канального уровня, точно так же может использоваться во всех стандартах.

Эта часть главы посвящена канальным протоколам технологии Ethernet, в частности, адресации в среде Ethernet, принципам формирования фреймов, методам определения ошибок и идентификации типов данных во фрейме Ethernet.

Адресация в технологии Ethernet

Механизм адресации в технологии Ethernet позволяет адресовать не только отдельные устройства, но и группу узлов в локальной сети. Адрес состоит из 6 байтов и обычно записывается в шестнадцатеричном виде (в устройствах компании Cisco такой адрес, как правило, записывается с точкой в качестве разделителя набора из четырех шестнадцатеричных цифр, например 0000.0C12.3456).

Одноадресатный (unicast) адрес Ethernet идентифицирует один сетевой адаптер. (Термин одноадресатный выбран в основном для противопоставления таким понятиям, как широковещательный (broadcast) и многоадресатный (multicast) адрес.) Компьютеры используют одноадресатный идентификатор, чтобы указать отправителя и получателя фрейма Ethernet. Например, представьте себе ситуацию, когда Фред и Барни находятся в одном сегменте сети Ethernet, и компьютер Фреда пересыпает компьютеру Барни фрейм. Компьютер Фреда помещает собственный MAC-адрес Ethernet в заголовок фрейма в качестве отправителя и использует MAC-адрес компьютера Барни в качестве адреса получателя. Когда компьютер Барни получает

фрейм, он определяет, что адрес получателя фрейма — это его собственный адрес, и начинает обработку фрейма. Если компьютер Барни получает фрейм с одноадресатным адресом какого-либо другого устройства в качестве получателя, он просто игнорирует этот фрейм.

IEEE стандартизировал формат и способ назначения адресов локальной сети. Стандарт требует глобальной уникальности одноадресатных MAC-адресов во всех сетевых платах. (IEEE использует название MAC-адреса, потому что протоколы уровня MAC, такие как IEEE 802.3, указывают механизмы адресации.) Чтобы добиться уникальности адресов, производители сетевых адаптеров прописывают их непосредственно в самих адаптерах (сетевых платах), обычно в микросхеме ПЗУ. Первая половина адреса идентифицирует производителя сетевого адаптера — эта часть адреса назначается IEEE каждому производителю и называется OUI (Organizationally Unique Identifier — уникальный идентификатор организации). Каждый производитель при назначении MAC-адреса сетевому адаптеру использует свой идентификатор OUI в первой части адреса и уникальный, ранее нигде не использовавшийся номер, для второй части (рис. 3.13).

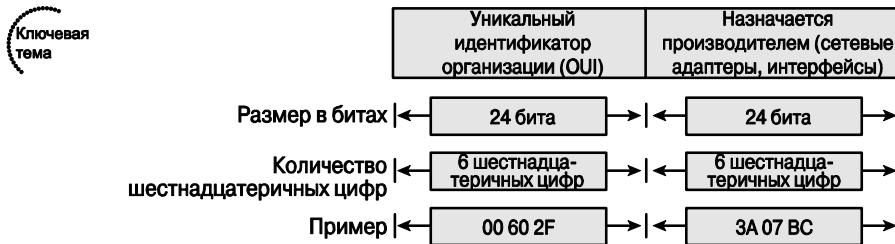


Рис. 3.13. Структура одноадресатного адреса Ethernet

Для описания одноадресатного адреса в локальной сети используется множество терминов. Зачастую говорят, что каждый сетевой адаптер поставляется с *прошитым адресом* (Burned-In Address — BIA), который записывается в микросхему ПЗУ на плате. Прошигтый адрес иногда называют *универсально управляемым адресом* (Universally Administered Address — UAA), потому что IEEE управляет назначением адресов во всем мире. Вне зависимости от того, используется ли прошигтый адрес или настроен другой адрес, множество людей воспринимают такой одноадресатный адрес как адрес локальной сети, или адрес Ethernet, или аппаратный адрес, или физический адрес, или MAC-адрес.

Кроме одноадресатных, существуют другие адреса, которые идентифицируют более одного сетевого адаптера. IEEE разделяет такие адреса на две группы, указанные ниже.

- *Широковещательный адрес* (broadcast addresses). Наиболее часто используемый групповой адрес, значение которого равно FFFF.FFFF.FFFF (в шестнадцатеричном виде). Широковещательный адрес используется в тех случаях, когда все устройства в локальной сети должны обработать фрейм.
- *Многоадресатный адрес* (multicast addresses) используется для взаимодействия с определенной группой устройств в локальной сети. Когда групповой пакет IP распространяется в среде Ethernet, используется специализированный групповой MAC-адрес в формате 0100.5exx.xxxx. Во второй половине адреса может использоваться любое значение.

В табл. 3.4 приведено резюме по разновидностям MAC-адресов.

Таблица 3.4. Терминология и функции MAC-адресов в локальной сети



Термин или функция	Описание
MAC-адрес	<i>Контроль доступа к среде передачи</i> (Media Access Control). Стандарт IEEE 802.3 (Ethernet) описывает подуровень MAC среды Ethernet
Адрес Ethernet, адрес сетевой платы, адрес локальной сети	Другие названия, часто используемые вместо термина <i>MAC-адрес</i> . Шестибайтовый адрес адаптера локальной сети
Прошитый адрес (Burned-in address)	Шестибайтовый адрес, назначенный производителем сетевого адаптера
Одноадресатный адрес (Unicast address)	Синоним MAC-адреса, который описывает единственное устройство в локальной сети
Широковещательный адрес (Broadcast address)	Адрес, который обозначает “все устройства в локальной сети в данный момент”
Многоадресатный адрес (Multicast address)	В среде Ethernet групповой адрес идентифицирует некую группу устройств в пределах одной локальной сети

Фреймирование Ethernet

Фреймирование (framing) определяет, как интерпретировать последовательность передаваемых битов. Другими словами, фреймирование задает значение передаваемых через сеть битов. Физический уровень передает последовательность битов с одного устройства на другое. Когда принимающее устройство получает набор битов, возникает вопрос: как их интерпретировать? Фреймированием называют метод идентификации полей, необходимых для передачи информации, и определения значения каждого бита, переданного или полученного из сети.

Обратимся к примеру, рассматриваемому выше, когда компьютер Фреда пересыпал данные компьютеру Барни через сеть Ethernet. Компьютер Фреда помещает адрес Ethernet компьютера Барни в заголовок фрейма, и компьютер Барни, получив этот фрейм, будет знать, что он предназначается именно ему. Стандарт IEEE 802.3 определяет месторасположение поля адреса получателя в последовательности битов, пересылаемой через сеть Ethernet.

Формат фрейма, используемый в среде Ethernet, несколько раз менялся с течением времени. Компания Xerox установила один формат фрейма, который был изменен IEEE при разработке стандартов в начале 1980-х. В итоге в 1997 году был выпущен стандарт фрейма, который содержит в себе как некоторые особенности оригинального фрейма Ethernet компании Xerox, так и фрейма IEEE. Этот пересмотренный вариант стандарта показан на рис. 3.14, *снизу*.

Большинство полей во фрейме Ethernet достаточно важно, чтобы сказать о них несколько слов в этой главе. В табл. 3.5 приведен список полей в заголовке и концепции фрейма и их краткое описание.

DIX

Преамбула	Получатель	Отправитель	Тип	Данные и заполнение	КСФ
8	6	6	2	46 – 1500	4

IEEE 802.3 (первоначальный)

Преамбула	РНФ	Получатель	Отправитель	Длина	Данные и заполнение	КСФ
7	1	6	6	2	46 – 1500	4

IEEE 802.3 (пересмотренный в 1997 г.)

Байты	Преамбула	РНФ	Получатель	Отправитель	Длина/ Тип 2	Данные и заполнение	КСФ
	7	1	6	6	2	46 – 1500	4

Рис. 3.14. Форматы заголовков фреймов

Таблица 3.5. Поля в заголовке и концевике фрейма стандарта IEEE 802.3

Поле	Длина поля в байтах	Описание или функция
Преамбула (preamble)	7	Синхронизация
Указатель начала фрейма (Start Frame Delimiter (SFD) — разделитель начала фрейма (РНФ))	1	Сигнализирует о начале фрейма. Следующий байт — первый байт в адресе получателя
MAC-адрес получателя (destination MAC address)	6	Задает получателя фрейма
MAC-адрес отправителя (source MAC address)	6	Задает отправителя фрейма
Длина (length)	2	Указывает длину поля данных во фрейме (присутствует или поле длины, или поле типа фрейма, но не оба одновременно)
Тип (type)	2	Определяет тип протокола, помещенного во фрейм (присутствует или поле длины, или поле типа фрейма, но не оба одновременно)
Данные и заполнение (data and pad) ¹	46-1500	Содержит данные верхних уровней, обычно блок PDU третьего уровня, очень часто — непосредственно пакет IP
Контрольная сумма фрейма, КСФ (Frame Check Sequence, FCS)	4	Используется для проверки фрейма на целостность и отсутствие ошибок

¹ Стандарт IEEE 802.3 ограничивает максимальный размер поля данных величиной в 1500 байтов. Поле данных предназначено для передачи пакета третьего уровня модели OSI; термин *максимальный блок передачи* (Maximum Transmission Unit — MTU) используется для указания максимального размера пакета третьего уровня, который можно переслать через среду передачи данных. Поскольку пакет третьего уровня должен находиться в поле данных фрейма Ethernet, то 1500 байт — наибольший размер блока MTU протокола IP, разрешенный в среде Ethernet. — Примеч. авт.

Распознавание данных во фрейме Ethernet

За многие годы было разработано множество сетевых протоколов (т.е. протоколов третьего уровня). Большинство из них — это просто компоненты в более крупных сетевых моделях, разработанных различными производителями оборудования для своих продуктов, такие как системная сетевая архитектура (System Network Architecture — SNA) компании IBM, операционная система NetWare компании Novell, сеть DECnet компании DEC, сеть AppleTalk компании Apple Computer и т.п. Кроме того, модели OSI и TCP/IP также имеют свои протоколы сетевого уровня.

Все перечисленные протоколы третьего уровня и некоторые другие могут использовать среду Ethernet в качестве средства передачи данных. Для этого протоколам сетевого уровня необходимо поместить свой пакет (или блок PDU третьего уровня) в поле данных фрейма Ethernet (рис. 3.14). Но когда устройство получает подобный фрейм Ethernet, как ему определить, какого типа PDU в нем содержится? Может быть, это пакет IP, или пакет OSI, или блок данных протокола SNA?

Чтобы ответить на этот вопрос, в большинстве протоколов канального уровня, включая Ethernet, в заголовке фрейма содержится поле с кодом, который и определяет тип передаваемого протокола. Это поле в протоколах канального уровня называется *полем типа протокола* (protocol type). Например, если фрейм Ethernet переносит пакет IP, то в его поле типа (см. рис. 3.14) будет содержаться шестнадцатеричное число 0x800 (десятичное 2048). Другие протоколы третьего уровня будут иметь собственные, отличные значения в поле типа протокола.

Обратите внимание на то, что в первом стандарте формата фрейма IEEE 802.3 вместо поля типа протокола используется поле длины фрейма, а в пересмотренном формате это поле объединено с полем длины фрейма. Если значение в этом поле меньше, чем шестнадцатеричное число 0x600 (1536 в десятичном виде), то это поле используется в значении длины фрейма и указывает длину всего поля данных (без преамбулы и указателя начала фрейма), в противном случае поле используется для указания типа протокола. В случае если это поле используется для определения размера фрейма, то во фрейме необходимо другое поле для указания протокола третьего уровня, передаваемого во фрейме.

Для этого используется еще один или два дополнительных заголовка, расположенных после заголовка стандарта IEEE 802.3, но перед вложенным в поле данных заголовком третьего уровня. Например, при пересылке пакета IP во фрейме Ethernet будут содержаться два дополнительных заголовка:

- заголовок IEEE 802.2 управления логическим каналом (Logical Link Control — LLC);
- заголовок стандарта IEEE протокола доступа к подсети (Subnetwork Access Protocol — SNAP).

На рис. 3.15 показан фрейм Ethernet с такими дополнительными заголовками. Обратите внимание: поле типа заголовка SNAP используется для тех же целей и с теми же значениями, что и поле типа протокола в заголовке Ethernet.

Байты	Заголовок IEEE 802.3					Заголовок IEEE 802.2 LLC				SNAP-заголовок		
	Преамбула	РНФ	Получатель	Отправитель	Длина*	DSAP	SSAP	CTL	OUI	тип	Данные и заполнение 46 - 1500	КСФ
7	1	6	6	2	1	1	1	1	3	2	46 - 1500	4

* Определяет длину в том случае, если десятичное значение меньше, чем 1536

Рис. 3.15. Заголовок SNAP стандарта 802.2

Обнаружение ошибок

Последняя рассматриваемая в данной главе функция канального уровня технологии Ethernet — это обнаружение ошибок. Обнаружение ошибок представляет собой процесс, позволяющий определить, не менялись ли биты во фрейме при передаче его через физическую среду. Изменение битов может произойти в результате множества различных небольших ошибок, и, как правило, эти ошибки — следствие различных видов электромагнитной интерференции. Как и любой другой протокол канального уровня, рассматриваемый в экзамене CCNA, Ethernet имеет и заголовок, и концевик фрейма, а в последнем содержится поле, используемое для обнаружения ошибок.

Поле *контрольной суммы фрейма* (Frame Check Sequence — FCS), единственное поле концевика фрейма Ethernet, позволяющее устройству, принявшему фрейм, определить, изменились ли его биты в процессе передачи по сети. Для заполнения поля контрольной суммы устройство-отправитель по сложной математической формуле, используя содержимое фрейма, рассчитывает четырехбайтовое число. Принимающее устройство производит те же самые математические операции. Если результат вычислений совпадает со значением, записанным в поле контрольной суммы, то фрейм передан без ошибок. Если же результат вычисления и записанное в поле числа не совпадают, то произошла ошибка, и фрейм уничтожается.

Обратите внимание на то, что механизм обнаружения ошибок не подразумевает восстановление данных. Стандарт Ethernet указывает, что фреймы с ошибками должны уничтожаться, и при этом никаких дополнительных действий, например повторная пересылка поврежденного фрейма, не производится. Задача повторной передачи поврежденной информации возлагается на верхние уровни модели OSI. Так, например, протокол TCP отслеживает потерю информации и производит повторную передачу (подробнее об этом рассказывается в главе 6).

Подготовка к экзамену

Повторите все ключевые темы

Повторите все ключевые темы данной главы, помеченные пиктограммой “Ключевая тема”. Ключевые темы и соответствующие им страницы перечислены в табл. 3.6.

Таблица 3.6. Ключевые темы главы 3

Элемент	Описание	Страница
Табл. 3.2	Наиболее распространенные разновидности технологии Ethernet	86
Список	Обобщение алгоритма CSMA/CD	89
Рис. 3.6	Стандартные схемы расположения выводов кабелей TIA	95
Рис. 3.7	Принцип работы прямого кабеля	96
Рис. 3.8	Перекрещенный кабель	96
Табл. 3.3	Использование контактов в стандартах 10BASE-T и 100BASE-TX	97
Список	Алгоритм CSMA/CD	99
Рис. 3.13	Структура одноадресатного адреса Ethernet	104
Табл. 3.4	Терминология и функции MAC-адресов в локальной сети	105

Заполните таблицы и списки по памяти

Распечатайте приложение М (Appendix L) с компакт-диска или его раздел, относящийся к этой главе, и заполните таблицы и списки по памяти. В приложении Н (Appendix M) приведены заполненные таблицы и списки для самоконтроля.

Ключевые термины

Дайте определения перечисленных ниже терминов и проверьте правильность их написания в списке терминов:

1000BASE-T, 100BASE-TX, 10BASE-T, перекрещенный кабель (crossover cable), алгоритм CSMA/CD (CSMA/CD), дуплексный режим передачи (full duplex), полу duplexный режим передачи (half duplex), концентратор (hub), схема расположения выводов кабелей (pinout), поле типа протокола (protocol type), совместно используемая среда Ethernet (shared Ethernet), прямой кабель (straight-through cable), коммутатор (switch), коммутируемая среда Ethernet (switched Ethernet), витая пара (twisted pair).

В этой главе...

- **Уровень 1 модели OSI в двухточечных каналах распределенной сети.** Описаны кабельная разводка и аппаратные средства, используемые для создания подключения по выделенной линии на стороне потребителя.
- **Уровень 2 модели OSI в двухточечных каналах распределенной сети.** Приведены основные сведения о таких протоколах канального уровня, используемых для создания подключения по выделенной линии, как HDLC и PPP.
- **Технология Frame Relay и службы с коммутацией пакетов.** Рассматриваются концепции организации службы с коммутацией пакетов распределенных сетей, причем основное внимание уделено технологии Frame Relay.

ГЛАВА 4

Основы сетей WAN

В предыдущей главе были подробно рассмотрены механизмы, используемые в локальных сетях Ethernet, для осуществления функций, определяемых первыми двумя уровнями модели OSI. В этой главе речь также идет о стандартах и протоколах, реализующих уровни 1 (физический уровень) и 2 (канальный уровень) модели OSI, но уже применительно к распределенным сетям. Кроме того, ниже приведены дополнительные сведения о физическом уровне модели OSI, а также описаны три протокола канального уровня, популярные в сетях WAN: *высокоуровневый протокол управления каналом* (High-Level Data Link Control — HDLC), *протокол двухточечного соединения* (Point-to-Point Protocol — PPP) и технология Frame Relay.

Контрольные вопросы: знаете ли вы уже темы главы

Этот раздел предназначен для того, чтобы читатель мог предварительно оценить свои знания и решить, нужно ли ему читать главу целиком. Если ответы на семь из восьми вопросов даны правильно, можно сразу же перейти к последнему разделу “Подготовка к экзамену”. Основные темы этой главы и предварительных контрольных вопросов перечислены в табл. 4.1. Отвечая на контрольные вопросы и используя таблицу, читатель сможет достаточно точно определить свои знания в той или иной области. Ответы на вопросы приведены в приложении А.

Таблица 4.1. Темы контрольных вопросов

Основная тема	Номера вопросов
Уровень 1 модели OSI в двухточечных каналах распределенной сети	1–4
Уровень 2 модели OSI в двухточечных каналах распределенной сети	5, 6
Технология Frame Relay и службы с коммутацией пакетов	7, 8

1. Какой из перечисленных ниже терминов наилучшим образом описывает основную функцию протоколов уровня 1 модели OSI?
 - а) Фреймирование (framing).
 - б) Пересылка последовательностей битов от одного устройства к другому.
 - в) Адресация (addressing).
 - г) Интерфейс локального управления (Local Management Interface — LMI).
 - д) Идентификаторы DLCI.
2. Какие типы устройств из перечисленных ниже обычно используются для подключения к четырехжильному телефонному проводу городской телефонной сети?

- а) Последовательный интерфейс маршрутизатора без внутреннего CSU/DSU.
 - б) Модуль CSU/DSU.
 - в) Последовательный интерфейс маршрутизатора с внутренним трансивером.
 - г) Последовательный интерфейс коммутатора.
3. Какие типы устройств из перечисленных ниже обычно используются для подключения к разъему V.35 или RS-232 при подключении по выделенной линии?
- а) Последовательный интерфейс маршрутизатора без внутреннего CSU/DSU.
 - б) Модуль CSU/DSU.
 - в) Последовательный интерфейс маршрутизатора с внутренним трансивером.
 - г) Последовательный интерфейс коммутатора.
4. При создании распределенной сети на основе выделенной линии, соединяющей два маршрутизатора, которые находятся за сотни километров один от другого, какие устройства рассматриваются в качестве терминального оборудования (устройств DTE)?
- а) Маршрутизаторы.
 - б) Модули CSU/DSU.
 - в) Станции АТС.
 - г) Процессор каждого маршрутизатора.
 - д) Ни один из указанных выше ответов не верен.
5. Какие из следующих функций уровня 2 модели OSI специфицированы стандартом протокола PPP, но реализуются с помощью поля заголовка собственной версии протокола HDLC компании Cisco?
- а) Фреймирование (framing).
 - б) Арбитраж (arbitration).
 - в) Адресация (addressing).
 - г) Обнаружение ошибок (error detection).
 - д) Идентификация типа протокола соответствующего фрейма.
6. Пусть маршрутизатор M1 имеет подключение к трем двухточечным последовательным каналам, каждый из которых связывает его с одним из трех дистанционных маршрутизаторов. Какое из следующих утверждений по поводу требуемой HDLC-адресации на стороне маршрутизатора M1 верно?
- а) M1 должен использовать адреса HDLC 1, 2 и 3.
 - б) M1 должен использовать три любых уникальных адреса в диапазоне от 1 до 1023.
 - в) M1 должен использовать три любых уникальных адреса в диапазоне от 16 до 1000.
 - г) M1 должен использовать три последовательных уникальных адреса в диапазоне от 1 до 1023.
 - д) Ни один из указанных выше ответов не верен.

-
7. Как называется поле протокола Frame Relay, используемое для идентификации виртуальных соединений Frame Relay?
 - а) Идентификатор канального подключения (data-link connection identifier).
 - б) Идентификатор соединения канала (data-link circuit identifier).
 - в) Индикатор подключения канала (data-link connection indicator).
 - г) Индикатор соединения канала (data-link circuit indicator).
 - д) Ни один из указанных выше ответов не верен.
 8. Какое из следующих утверждений справедливо для виртуальных каналов (Virtual Circuit — VC) Frame Relay?
 - а) Каждому виртуальному каналу нужен отдельный канал связи (access link).
 - б) Несколько виртуальных каналов могут использовать один и тот же канал связи.
 - в) Все виртуальные каналы, использующие один и тот же канал связи, должны быть подключены к одному и тому же маршрутизатору на другой стороне соединения по виртуальному каналу.
 - г) Все виртуальные каналы одного и того же физического канала связи должны использовать один и тот же идентификатор DLCI.

Основные темы

Как читателю известно из предыдущей главы, пересылку данных в физических сетях самых разных типов можно описать, применяя канальный и физический уровни модели OSI. При этом можно выделить две группы сетевых стандартов и протоколов. К первой группе относятся стандарты и протоколы сетей, связывающих *локальные* устройства, т.е. находящиеся относительно недалеко одно от другого (отсюда и произошло название таких сетей). Ко второй группе относятся стандарты и протоколы сетей, связывающих устройства, *распределенные* по достаточно большой площади (в некоторых случаях расстояния между устройствами таких сетей могут составлять тысячи километров), что также нашло свое отражение в названии таких сетей — *распределенные*.

Тем не менее как локальные, так и распределенные сети реализуют функции, соответствующие уровням 1 и 2 модели OSI. Различаются лишь механизмы реализации, а также второстепенные детали. В текущей главе перечислены общие принципы реализации требуемых функций и подробно описаны их различия.

Следует отметить, что при описании распределенных сетей в данной главе основной акцент сделан на корпоративные сети, использующие технологии WAN для соединения дистанционных площадок. В части V данной книги распределенные сети рассматриваются в более широком контексте, включая такие популярные технологии доступа к сети Интернет, как *цифровые абонентские каналы* (Digital Subscriber Line — DSL) и различные кабельные технологии. Кроме того, в ней подробно рассматриваются вопросы конфигурации распределенных сетей. Дополнительную информацию о технологии Frame Relay, а также о построении *виртуальных частных сетей* (Virtual Private Network — VPN) в сети Интернет, позволяющих использовать ее вместо традиционных технологий WAN, можно найти во втором томе книги.

Уровень 1 модели OSI в двухточечных каналах распределенной сети

Физический уровень модели OSI, или уровень 1, детально определяет механизм пересылки физических данных от одного устройства к другому. Поэтому часто об уровне 1 модели OSI говорят как об уровне, на котором “пересылаются биты”. Собственно данные инкапсулируются на более высоких уровнях, как было описано в главе 2. Действительно, несмотря на то, что происходит на остальных уровнях модели OSI, в конечном итоге устройство-отправитель должно переслать определенную последовательность битов устройству-получателю. Физический уровень модели OSI как раз и описывает стандарты и протоколы, используемые для создания физической сети и пересылки битовых последовательностей по этой сети.

Во многом работа двухточечного канала распределенной сети подобна *магистральному каналу* (trunk) Ethernet, соединяющему два *коммутатора* (switch) Ethernet. Пример такого канала приведен на рис. 4.1, на котором показана локальная сеть, развернутая в двух зданиях, в каждом из которых есть свой коммутатор. Как, должно быть, помнит читатель, многие устройства Ethernet используют одну пару в кабеле для получения данных и вторую — для отправки данных, что позволяет снизить помехи от электромагнитной интерференции. Обычно между устройствами конечных

пользователей и коммутаторами используются кабели Ethernet *прямого* (straight-through) расположения выводов. Для магистральных линий, соединяющих коммутаторы, используются *перекрещенные* (crossover) кабели, поскольку каждый из коммутаторов передает данные на те же контакты разъема подключения кабеля. Таким образом, перекрещенные кабели соединяют передающую пару контактов одного устройства с принимающей парой контактов другого устройства. Этот принцип передачи данных показан в нижней части рис. 4.1.

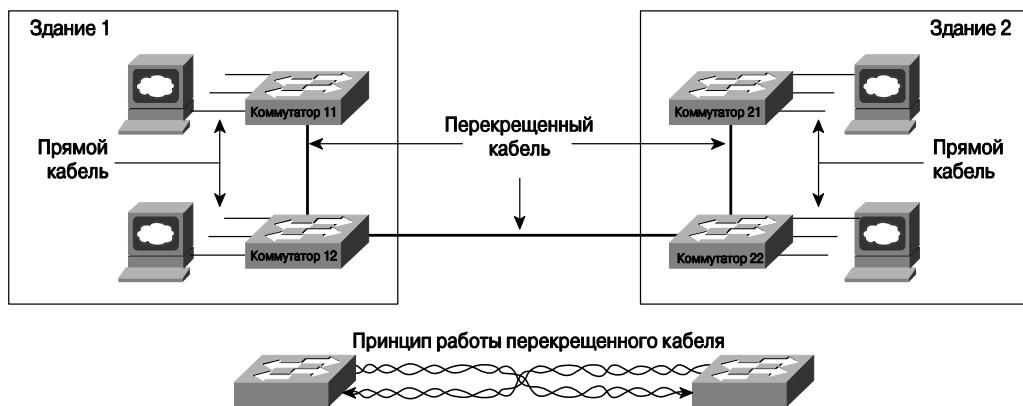


Рис. 4.1. Пример локальной сети между двумя зданиями

Ну а теперь представьте, что здания находятся не в пределах одного квартала, а на расстоянии 1000 км одно от другого. Сразу же становится понятно, что в этом случае мы имеем дело как минимум с двумя следующими проблемами.

- Технология Ethernet не позволяет создавать кабельные системы, обеспечивающие работу отдельной магистральной линии протяженностью 1000 км.
- Даже если бы технология Ethernet и обеспечивала поддержку магистральных линий протяженностью 1000 км, вряд ли кому-либо удастся получить все необходимые разрешения для прокладки такой линии по территории всех без исключения соответствующих земельных участков, которые находятся между двумя зданиями.

Поэтому основное различие между локальными и распределенными сетями заключается в том, насколько далеко могут находиться одно от другого принимающее и передающее устройства при условии гарантированной отправки и гарантированного получения данных. Локальные сети, как правило, размещаются в пределах одного здания или, как вариант, в пределах нескольких зданий, т.е. некоторой территории (например кампуса). Но даже в последнем случае магистральные оптоволоконные линии работают по технологии Ethernet. Распределенные сети обычно работают на расстояниях, гораздо больших, чем это предусмотрено технологией Ethernet, — в сетях, объединяющих районы города или даже целые города. Более того, часто право прокладки кабельных сетей между городами в стране имеет лишь несколько компаний. Поэтому разработчики стандартов распределенных сетей должны были использовать для описания механизмов отправки и получения данных

на расстояния, измеряемые тысячами километров, спецификации, отличные от аналогичных спецификаций физического уровня Ethernet.

ВНИМАНИЕ!

Помимо терминов *локальная сеть* и *распределенная сеть*, для описания сетей, объединяющих отдельные здания, которые находятся на значительном расстоянии одно от другого, используется термин *городская сеть*, или *региональная сеть* (Metropolitan-Area Networks — MAN). Термином MAN обычно обозначаются распределенные сети, которые “не дотягивают” до того, чтобы называться полноценной сетью WAN. Как правило, к таким сетям относятся сети масштаба отдельного города или мегаполиса. Тем не менее различия между локальными, городскими, региональными и распределенными сетями достаточно размыты. Проще говоря, нельзя назвать точные цифры протяженности линии, на основании которой эту линию однозначно можно было бы назвать сегментом сети LAN, MAN или WAN.

На физическом уровне созданием подобных сетей большой протяженности занимаются специализированные компании, которые обеспечивают приобретение, прокладку и эксплуатацию соответствующих кабельных систем. Естественно, именно такие компании имеют все необходимые документы и разрешения для проведения земляных работ в городе. Поэтому компания, которая нуждается в передаче данных по распределенным сетям, не являясь владельцем кабельной системы, вынуждена арендовать каналы связи у владельца. В таких случаях каналы связи называются *арендованными* (leased), или *выделенными* (dedicated), поскольку компания-владелец не продает, а сдает в аренду, или “выделяет” (возможно, во временное пользование), канал компании-потребителю. Очень часто в роли компаний-владельцев выделенных каналов связи для распределенных сетей выступают местные *телефонные компании* (telephone company — telco). Во многих странах, где сохраняется государственное регулирование электросвязи или государственная монополия на электросвязь, такие компании называются ОТТК, или *общественными телефонно-телеграфными компаниями* (Public Telephone and Telegraph — PTT). Однако в настоящее время большинство пользователей, говоря о компании, обеспечивающей доступ к распределенной сети любого вида (особенно к Интернету), предпочитают использовать термин *провайдер*, или *провайдер служб* (service provider).

Двухточечные магистральные каналы WAN обеспечивают базовое соединение между двумя точками. Для получения такого канала нужно обратиться к провайдеру, который обеспечит прокладку кабеля. Услуга, предоставляемая в подобных случаях телефонной компанией или провайдером, подобна наличию постоянной телефонной связи между двумя площадками. Такое утверждение означает, что два устройства на каждой из оконечных точек линии WAN могут отправлять битовые последовательности одно другому и получать их в любой момент времени, не занимаясь набором номера и не тратя время на установление соединения. Поскольку такое соединение WAN всегда доступно для обмена информацией, его нередко называют *арендуемым каналом* (leased circuit), или *выделенной линией* (leased line), поскольку пользователь имеет эксклюзивное право занимать этот канал, если он оплачивает его аренду.

Теперь вернемся к сравнению локальной сети, соединяющей два расположенных рядом здания, с распределенной сетью, соединяющей два здания, находящихся одно от другого на расстоянии 1000 км. Как показано на рис. 4.2, хотя физические детали соединения отличаются, обе сети выполняют одни и те же основные функции.

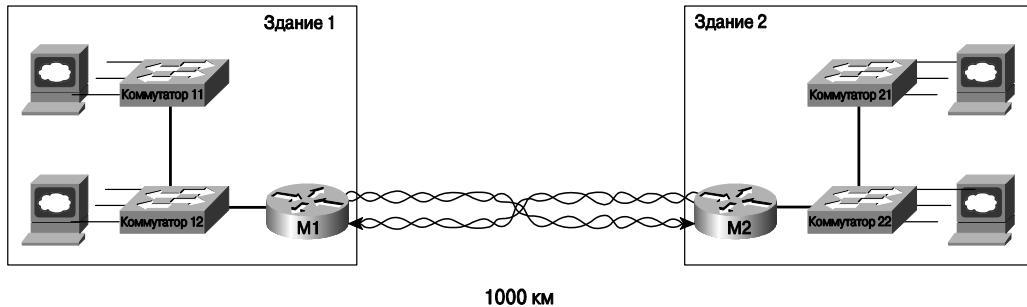


Рис. 4.2. Концептуальное представление двухточечной выделенной линии

Еще раз нужно подчеркнуть, что на рис. 4.2 представлено только концептуальное представление двухточечного канала WAN. С концептуальной точки зрения телекоммуникационная компания прокладывает между зданиями физический кабель, в состав которого входят пары проводов для приема и передачи. Кабель соединяет между собой оба маршрутизатора, каждый из которых подключен к коммутатору своей локальной сети. В результате образуется новый физический канал WAN и логическое соединение между маршрутизаторами, что позволяет обмениваться данными между обеими площадками. В следующем разделе физические детали работы каналов WAN описаны более подробно.

ВНИМАНИЕ!

Коммутаторы Ethernet могут быть оборудованы самыми разными интерфейсами, однако все интерфейсы относятся к той или иной форме технологии Ethernet. Маршрутизаторы обеспечивают соединение различных типов технологий уровней 1 и 2 модели OSI. Поэтому, когда локальная сеть подключается к сети удаленной площадки с помощью канала WAN, такое подключение обеспечивается с помощью двух маршрутизаторов, как и показано на рис. 4.2.

Соединение сети WAN с точки зрения потребителя

Итак, сама концепция двухточечного соединения достаточно проста. Однако чтобы полностью разобраться в том, каким образом провайдер строит свою сеть для поддержки двухточечного канала связи, читателю придется потратить немало времени на изучение технологий, которые лежат далеко за рамками тем экзамена ICND1. С другой стороны, большинство сведений о сетях WAN, которые читателю нужны для сдачи экзамена ICND1, относятся к тому, как соединения WAN реализуются между поставщиком услуг и площадкой потребителя. Кроме того, читателю понадобится также немного ознакомиться с терминологией, используемой провайдером.

Как было показано на рис. 4.2, выделенный канал WAN можно представить в виде двух витых пар, с помощью которых телефонная (или телекоммуникационная) компания обеспечивает связь между двумя площадками. Да, в действительности все не так просто. Конечно, на самом деле для обеспечения связи используется гораздо больше технологий, причем терминология, которая при этом применяется телефонными компаниями, значительно отличается от терминологии, принятой для описа-

ния локальных сетей. Вряд ли найдется такая телефонная компания, которая сможет проложить тысячекилометровую линию для связи двух площадок. В действительности компании обычно создают обширную сеть, а затем просто прокладывают несколько кабельных линий от местной АТС к вашему зданию (АТС — это просто здание, в котором телефонная компания размещает оборудование, поддерживающее работу ее сети). Независимо от того, что телефонная компания предпринимает внутри своей сети, потребитель в результате получает эквивалент выделенного четырехжильного канала, соединяющего два здания.

На рис. 4.3 представлены некоторые ключевые концепции и термины, имеющие отношение к сетям WAN.

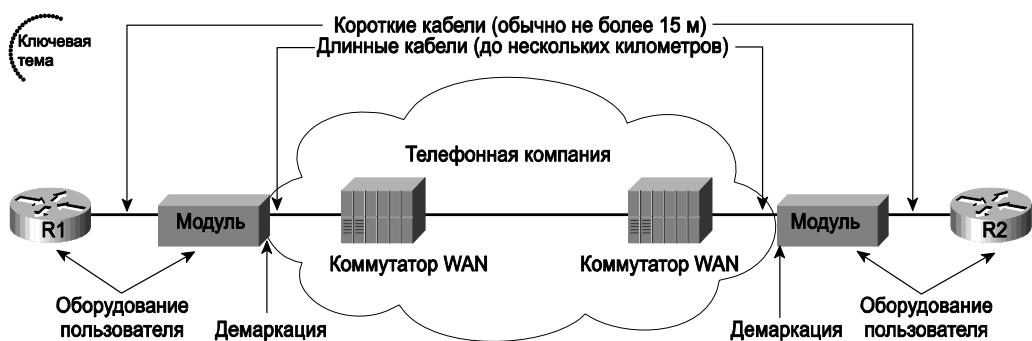


Рис. 4.3. Двухточечная выделенная линия: компоненты и терминология

Обычно маршрутизаторы подключаются к устройству, называемому внешним модулем обслуживания канала/модулем обработки данных (Channel Service Unit/Data Service Unit — CSU/DSU). Такое подключение маршрутизатора к модулю CSU/DSU осуществляется с помощью относительно короткого кабеля, длина которого не превышает 15 м (в более длинных кабелях, как правило, нет необходимости, поскольку модули обычно монтируются в стойке поблизости от маршрутизатора). Гораздо более длинный четырехжильный канал, предоставленный телефонной компанией, подключается к модулю CSU/DSU. Именно этот четырехжильный кабель выходит за пределы здания и идет к АТС вместе с другими подобными кабелями (обычно под землей), проходя при этом через коммутационные щиты (вам, наверное, доводилось видеть работников АТС, занимающихся обслуживанием таких щитов, которые обычно устанавливают у обочин дорог, в подъездах и т.п.). Далее кабель входит в здание АТС, где и подключается к устройству в станции, которое в общем случае называется коммутатором WAN.

Описанный принцип физического подключения реализуется на обеих сторонах двухточечного канала WAN. На участке между двумя АТС провайдер (телефонная компания или несколько телефонных компаний) может создавать собственную сеть, основанную на одновременном использовании различных технологических решений, каждое из которых лежит за пределами любого из экзаменов CCNA. Однако общий принцип, показанный на рис. 4.2, остается неизменным: два маршрутизатора могут одновременно отправлять и получать данные по двухточечному каналу WAN.

С юридической точки зрения различные компоненты оборудования и линии связи, показанные на рис. 4.3, принадлежат двум разным компаниям. Например, ка-

бельные линии маршрутизаторов, а также обычно модули CSU/DSU являются собственностью клиента телефонной компании. Кабели, связывающие потребителя с АТС, а также оборудование АТС принадлежат телефонной компании. Поэтому телефонные компании используют такое понятие, как *демаркация* (demarc), являющееся сокращением от выражения *точка демаркации* (demarcation point), для обозначения линии, которая разграничивает зоны ответственности телефонной компании и потребителя. Следует заметить, что демаркация — это не какое-то конкретное устройство или сегмент кабеля, а скорее некое концептуальное понятие, показывающее границы зон ответственности телефонной компании и потребителя.

В США демаркация обычно соответствует точке, в которой телефонная компания физически размещает выводы двух витых пар внутри здания потребителя. Как правило, потребитель просит телефонную компанию смонтировать такие выводы в определенном помещении, причем в этом же помещении размещаются большинство или вообще все выводы линий, которые телефонная компания предоставляет потребителю.

Термин *оборудование клиента* (Customer Premises Equipment — CPE) относится к устройствам, которые с точки зрения телефонной компании находятся в зоне ответственности потребителя. Например, модуль CSU/DSU и маршрутизатор в этом контексте относятся к оборудованию клиента.

Следует также заметить, что демаркационная точка не всегда располагается так, как показано на рис. 4.3. В некоторых случаях модуль CSU/DSU является собственностью телефонной компании, поэтому точка демаркации может находиться между этим модулем и маршрутизатором. Кроме того, в последнее время проявляется тенденция размещения модуля CSU/DSU, принадлежащего телефонной компании и обслуживаемого телефонной компанией, на территории потребителя. Естественно, это соответствующим образом сдвигает точку демаркации на площадку потребителя. Но независимо от того, где юридически находится демаркационная линия, термин *оборудование CPE* всегда относится к тому оборудованию, которое принадлежит клиенту, а не телефонной компании.

Стандарты кабельных соединений WAN

Компания Cisco устанавливает в своих маршрутизаторах широкий спектр интерфейсов соединений WAN, включая синхронные и асинхронные *последовательные* (serial) интерфейсы. Поэтому, когда в этой главе обсуждаются двухточечные кабельные последовательные соединения или соединения Frame Relay, читатель должен понимать, что речь идет об интерфейсах маршрутизаторов, поддерживающих синхронные коммуникации.

Синхронные последовательные интерфейсы маршрутизаторов Cisco используют разъемы разнообразных собственных (proprietary) типов, такие, например, как 60-контактный разъем D, показанный на рис. 4.4, сверху. Кабель, соединяющий маршрутизатор с модулем CSU/DSU, подключается на стороне маршрутизатора разъемом, соответствующим последовательному интерфейсу маршрутизатора, а на стороне модуля CSU/DSU — разъемом WAN одного из стандартных типов, соответствующим интерфейсу модуля CSU/DSU. На рис. 4.4 показаны типичные подключения с примерами некоторых типов разъемов для последовательных интерфейсов.

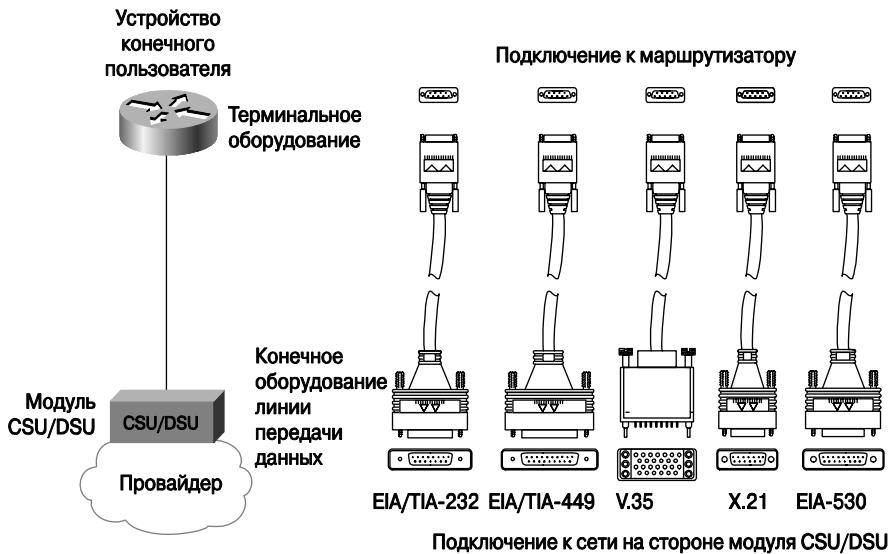


Рис. 4.4. Варианты последовательных подключений

Инженер, занимающийся внедрением сети, должен просто выбрать нужный кабель, основываясь на типах разъема маршрутизатора и модуля CSU/DSU. Никакие другие обстоятельства или соображения при выборе кабеля (например, что именно передается по контактам разъема) инженеру учитывать не нужно — достаточно подключить правильно выбранный кабель, и он будет работать! Этот момент принципиально важен, поскольку многие контакты разъемов на самом деле используются для управляющих функций, и лишь несколько — собственно для передачи данных. Правда, некоторые контакты задействуются для синхронизации, о них читатель узнает из следующего раздела.

ВНИМАНИЕ!

Ассоциация телекоммуникационной промышленности (Telecommunications Industry Association — TIA) уполномочена Национальным институтом стандартизации США (American National Standards Institute — ANSI) представлять США в международных органах по стандартизации. Ассоциация TIA разработала несколько стандартов соединений WAN, а также стандарты соединений LAN. Более подробная информация о международных органах по стандартизации, а также о том, как приобрести экземпляры этих стандартов, находится на веб-сайтах этих организаций (<http://www.tiaonline.org> и <http://www.ansi.org>).

Кабель, соединяющий модуль CSU/DSU со станцией АТС, обычно заканчивается разъемом RJ-48 для подключения к модулю CSU/DSU. Размер и форма разъема RJ-48 соответствуют размеру и форме разъема RJ-45, которыми оборудуются кабельные системы сетей Ethernet.

Многие маршрутизаторы Cisco поддерживают последовательные интерфейсы, имеющие интегрированные внутренние модули CSU/DSU. Если маршрутизатор оборудован таким интегрированным модулем, кабель для соединения маршрутизатора с внешним модулем CSU/DSU, естественно, не нужен. В таких случаях после-

довательные кабели, показанные на рис. 4.4, не используются, а физическая линия, проложенная от АТС, подключается непосредственно к порту маршрутизатора (как правило, такой порт последовательного интерфейса маршрутизатора имеет встроенный разъем RJ-48).

Тактовая частота, синхронизация, оконечное оборудование линии передачи данных и терминальное оборудование

Инженеру, занимающемуся развертыванием корпоративной сети, при создании нового двухточечного выделенного канала между двумя маршрутизаторами предстоит решить несколько задач. Прежде всего сетевой инженер должен связаться с провайдером и заказать предоставление выделенной линии. При этом сетевой инженер должен указать пропускную способность этой линии, выраженную в килобитах в секунду (Кбит/с). Пока телефонная компания занимается прокладкой линии, инженер приобретает для предприятия два модуля CSU/DSU, устанавливает каждый из них на одной из площадок и соответствующим образом настраивает их. Кроме того, сетевой инженер приобретает и устанавливает маршрутизаторы и соединяет каждый из них с помощью кабелей, показанных на рис. 4.4, с соответствующим модулем CSU/DSU. Как только инженеры АТС закончат прокладку линии, к ней подключаются модули CSU/DSU, как показано на рис. 4.4.

Каждый из каналов связи WAN, предоставляемых провайдером, работает на одной из заранее оговоренных скоростей. Такую скорость часто называют *тактовой частотой* (clock rate), *шириной полосы пропускания* (bandwidth) или *скоростью канала* (link speed). Сетевой инженер предприятия (т.е. специалист клиента) обязан указать минимально допустимую скорость при оформлении договора на предоставление канала, поскольку она влияет на технические параметры линии, прокладываемой от АТС. Кроме того, сетевой инженер предприятия должен настроить модуль CSU/DSU на каждой из площадок так, чтобы эта настройка соответствовала требуемой скорости.

Чтобы канал связи устойчиво работал, нужно, чтобы различные подключенные к нему устройства приводили свои частоты в соответствие с некоторой эталонной частотой. Этот процесс и называется *синхронизацией* (synchronization). В *синхронных каналах* (synchronous circuits) временная выборка осуществляется как на стороне отправителя, так и на стороне получателя. Естественно, в идеале все устройства должны согласовать свои скорости так, чтобы работать на одной и той же скорости. Однако на практике задача обеспечения поддержания истинно одинаковых значений скорости является слишком сложной и дорогой в реализации. Поэтому в действительности устройства работают на *примерно* одинаковой скорости, периодически согласовывая свою скорость со скоростью устройств, находящихся на другой стороне канала связи. В том случае, если обнаруживается рассогласование, одна из сторон выполняет подстройку своей скорости.

Синхронизация двух модулей CSU/DSU, соединенных выделенной линией, выполняется за счет принудительного приведения таймера одного из модулей CSU/DSU (ведомого) в соответствие с тактовой частотой другого модуля CSU/DSU (ведущего). Процесс происходит практически так же, как это показывают в фильмах о разведчиках, сверяющих часы. Единственное отличие сетевых устройств от разведчиков заключается в том, что сетевые устройства сверяют свои часы несколько раз в секунду.

На практике простая концепция синхронизации выливается в использование цепи иерархии различных источников сигналов таймера. Телефонная компания предоставляет информацию о временных параметрах модулям CSU/DSU, основываясь на передаче электрических сигналов в линии связи. Затем оба модуля CSU/DSU подстраивают свои скорости в соответствии с *синхросигналом* (*clocking signal*), полученным от телефонной компании. Каждый из модулей CSU/DSU, в свою очередь, передает синхросигналы маршрутизаторам, которым остается лишь реагировать на эти сигналы, отправляя и получая данные с корректной частотой. Поэтому с точки зрения маршрутизаторов заданием частоты канала связи занимаются модули CSU/DSU.

С процессом синхронизации связано еще несколько ключевых понятий распределенных сетей. Так, устройство, обеспечивающее задание частоты (обычно это модуль CSU/DSU), рассматривается в качестве *оконечного оборудования канала передачи данных* (Data Communication Equipment — DCE). Устройство же, управляемое синхросигналами (обычно это маршрутизатор), называют *терминальным оборудованием* (Data Terminal Equipment — DTE).

Создание соединения WAN в лаборатории

С практической точки зрения при приобретении последовательного кабеля для устройств Cisco нужно выбирать либо кабель с разъемом для подключения устройства DTE, либо кабель с разъемом для подключения устройства DCE. Конкретный тип кабеля определяется тем, какую роль играет маршрутизатор: роль терминального оборудования или роль конечного оборудования линии передачи данных. В реальных соединениях WAN маршрутизатор в большинстве случаев играет роль терминального оборудования, поэтому для подключения к модулю CSU/DSU нужно использовать кабель для устройства DTE.

В лабораторных условиях можно создать последовательный канал без использования модулей CSU/DSU, нужно лишь, чтобы один из маршрутизаторов обеспечивал генерацию тактовой частоты. Иными словами, когда в процессе подготовки к экзаменам Cisco вы захотите создать лабораторную сеть, вам не нужно для этого приобретать модули CSU/DSU или заказывать подключение к реальному каналу WAN. Достаточно лишь приобрести два маршрутизатора, последовательный кабель DTE для одного маршрутизатора, последовательный кабель DCE для второго, а затем подключить маршрутизаторы один к другому, соединив кабели вместе. Маршрутизатор, к которому подключен кабель DCE, можно настроить так, чтобы он генерировал тактовую частоту, что позволит обойтись без модуля CSU/DSU. Таким образом, даже в скромных лабораторных условиях можно развернуть распределенную сеть, сэкономив при этом несколько сотен долларов на покупке модуля CSU/DSU. Кабели DTE и DCE можно подключить один к другому (кабель DCE имеет оконечный разъем в виде гнезда, а кабель DTE — в виде штекера), а затем каждый из них — к соответствующему маршрутизатору. Введя на одном из маршрутизаторов одну-единственную команду (команду `clock rate`), читатель получит готовый двухточечный последовательный канал. Такой тип подключения двух маршрутизаторов иногда называют *прямым лабораторным подключением* (back-to-back link).

На рис. 4.5 показаны кабельные линии при прямом лабораторном подключении, а также подключенные один к другому кабели DCE/DTE, в которых инвертированы

контакты передачи и приема. Такой кабель напоминает по своему принципу работы перекрещенный кабель Ethernet, с помощью которого обеспечивается обмен данными между двумя одинаковыми устройствами локальной сети, непосредственно подключенными одно к другому.

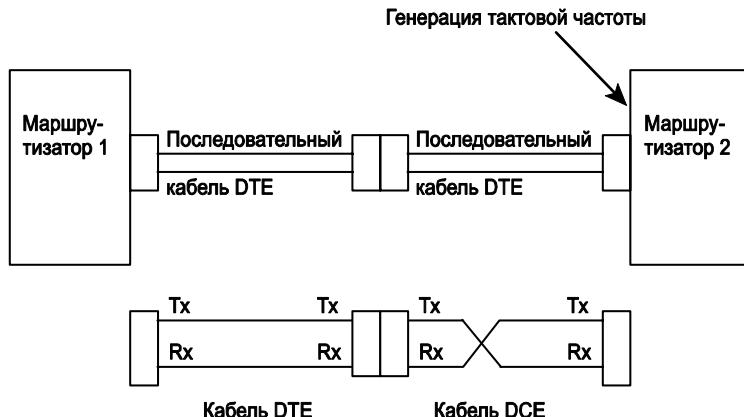


Рис. 4.5. Последовательные кабельные соединения, использующие кабели DTE и DCE

Как видно на рис. 4.5, кабель DTE, т.е. кабель, который обычно используется для подключения модуля CSU/DSU, не имеет перекрещенных линий передачи и приема. В кабеле DCE линии передачи и приема перекрещены, поэтому проводники, идущие от передающих контактов одного маршрутизатора, подключаются к принимающим контактам второго маршрутизатора, и наоборот, поэтому такое подключение остается прозрачным для маршрутизаторов. Поскольку маршрутизатор, к которому подключен кабель DCE, должен генерировать тактовую частоту, в конфигурацию этого маршрутизатора необходимо добавить команду `clock rate` для указания скорости обмена данными в соответствующем интерфейсе.

Скорость канала, предоставляемая телекоммуникационной компанией

Независимо от того, кто обеспечивает подключение (АТС, провайдер и др.), соответствующие компании не позволяют выбирать произвольную скорость обмена данными подключения WAN. Скорость двухточечного канала регламентируется стандартами.

На протяжении длительного периода времени телефонные компании всего мира зарабатывали гораздо больше на продаже услуг по передаче голоса, чем на продаже услуг по передаче данных. Однако в связи с развитием технологий в середине XX века телефонные компании разработали стандарт передачи голоса по цифровым каналам. Цифровая передача сигнала в сетях телефонных компаний благоприятствовала росту прибыльности услуг по передаче данных, в частности предоставлению выделенных линий. Кроме того, благодаря переходу на цифровую технологию передачи сигнала повысилась эффективность бизнеса телефонных компаний, поскольку она привела к снижению расходов на расширение сетей голосовой связи.

Базовый механизм, используемый для преобразования аналогового голосового сигнала в цифровой сигнал, называется ИКМ — *импульсно-кодовой модуляцией* (Pulse Code Modulation — PCM). В соответствии с этим механизмом для исходного аналогового голосового сигнала осуществляется выборка 8000 раз в секунду, а каждое значение должно представляться 8-битовым кодом. Таким образом, для представления 1 секунды голосового сигнала нужно 64000 битов. Когда телефонные компании начали разворачивать первые цифровые сети, они выбрали базовую скорость передачи, равную 64 Кбит/с, поскольку такой ширины полосы было достаточно для передачи одного голосового вызова. Для обозначения стандартной единичной линии со скоростью передачи 64 Кбит/с используется термин *цифровой сигнал уровня 0* (Digital Signal level 0 — DS0).

На сегодняшний день большинство телефонных компаний предоставляет выделенные линии со скоростью передачи, кратной 64 Кбит/с. В США стандарт *цифрового сигнала уровня 1* (Digital Signal level 1 — DS1) обозначает единичную линию, в которую входит 24 линии DS0 и один канал для служебной информации со скоростью 8 Кбит/с. Суммарная пропускная способность линии DS1, называемой также линией T1, составляет 1,544 Мбит/с. Предоставляются также линии *цифрового сигнала уровня 3* (Digital Signal level 3 — DS3), или линии T3, каждая из которых содержит 28 линий DS1. В других регионах мира используются собственные стандарты. Например, в Европе и Японии используются линии E1, содержащие 32 линии DS0, и линии E3, содержащие 16 линий E1.

ВНИМАНИЕ!

Объединение нескольких низкоскоростных линий и каналов в одну высокоскоростную линию или единый высокоскоростной канал (например, объединение 24 линий DS0 в одну линию T1) в общем случае называется *мультиплексированием с разделением времени* (Time-Division Multiplexing — TDM).

В табл. 4.2 перечислены некоторые стандартные скорости для распределенных сетей. В таблице представлены типы линий и соответствующие им стандарты передачи цифрового сигнала (например, DS1). Спецификации передачи сигналов определяют электрические сигналы, с помощью которых в линии представляется бинарный 0 или бинарная 1. Для сдачи экзамена ICND1 от читателя требуется понимать в общем механизмы, а также знать, что стоит за такими обозначениями, как T1 и E1.



Таблица 4.2. Стандартные скорости передачи данных в распределенных сетях

Название канала	Скорость передачи данных
DS0	64 Кбит/с
DS1 (T1)	1,544 Мбит/с (24 DS0 + 1 дополнительный канал на 8 Кбит/с)
DS3 (T3)	44,763 Мбит/с (28 DS1 + 1 дополнительный канал управления)
E1	2,048 Мбит/с (32 DS0)
E3	34,368 Мбит/с (16 E1 + 1 дополнительный канал управления)
J1 (Y1)	2,048 Мбит/с (32 DS0, стандарт Японии)

Выделенные каналы, которые обсуждались до настоящего времени в этой главе, формируют основу для предоставления услуг по созданию распределенных сетей, которыми пользуются многие современные предприятия. В следующем разделе речь идет о протоколах канального уровня, к использованию которых можно перейти после того, как два маршрутизатора соединены выделенной линией.

Уровень 2 модели OSI в двухточечных каналах распределенной сети

Используемые в двухточечных последовательных каналах протоколы WAN предназначены для обеспечения базовых функций передачи данных по каналу. К двум наиболее популярным протоколам канального уровня в двухточечных каналах относятся *высокоуровневый протокол управления каналом* (High-Level Data Link Control — HDLC) и *протокол двухточечного соединения* (Point-to-Point Protocol — PPP).

Протокол HDLC

Поскольку организация двухточечного канала сравнительно проста, протоколу HDLC не требуется выполнять большого объема работ. В частности, протокол HDLC должен определить, не содержат ли передаваемые по каналу данные ошибок; если ошибки обнаруживаются, протокол HDLC отбрасывает соответствующие фреймы (frame). Кроме того, протокол HDLC должен идентифицировать типы пакетов, находящихся во фреймах HDLC, чтобы получающее устройство могло определить тип пакета.

Для решения основной задачи передачи данных в канале, а также с целью обеспечения обнаружения ошибок и идентификации типа пакета протоколом HDLC определяется формат *фреймирования* (framing) данных. Заголовок (header) фрейма HDLC содержит поле адреса (Address) и поле типа протокола (Protocol Type), а концевик (trailer) — поле *контрольной последовательности фрейма* (Frame Check Sequence — FCS). На рис. 4.6 представлен формат как стандартного фрейма HDLC, так и собственного фрейма HDLC компании Cisco.

Хотя, как видно на рис. 4.6, протокол HDLC определяет 1-байтовое поле Address, в двухточечных каналах в его использовании нет особой необходимости. Этот тезис можно проиллюстрировать следующим примером. Допустим, автор пригласил на ланч своего друга Гарри. Если за столом нет никого, кроме Гарри и автора, у последнего нет особой необходимости предварять каждую фразу словами “Гарри, послушай” — Гарри и так знает, что автор обращается к нему и только к нему. Точно так же происходит и в распределенных сетях, соединенных двухточечным каналом, — маршрутизатор в первой точке канала знает, что имеется только один получатель данных, т.е. маршрутизатор во второй точке (на втором конце) канала. Поэтому на сегодняшний день использование поля Address лишено какого-либо смысла.

ВНИМАНИЕ!

В прошлом, когда телефонные компании предоставляли доступ к линиям с многоточечными подключениями, поле Address использовалось. Его необходимость была обусловлена тем, что к такой линии могло быть подключено более двух устройств.

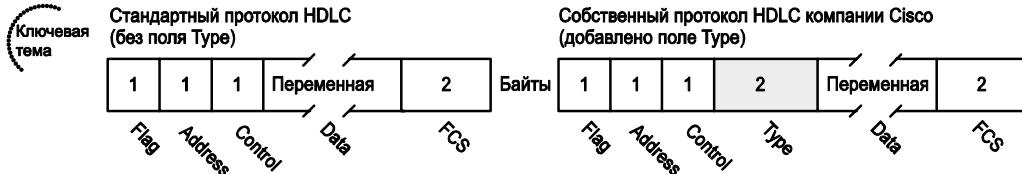


Рис. 4.6. Структура фрейма протокола HDLC

Обнаружение ошибок выполняется протоколом HDLC так же, как и в технологии Ethernet, т.е. с использованием поля контрольной суммы фрейма HDLC. Если полученный фрейм содержит ошибку, то, как и в случае аналогичной ситуации в сети Ethernet, устройство, получившее сбойный фрейм, отбрасывает его. Никаких механизмов восстановления поврежденных данных протоколом HDLC не предусмотрено.

Кроме того, как и в технологии Ethernet, на протокол HDLC также возлагается функция идентификации инкапсулированных данных. Когда маршрутизатор получает фрейм HDLC, нужен механизм, с помощью которого устройство могло бы выяснить тип пакета, заключенного в этот фрейм. «Фирменная» версия протокола HDLC, разработанная компанией Cisco, предусматривает для этих целей поле типа протокола, Protocol Type. Назначение этого поля как раз и заключается в идентификации типа пакета, содержащегося во фрейме. Значения 2-байтового поля Protocol Type, используемые компанией Cisco, полностью соответствуют значениям аналогичного поля технологии Ethernet.

Поскольку в оригинальной версии протокола HDLC поле Protocol Type отсутствует, компании Cisco пришлось ввести его в конце 1980-х годов, чтобы обеспечить поддержку первых последовательных каналов, соединяющих маршрутизаторы Cisco на заре деятельности компании. Таким образом, изменив стандартную спецификацию протокола HDLC, компания Cisco создала собственную версию этого протокола. Поэтому реализация протокола HDLC, используемая компанией Cisco, не будет работать при соединении маршрутизатора Cisco с маршрутизаторами других производителей.

Таким образом, протокол HDLC очень прост, что вполне логично объясняется узким кругом задач, которые нужно решать протоколам канального уровня.

Протокол PPP

Исторически сложилось так, что первым протоколом канального уровня, который был разработан Международным союзом телекоммуникаций (International Telecommunications Union — ITU), ранее известным как Международный консультативный комитет по телеграфии и телефонии (Consultative Committee for International Telephone and Telegraphy — CCITT), был протокол HDLC. Со временем группа IETF (Internet Engineering Task Force — Проблемная группа проектирования Интернета) осознала необходимость разработки дополнительного протокола канального уровня для использования между маршрутизаторами, соединенными двухточечным каналом. В документе RFC 1661 (1994 г.) группа IETF определила спецификации протокола двухточечного соединения (Point-to-Point Protocol — PPP).

По большому счету, работа протокола PPP строится так же, как и работа протокола HDLC. В частности, структура фрейма протокола PPP соответствует структуре фрейма собственной версии протокола HDLC компании Cisco. Как и в протоколе

HDLC, в протоколе PPP предусмотрено поле Address, в использовании которого также нет особой необходимости. Точно так же как и протокол HDLC, протокол PPP просто отбрасывает ошибочные фреймы, которые не проходят проверку поля FCS. Кроме того, протокол PPP использует 2-байтовое поле Protocol Type. Однако, поскольку поле Protocol Type является стандартным компонентом фрейма PPP, устройства любого производителя, реализующие стандартный протокол PPP, без проблем смогут работать с продуктами другого производителя, также реализующими этот протокол. Поэтому при подключении маршрутизатора Cisco к маршрутизатору другого производителя с помощью двухточечного последовательного канала протокол PPP — это единственный выбор в качестве протокола канального уровня.

Поскольку спецификации протокола PPP создавались гораздо позже оригинальных спецификаций протокола HDLC, разработчики PPP включили в описание протокола много дополнительных возможностей, которые отсутствовали на тот момент в других протоколах канального уровня для распределенных сетей. Именно благодаря этому фактору протокол PPP стал наиболее развитым из всех протоколов WAN канального уровня и, как следствие, наиболее популярным.

Резюме по технологиям распределенных сетей

При описании технологий, используемых для организации выделенных линий, которые представляют собой двухточечные каналы распределенных сетей, а также соответствующих протоколов канального уровня применяются дополнительные термины и концепции, выходящие за рамки аналогичных технологий, используемых для организации локальных сетей (табл. 4.3).

Таблица 4.3. Терминология, используемая для описания технологий распределенных сетей



Термин	Определение
Синхронный (synchronous), синхронизация (synchronization)	Процесс упорядочения по времени потока битов. На практике сводится к тому, что одно устройство, подключенное к последовательному каналу, пытается использовать ту же скорость, с которой работает второе устройство, подключенное к этому же каналу. Однако, отслеживая переходы между уровнями напряжения в канале, каждое из устройств может обнаруживать небольшие отклонения в скорости и соответствующим образом подстраивать свою скорость работы
Источник тактовой частоты (clock source)	Устройство, по которому подстраивают свою скорость работы другие устройства, подключенные к синхронизированному каналу
Модуль CSU/DSU	Модуль обслуживания канала/модуль обработки данных (Channel Service Unit/Data Service Unit). В США используется в цифровых каналах для создания интерфейса с оборудованием телефонной компании. Обычно последовательный интерфейс маршрутизатора подключается к модулю CSU/DSU с помощью короткого кабеля. Модуль CSU/DSU, в свою очередь, подключается к линии, предоставленной АТС, а на другом конце этой линии создается аналогичная конфигурация

Окончание табл. 4.3

Термин	Определение
Телекоммуникационная или телефонная компания (Telco)	Территориальное подразделение телефонной компании или оператор телефонной связи
Выделенный четырехжильный канал (four-wire circuit)	Четырехжильный кабельный канал связи, проложенный АТС, содержащий две витых пары. Каждая пара используется для пересылки данных в одном направлении. Таким образом, четырехжильный канал обеспечивает возможность дуплексной коммуникации
Канал T1	Выделенный канал, позволяющий передавать данные на скорости 1,544 Мбит/с. Используется в США
Канал E1	Подобен T1, но для Европы. Обеспечивает передачу данных на скорости 2,048 Мбит/с и содержит 32 канала с пропускной способностью 64 Кбит/с каждый

Кроме того, при изучении материала, связанного с технологиями распределенных сетей, помните, что двухточечные выделенные каналы, описанные в данной главе, могут обозначаться следующими терминами:



Перечень синонимов для термина *двуточечный выделенный канал*

выделенная линия (leased line); выделенный канал (leased circuit); линия (link); последовательная линия (serial link); двухточечный канал (point-to-point link); канал (circuit).

Технология Frame Relay и службы с коммутацией пакетов

Помимо выделенных линий, провайдеры могут предоставлять доступ к распределенным сетям еще одного класса, которые можно назвать *службами с коммутацией пакетов* (packet-switching service). Как и в случае выделенного канала, при предоставлении службы с коммутацией пакетов у потребителя имеется физическое подключение к WAN. Однако при этом компания-потребитель получает возможность подключить к службе с коммутацией пакетов не один, а несколько маршрутизаторов. Каждый из маршрутизаторов подключается к службе с коммутацией пакетов с помощью одного последовательного канала. После подключения маршрутизатор получает возможность отправлять пакеты всем остальным маршрутизаторам — что-то вроде того, как все устройства, подключенные к концентратору или коммутатору Ethernet, могут обмениваться данными непосредственно друг с другом.

Сегодня наиболее популярными являются два типа служб с коммутацией пакетов — технология Frame Relay (иногда называемая ретрансляцией фреймов) и технология ATM (Asynchronous Transfer Mode — асинхронный режим передачи). Поскольку наибольшее распространение из этих двух служб получила технология Frame Relay, в данном разделе рассматриваются основные концепции организации служб с коммутацией пакетов, а также основы технологии Frame Relay.

Преимущества коммутации пакетов с точки зрения масштабирования

Когда нужно подключить несколько дистанционных площадок к распределенной сети, это можно сделать с помощью двухточечных каналов, устанавливая по паре мар-

шлюзов на каждый канал. Однако альтернативный подход к организации распределенной сети, основанный на технологии Frame Relay, предоставляет определенные преимущества по сравнению с двухточечными каналами, которые особенно заметны в тех случаях, когда с помощью распределенной сети нужно связать между собой несколько дистанционных площадок. Для ознакомления читателя с технологией Frame Relay в этом разделе уделено внимание некоторым ключевым преимуществам данной технологии перед технологией, основанной на использовании выделенных линий. Одно из этих преимуществ легко понять, внимательно изучив рис. 4.7.

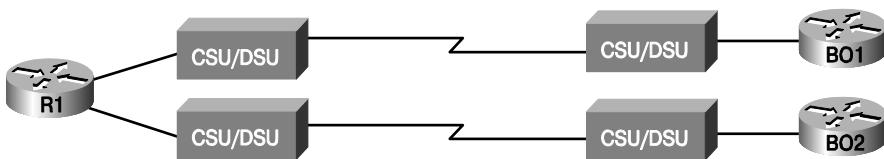


Рис. 4.7. Две выделенные линии для двух дистанционных площадок

На рис. 4.7 показано, что главная площадка соединена с двумя дистанционными площадками. Маршрутизатору главной площадки потребуются два отдельных последовательных интерфейса и два отдельных модуля CSU/DSU. Если площадок всего две, это не составляет большой проблемы. Но что будет в том случае, когда количество дистанционных подразделений компании вырастет до 10? А до 100? А если до 500? Для организации каждого дополнительного двухточечного канала центральному маршрутизатору нужен дополнительный последовательный интерфейс и отдельный модуль CSU/DSU. Как легко представить, если счет площадок пойдет на сотни, главной компании придется обзавестись десятками маршрутизаторов с несколькими интерфейсами каждый, а также выделить достаточно много места для размещения стоек с этими маршрутизаторами и модулями CSU/DSU.

А теперь читатель может представить, как сотрудник отдела сбыта телефонной компании, узнав, что пользователь в своей компании намеревается установить вторую выделенную линию, как показано на рис. 4.7, сообщает ему следующее.

“Мы можем вместо второй выделенной линии предложить вам канал Frame Relay. Это позволит обойтись одним последовательным интерфейсом на центральном маршрутизаторе и одним модулем CSU/DSU. Даже если количество подключаемых площадок достигнет сотни, вам понадобится лишь два-три последовательных интерфейса для центрального устройства, да и то лишь для расширения полосы пропускания. И, кстати, поскольку ваша выделенная линия работает на скорости 128 Кбит/с, мы даем гарантию, что на этой же скорости вы сможете обмениваться данными с каждой площадкой. Но на самом деле мы расширим канал для центрального маршрутизатора до T1 (т.е. до 1,544 Мбит). Поэтому, если трафик с какой-то площадки будет превышать 128 Кбит/с, вы этого даже не заметите! Если пропускная способность канала позволит, весь дополнительный трафик будет идти без задержек и это не будет вам стоить ни цента! Кстати, о стоимости. Я уже говорил вам, что канал Frame Relay в любом случае вам обойдется дешевле, чем аренда выделенной линии?”

Итак, основные доводы “за” понятны: Frame Relay дешевле, работает как минимум так же быстро, как уже имеющийся канал (а потенциально может работать быстрее), а также позволит сэкономить деньги в будущем при подключении новых площадок. Поэтому читатель, оказавшись в подобной ситуации, скорее всего, по-

старается побыстрее подписать договор на подключение по технологии Frame Relay, пока предложение остается в силе. Ситуация выглядит довольно надуманной? В общем-то, да. Но, тем не менее, стоимость подключения Frame Relay, а также экономия при масштабировании, в сравнении с аналогичными показателями для выделенных линий, весьма значительны. Именно поэтому многие компании, особенно в 90-х годах, перешли с выделенных линий на Frame Relay, что привело к возникновению обширной инфраструктуры установленных сетей Frame Relay в наши дни. Дальше читатель узнает, как работает технология Frame Relay, а также поймет, за счет чего эта технология обеспечивает все функции, перечисленные выше нашим вымышленным персонажем.

Основы технологии Frame Relay

Технология Frame Relay, на основе которой создаются распределенные сети, представляет больше возможностей, чем технологии, обеспечивающие работу аналогичных сетей с двухточечными каналами. Однако своего рода платой за это является более высокая сложность протоколов Frame Relay. Сети Frame Relay являются сетями со множественным доступом (multiaccess network). Это означает, что к такой сети можно подключить более двух устройств (примерно так же, как и в локальных сетях). Понятно, что задача обеспечения обслуживания более двух устройств неизбежно требует усложнения протоколов. На рис. 4.8 показаны некоторые базовые компоненты, необходимые для организации подключения к сети Frame Relay.

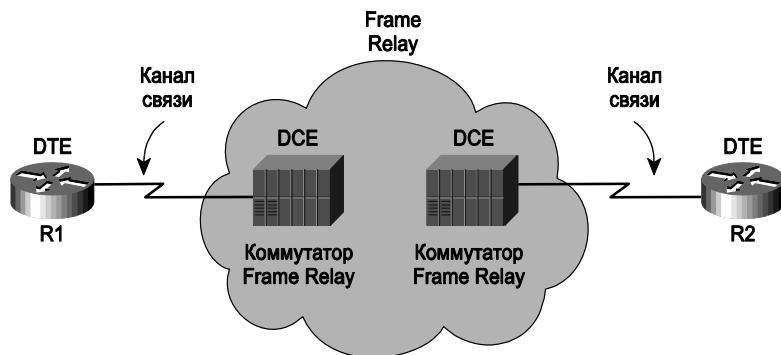


Рис. 4.8. Компоненты подключения к сети Frame Relay

На рис. 4.8 показано, что технология Frame Relay использует те же средства уровня 1, которые применяются для организации выделенных двухточечных каналов. При подключении к службе Frame Relay выделенные каналы связывают каждый из маршрутизаторов с ближайшим коммутатором Frame Relay. В терминах технологии Frame Relay эти каналы называются *канал связи* (access link). Каналы связи работают на тех же скоростях и используют те же стандарты обработки сигналов, что и выделенные двухточечные каналы. Однако в технологии Frame Relay выделенные линии связывают между собой не маршрутизаторы, а каждый из маршрутизаторов с коммутатором Frame Relay.

Различие между технологией Frame Relay и технологией, основанной на выделенных двухточечных каналах, состоит в том, что контроль фреймов данных, пере-

сылаемых маршрутизатором, осуществляет оборудование телефонной компании. В заголовке каждого фрейма Frame Relay содержится адресное поле DLCI (Data Link Connection Identifier — *идентификатор подключения канального уровня*). Коммутатор WAN, основываясь на идентификаторе DLCI, направляет по сети провайдера передаваемые фреймы, пока они не достигнут нужного маршрутизатора на дистанционной площадке.

ВНИМАНИЕ!

Заголовок и концевик фрейма Frame Relay определяются *протоколом доступа к каналу связи Frame Relay* (Link Access Procedure Frame — LAPF).

Поскольку оборудование телефонной компании может направлять один фрейм на одну дистанционную площадку, а другой — на другую, технологию Frame Relay рассматривают как одну из форм *коммутации пакетов* (packet switching). Этот термин означает, что решение, куда направить очередной пакет данных, поступивший в сеть провайдера, принимает провайдер, коммутируя тем самым один пакет одному устройству, следующий пакет — другому и т.д. Однако протоколы Frame Relay больше всего напоминают протоколы уровня 2 модели OSI, а устройства, работающие на уровне 2, отправляют битовые последовательности, которые обычно называют *фреймами* (frame). Поэтому технологию Frame Relay также называют *службой с коммутацией фреймов* (frame-switching service), что более корректно, поскольку “коммутация пакетов” — это более общий термин.

В службах с коммутацией пакетов и службах с коммутацией фреймов понятия DTE и DCE немного отличаются. В частности, в технологии Frame Relay коммутаторы Frame Relay называются устройствами DCE, а оборудование потребителя (в данном случае — маршрутизаторы) — устройствами DTE. Иными словами, устройство DCE — это устройство, обеспечивающее работу службы, а устройство DTE — это устройство, требующее работы службы с коммутацией фреймов. В то же время, поскольку тактовую частоту маршрутизатору обеспечивает модуль CSU/DSU, то с точки зрения уровня 1 модуль CSU/DSU по-прежнему остается устройством DCE, а маршрутизатор — устройством DTE. Таким образом, имеет место различное применение одних и тех же терминов.

Если на рис. 4.8 были показаны физические и логические компоненты подключения к сети Frame Relay, то на рис. 4.9 представлено *сквозное* (end-to-end) подключение, ассоциируемое с *виртуальными каналами* (Virtual Circuit — VC).



Рис. 4.9. Компоненты виртуального соединения Frame Relay

Логический маршрут, по которому проходит каждый фрейм на пути от одного маршрутизатора к другому, называется *виртуальным каналом Frame Relay*. На рис. 4.9 показано одно виртуальное соединение в виде пунктирной линии, соединяющей два маршрутизатора. Обычно всю необходимую предварительную настройку виртуального

канала выполняет провайдер. Такие виртуальные соединения называются *постоянными виртуальными каналами* (Permanent Virtual Circuit — PVC). Когда маршрутизатор должен отправить пакет второму маршрутизатору, он инкапсулирует пакет уровня 3 в заголовок и концевик Frame Relay, а затем отправляет полученный фрейм. При этом маршрутизатор использует содержащийся в заголовке адрес Frame Relay, называемый идентификатором DLCI, который, в свою очередь, идентифицирует для провайдера корректное виртуальное соединение. Такая схема работы позволяет коммутаторам доставить фрейм до дистанционного маршрутизатора, игнорируя детали пакета уровня 3, а основываясь лишь на анализе заголовка и концевика Frame Relay. Как читатель, должно быть, помнит, в двухточечных последовательных каналах провайдер пересыпает фреймы по физическому соединению двух маршрутизаторов. Нечто подобное происходит и в сетях Frame Relay, с той лишь разницей, что в этом случае провайдер пересыпает фреймы по виртуальному соединению между двумя устройствами.

Технология Frame Relay, помимо упрощения использования двухточечных выделенных линий, обладает другими серьезными достоинствами. Основное из них напрямую связано с возможностью получения виртуальных соединений. Рассмотрим, например, рис. 4.10, на котором показано использование технологии Frame Relay вместо трех двухточечных выделенных каналов.

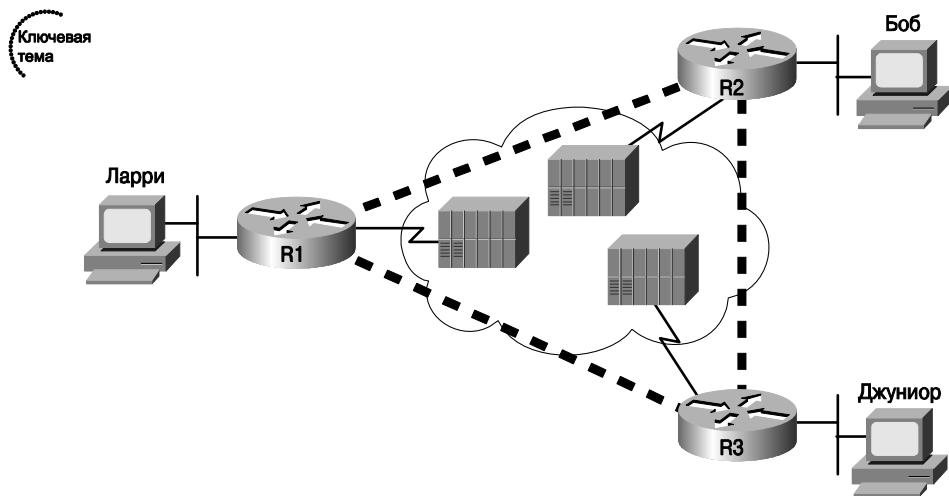


Рис. 4.10. Типичная сеть Frame Relay, объединяющая три площадки

Как видно на рис. 4.10, технология Frame Relay позволяет создать логический маршрут (т.е. виртуальное соединение) между двумя устройствами DTE Frame Relay. Виртуальное соединение работает в данном случае подобно двухточечному каналу, но при этом не требует отдельного физического канала, поскольку оно виртуальное. Например, на рис. 4.10 показано, что центральный маршрутизатор инициирует два виртуальных соединения — одно, оканчивающееся на маршрутизаторе сверху, и второе — на маршрутизаторе снизу на схеме. Центральный маршрутизатор может направить трафик непосредственно на любой из двух других маршрутизаторов, просто переслав его соответствующему виртуальному соединению. При этом следует отметить, что у маршрутизатора имеется лишь один физический канал связи к сети Frame Relay.

Все виртуальные соединения совместно используют один и тот же канал связи и одну и ту же сеть Frame Relay. Например, оба виртуальных соединения центрального маршрутизатора совместно используют один и тот же канал связи. Таким образом, в больших распределенных сетях, в которых много площадок, нужно подключить к центральной площадке только один физический канал связи, чтобы соединить маршрутизатор главной площадки с сетью Frame Relay. Если бы та же задача пришлось решать с помощью двухточечных каналов, потребовалось бы прокладывать отдельную физическую линию, приобретать отдельный модуль CSU/DSU и воздействовать отдельный последовательный интерфейс на маршрутизаторе для каждого такого канала. Поэтому технология Frame Relay позволяет расширять распределенную сеть, практически не используя дополнительного оборудования.

Еще одной особенностью технологии Frame Relay является то, что у каждого провайдера Frame Relay имеется много потребителей, использующих одну и ту же сеть Frame Relay провайдера. Поначалу потребители выделенных линий отказывались переходить на технологию Frame Relay, поскольку опасались, что в режиме конкурентной работы с другими потребителями этого же провайдера им придется сталкиваться с недостаточной пропускной способностью сети. Чтобы потребители избавились от этих опасений, в технологии Frame Relay реализована концепция *согласованной скорости передачи* (Committed Information Rate — CIR). Для каждого виртуального соединения устанавливается показатель CIR. С его помощью провайдер гарантирует, что то или иное конкретное виртуальное соединение будет работать на скорости, не меньшей, чем соответствующее значение CIR. Иными словами, показатель CIR виртуального соединения можно рассматривать в качестве аналога ширины полосы или тактовой частоты двухточечного канала, с тем лишь различием, что показатель CIR — это минимально допустимое значение. На практике нередко потребители могут работать на скорости, большей, чем это установлено параметром CIR для канала.

Даже в случае с сетью, объединяющей всего три площадки, как показано на рис. 4.10, эксплуатация сети в случае использования технологии Frame Relay обходится дешевле, чем эксплуатация сети, основанной на использовании двухточечных каналов. Что уж говорить о значительно более обширных сетях, объединяющих десятки и даже сотни площадок, особенно с учетом того, что каждая из площадок должна иметь доступ ко всем остальным площадкам. Для получения такой сети между 100 площадками с помощью выделенных каналов пришлось бы проложить 4950 выделенных линий! Кроме того, на каждом маршрутизаторе понадобилось бы 99 последовательных интерфейсов. Сравните такую структуру теперь с сетью аналогичной протяженности, основанной на технологии Frame Relay. В этом случае понадобится проложить всего 100 каналов связи к локальным коммутаторам Frame Relay (1 канал на каждый маршрутизатор). Все необходимые 4950 соединений будут реализованы в виде виртуальных соединений, и при этом в каждом маршрутизаторе достаточно будет всего одного последовательного интерфейса. В результате сеть Frame Relay имеет более простую в реализации топологию, обходится провайдеру дешевле, а также эффективнее использует возможности сети провайдера. Как нетрудно догадаться, именно поэтому сети Frame Relay оказываются более выгодным предложением и для потребителей. В тех случаях, когда нужно развернуть распределенную сеть между множеством площадок, технология Frame Relay значительно дешевле в реализации, чем технология, основанная на выделенных каналах.

Подготовка к экзамену

Повторите все ключевые темы

Повторите все ключевые темы данной главы, помеченные на полях пиктограммой “Ключевая тема”. Ключевые темы и соответствующие им страницы перечислены в табл. 4.4.

Таблица 4.4. Ключевые темы главы 4

Элемент	Описание	Страница
Рис. 4.3	Двухточечная выделенная линия: компоненты и терминология	118
Табл. 4.2	Стандартные скорости передачи данных в распределенных сетях	124
Рис. 4.6	Структура фрейма протокола HDLC	126
Табл. 4.3	Терминология, используемая для описания технологий распределенных сетей	127
Абзац	Перечень синонимов для термина двухточечный выделенный канал	128
Рис. 4.10	Типичная сеть Frame Relay, объединяющая три площадки	132

Заполните таблицы и списки по памяти

Распечатайте приложение М (Appendix L) с компакт-диска или его раздел, относящийся к этой главе, и заполните таблицы и списки по памяти. В приложении Н (Appendix M) приведены заполненные таблицы и списки для самоконтроля.

Ключевые термины

Дайте определения перечисленных ниже терминов и проверьте правильность их написания в списке терминов:

канал связи (access link), прямое лабораторное подключение (back-to-back link), тактовая частота (clocking), устройство DTE (уровень 1) (DTE (Layer 1)), модуль CSU/DSU (CSU/DSU), устройство DCE (уровень 1) (DCE (Layer 1)), DS0, DS1, технология Frame Relay (Frame Relay), протокол HDLC (HDLC), выделенная линия (leased line), коммутация пакетов (packet switching), протокол PPP (PPP), последовательный кабель (serial cable), синхронный (synchronous), канал T1 (T1), виртуальный канал (virtual circuit).

В этой главе...

- **Обзор функций сетевого уровня.** Представлены концепции маршрутизации, логической адресации и протоколов маршрутизации.
- **IP-адресация.** Объясняются основы 32-битовых IP-адресов; основное внимание уделено тому, как они способствуют процессу маршрутизации.
- **Маршрутизация IP.** Объясняется, как узлы и маршрутизаторы принимают решения о перенаправлении пакетов.
- **Протоколы маршрутизации IP.** Объясняются принципы, которые лежат в основе того, как протоколы маршрутизации заполняют таблицы маршрутизации каждого маршрутизатора.
- **Утилиты сетевого уровня.** Представлено несколько других функций, связанных с процессом доставки пакетов.

ГЛАВА 5

Основы адресации и маршрутизации IPv4

Физический уровень модели OSI (уровень 1) определяет то, как передавать биты по определенному типу физической сети. Канальный уровень модели OSI (уровень 2) определяет фреймирование, адресацию, обнаружение ошибок и правила использования физической передающей среды. Несмотря на то что эти уровни важны, ни один из них не определяет то, как данные будут передаваться между устройствами, расположенными на большом расстоянии друг от друга и соединенными множеством различных физических сетей.

В этой главе описываются функции и назначение сетевого уровня модели OSI (уровня 3): сквозная доставка данных между двумя компьютерами. Независимо от типа физической сети, к которой подключен каждый конечный компьютер, и типов физических сетей, которые используются между этими компьютерами, сетевой уровень определяет, как перенаправлять (или маршрутизировать) данные между этими компьютерами.

В этой главе описываются основные принципы того, как сетевой уровень маршрутизирует пакеты данных от одного компьютера к другому. После краткого обзора основ в этой главе более подробно рассматривается сетевой уровень TCP/IP, включая IP-адресацию (которая обеспечивает возможности эффективной маршрутизации), маршрутизацию IP (собственно процесс перенаправления), протоколы маршрутизации IP (процесс, благодаря которому маршрутизаторы изучают маршруты), а также некоторые другие важные особенности сетевого уровня.

Контрольные вопросы: знаете ли вы уже темы главы

Этот раздел предназначен для того, чтобы читатель мог предварительно оценить свои знания и решить, нужно ли ему читать главу целиком. Если ответы на двенадцать из тринадцати вопросов даны правильно, можно сразу же перейти к последнему разделу “Подготовка к экзамену”. Основные темы этой главы и предварительных контрольных вопросов перечислены в табл. 5.1. Отвечая на контрольные вопросы и используя таблицу, читатель сможет достаточно точно определить свои знания в той или иной области. Ответы на вопросы приведены в приложении А.

Таблица 5.1. Темы контрольных вопросов

Основная тема	Номера вопросов
Обзор функций сетевого уровня	1–3
IP-адресация	4–8
Маршрутизация IP	9, 10
Протоколы маршрутизации IP	11
Утилиты сетевого уровня	12, 13

1. Что из перечисленного ниже является функциями протоколов третьего уровня модели OSI? (Выберите несколько ответов.)
 - а) Логическая адресация (logical addressing).
 - б) Физическая адресация (physical addressing).
 - в) Выбор пути (path selection).
 - г) Арбитраж (arbitration).
 - д) Восстановление после ошибок (error recovery).
2. Предположим, компьютер ПК1 должен отправить данные компьютеру ПК2 и компьютеры ПК1 и ПК2 отделены друг от друга несколькими маршрутизаторами. Укажите наибольший блок данных, который передается от ПК1 к ПК2. (Выберите несколько ответов.)
 - а) Фрейм (frame).
 - б) Сегмент (segment).
 - в) Пакет (packet).
 - г) L5 PDU.
 - д) L3 PDU.
 - е) L1 PDU.
3. Представьте себе сеть с двумя маршрутизаторами, которые соединены с помощью последовательного двухточечного канала HDLC. Каждый маршрутизатор поддерживает сеть Ethernet. Компьютер ПК1 подключен к сети Ethernet первого маршрутизатора (Router1), а ПК2 подключен к сети Ethernet второго маршрутизатора (Router2). Какое утверждение справедливо при передаче данных от ПК1 к ПК2?
 - а) Маршрутизатор Router1 удаляет из фрейма, полученного от ПК1, заголовок и концевик Ethernet, которые не будут использоваться.
 - б) Маршрутизатор Router1 инкапсулирует фрейм Ethernet в заголовок HDLC и отправляет этот фрейм маршрутизатору Router2, который выделяет фрейм Ethernet для перенаправления к ПК2.
 - в) Маршрутизатор Router1 удаляет из фрейма, полученного от ПК1, заголовок и концевик Ethernet, который восстанавливается маршрутизатором Router2 перед отправкой данных компьютеру ПК2.
 - г) Маршрутизатор Router1 удаляет заголовки Ethernet, IP и TCP и перестраивает соответствующие заголовки перед отправкой пакета маршрутизатору Router2.
4. Какие из перечисленных ниже адресов являются правильными IP-адресами класса C, которые можно назначать хостам?
 - а) 1.1.1.1
 - б) 200.1.1.1
 - в) 128.128.128.128
 - г) 224.1.1.1
 - д) 223.223.223.255

5. Укажите диапазон значений для первого октета сетей IP класса А.
- а) от 0 до 127
 - б) от 0 до 126
 - в) от 1 до 127
 - г) от 1 до 126
 - д) от 128 до 191
 - е) от 128 до 192
6. Компьютеры ПК1 и ПК2 находятся в двух разных сетях Ethernet, разделенных маршрутизатором IP. IP-адрес ПК1 10.1.1.1 в подсети не используется. Какой из следующих адресов можно использовать для ПК2? (Выберите несколько ответов.)
- а) 10.1.1.2
 - б) 10.2.2.2
 - в) 10.200.200.1
 - г) 9.1.1.1
 - д) 225.1.1.1
 - е) 1.1.1.1
7. Сколько IP-адресов, которые можно назначить хостам, может содержать сеть класса В?
- а) 16 777 214
 - б) 16 777 216
 - в) 65 536
 - г) 65 536
 - д) 65 534
 - е) 65 532
 - ж) 32 768
 - з) 32 766
8. Сколько IP-адресов, которые можно назначить хостам, может содержать сеть класса С?
- а) 65 534
 - б) 65 532
 - в) 32 768
 - г) 32 766
 - е) 256
 - ж) 254
9. Какие из следующих адресов обычно использует маршрутизатор, принимая решение о маршрутизации пакетов TCP/IP?
- а) MAC-адрес получателя.

- б) MAC-адрес отправителя.
в) IP-адрес получателя.
г) IP-адрес отправителя.
е) MAC- и IP-адреса получателя.
10. Какое из приведенных ниже утверждений справедливо для подключенного к локальной сети хоста TCP/IP и его решениях о маршрутизации IP? (Выберите несколько ответов.)
- а) Хост всегда отправляет пакеты своему стандартному шлюзу.
б) Хост всегда отправляет пакеты своему стандартному шлюзу, если IP-адрес получателя находится в сети IP другого класса.
в) Хост всегда отправляет пакеты своему стандартному шлюзу, если IP-адрес получателя находится в другой подсети.
г) Узел всегда отправляет пакеты своему стандартному шлюзу, если IP-адрес получателя находится в той же подсети.
11. Какие из перечисленных ниже функций являются функциями протокола маршрутизации? (Выберите несколько ответов.)
- а) Уведомление соседних маршрутизаторов об известных маршрутах.
б) Изучение маршрутов для подсетей, непосредственно подключенных к маршрутизатору.
в) Изучение маршрутов, представленных маршрутизатору соседними маршрутизаторами, и помещение этих маршрутов в таблицу маршрутизации.
г) Перенаправление пакетов IP на основании IP-адреса получателя пакета.
12. Какие из перечисленных ниже протоколов позволяют клиентскому ПК определить IP-адрес другого компьютера по имени этого компьютера?
- а) ARP.
б) RARP.
в) DNS.
г) DHCP.
13. Какой из перечисленных протоколов позволяет клиентскому компьютеру запрашивать назначение ему IP-адреса, а также узнавать адрес своего стандартного шлюза?
- а) ARP.
б) RARP.
в) DNS.
г) DHCP.

Основные темы

Протоколы, эквивалентные третьему уровню модели OSI, определяют то, как пакеты доставляются от компьютера, который их создал, к компьютеру, который должен их получить. Для достижения этой цели протоколы сетевого уровня модели OSI определяют следующие функции.

- **Маршрутизация** (routing). Процесс перенаправления пакетов (блоков PDU третьего уровня).
- **Логическая адресация** (logical addressing). Адреса, которые можно использовать независимо от типа применяемых физических сетей, при условии, что каждое устройство (как минимум) получает один адрес. Логическая адресация позволяет процессу маршрутизации идентифицировать отправителя и получателя пакета.
- **Протокол маршрутизации** (routing protocol). Протокол, который помогает маршрутизаторам динамически изучать группы адресов в сети, что, в свою очередь, позволяет правильно работать процессу маршрутизации (перенаправления).
- **Другие утилиты.** Сетевой уровень также опирается на другие утилиты. Для TCP/IP эти утилиты включают в себя *систему доменных имен* (Domain Name System — DNS), *протокол динамической конфигурирования хоста* (Dynamic Host Configuration Protocol — DHCP), *протокол преобразования адресов* (Address Resolution Protocol — ARP) и утилиту эхо-запросов ping.

ВНИМАНИЕ!

Термин *выбор пути* (path selection) иногда используется как синоним термина протокол маршрутизации, иногда как синоним термина маршрутизация (перенаправление) пакетов, а иногда для упоминания обеих функций.

Эта глава начинается с обзора маршрутизации, логической адресации и протоколов маршрутизации. Далее более подробно описывается специфика сетевого уровня TCP/IP (в модели TCP/IP он называется уровнем *межсетевого взаимодействия* (internetwork layer)). В частности, здесь рассматриваются темы IP-адресации, маршрутизации, протоколов маршрутизации и утилит сетевого уровня.

Обзор функций сетевого уровня

Протокол, который определяет маршрутизацию и логическую адресацию, считается протоколом сетевого уровня (или уровня 3). Модель OSI определяет уникальный протокол уровня 3, который называется *сетевой службой без установления соединения* (Connectionless Network Services — CLNS), но, как это обычно бывает с протоколами OSI, он не часто встречается в сетях в настоящее время. Сейчас встречается множество других протоколов сетевого уровня, таких как *протокол Интернета* (Internet Protocol — IP), *протокол межсетевого обмена пакетами Novell* (Novell Internetwork Packet Exchange — IPX) или *протокол доставки дейтаграмм AppleTalk* (AppleTalk Datagram Delivery Protocol — DDP). В наши дни единственным широко используемым протоколом уровня 3 является протокол сетевого уровня TCP/IP, а именно протокол IP.

Главная задача протокола IP заключается в перенаправлении данных (пакетов) от хоста отправителя к хосту получателя. Поскольку в сети может потребоваться перенаправление большого количества пакетов, процесс маршрутизации IP весьма прост. Протокол IP не требует накладных расходов на доставку подтверждений или сообщений перед отправкой пакета. Протокол IP — это протокол без организации соединения. Он пытается доставить каждый пакет, но если маршрутизатор или процесс IP хоста не может доставить пакет, то этот пакет отбрасывается без возможности устранения ошибок. Цель протокола IP заключается в доставке пакетов с минимально возможными затратами на каждый пакет, что позволяет передавать большие пакеты данных. Другие протоколы осуществляют некоторые другие вспомогательные сетевые функции. Например, *протокол управления передачей* (Transmission Control Protocol — TCP), который подробно описывается в главе 6, обеспечивает восстановление после ошибок и повторную передачу потерянных данных, а протокол IP этого не делает.

Маршрутизация IP опирается на структуру и содержание IP-адреса, а IP-адресация разрабатывалась с учетом маршрутизации IP. Первый главный раздел этой главы начинается с ознакомления с маршрутизацией IP. Здесь также рассматриваются некоторые понятия IP-адресации, а потом основы IP-адресации.

Маршрутизация

Маршрутизация (перенаправление) фокусируется на сквозной логике перенаправления данных. На рис. 5.1 показан простой пример маршрутизации. Иллюстрируемая логика сравнительно проста. Чтобы отправить данные компьютеру ПК2, компьютер ПК1 должен что-то отправить маршрутизатору R1, который отправляет это маршрутизатору R2, потом маршрутизатору R3 и, наконец, компьютеру ПК2. Однако логика каждого устройства на пути пакетов несколько отличается.

Логика ПК1: отправка данных соседнему маршрутизатору

В примере на рис. 5.1 компьютер ПК1 должен передать некоторые данные компьютеру ПК2. Поскольку ПК2 находится не в той же сети Ethernet, что и ПК1, компьютер ПК1 должен отправить пакет маршрутизатору, который подключен к его сети Ethernet. Отправитель отсылает по среде передачи канальный фрейм соседнему маршрутизатору; в область данных этого фрейма включен пакет. В заголовке канального уровня фрейма используется адресация канального уровня (уровня 2), чтобы гарантировать, что соседний маршрутизатор получит этот фрейм.

Здесь важно отметить то, что компьютер, создающий данные, знает о сети не много — он знает только, как отправить данные соседнему маршрутизатору. Используя аналогию с обычной почтой, можно сказать, что отправитель должен знать только то, как доставить данные в местное почтовое отделение, и не более. Аналогично компьютер ПК1 должен знать только то, как доставить пакет маршрутизатору R1. Весь остальной путь, по которому отправляются пакеты к компьютеру ПК2, ему не известен.

Логика R1 и R2: маршрутизация данных в сети

Маршрутизаторы R1 и R2 в данном случае используют один общий процесс для маршрутизации пакета. В *таблице маршрутизации* (routing table) для любого определенного протокола сетевого уровня содержится список *групп* (groupings) адресов сетевого уровня. Вместо одной записи для каждого отдельного сетевого адреса получа-

теля в таблице маршрутизации существует одна запись для группы адресов. Маршрутизатор сравнивает содержащийся в пакете адрес (сетевого уровня) получателя с записями в таблице маршрутизации и находит совпадение. Совпадающая запись таблицы маршрутизации сообщает маршрутизатору, куда следует перенаправить пакет дальше. Эта базовая логика показана на рис. 5.1.

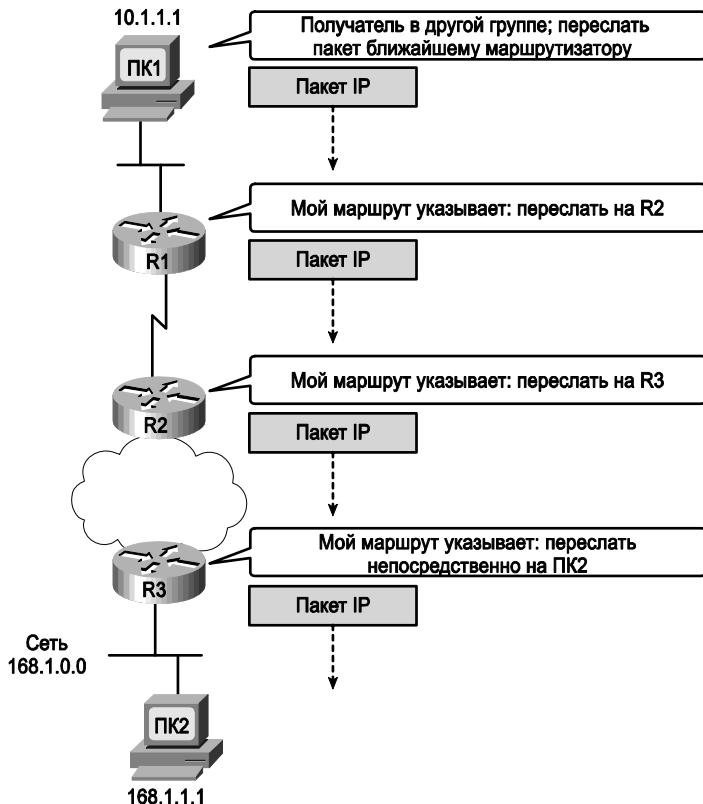


Рис. 5.1. Логика маршрутизации: компьютер ПК1 отправляет данные компьютеру ПК2

Концептуально группировка адресов сетевого уровня подобна системе почтовых индексов США. Все, кто живет в одной местности, имеют одинаковый почтовый индекс. Сортировщики на почте смотрят только на почтовые коды, игнорируя остальную часть адресов. Аналогично на рис. 5.1 все устройства в этой сети, имеющие IP-адреса, которые начинаются с 168.1, находятся в той же сети Ethernet, что и ПК2. Поэтому маршрутизаторы могут хранить только одну запись в таблице маршрутизации, описывающую “все адреса 168.1”.

Все промежуточные маршрутизаторы повторяют тот же процесс: маршрутизатор сравнивает имеющийся в пакете адрес сетевого уровня (уровня 3) получателя с группами, перечисленными в таблице маршрутизации, и совпадающая запись в таблице маршрутизации сообщает маршрутизатору, куда следует перенаправить пакет. В конце концов пакет доставляется маршрутизатору, который подключен к сети или подсети хоста получателя (т.е. маршрутизатору R3), как показано на рис. 5.1.

Логика R3: доставка данных конечному получателю

Последний маршрутизатор в пути, R3, использует почти такую же логику, как и два других маршрутизатора, но с одним незначительным отличием. Маршрутизатор R3 должен перенаправить пакет непосредственно компьютеру ПК2, а не какому-либо другому маршрутизатору. На первый взгляд это отличие кажется несущественным. Из материала следующего раздела читатель узнает, как канальный уровень используется сетевым уровнем, и важность этого отличия станет очевидной.

Взаимодействие сетевого и канального уровней

Когда протокол сетевого уровня обрабатывает пакет, он принимает решение о его отправке через соответствующий сетевой интерфейс. Прежде чем в физический интерфейс поступят фактические биты, сетевой уровень должен передать пакет протоколам канального уровня, которые в свою очередь “попросят” сетевой уровень отправить эти данные. Как было сказано в главе 3, перед отправкой фреймов через физическую сеть канальный уровень добавляет к пакету соответствующий заголовок и концевик, создавая фрейм. Процесс маршрутизации перенаправляет через сеть только пакет, *отбрасывая по пути заголовки и концевики канального уровня*. Сетевой уровень обрабатывает доставку пакетов из конца в конец, используя последовательные канальные заголовки и концевики только для того, чтобы доставить пакет к следующему маршрутизатору или хосту. Каждый последующий канальный уровень просто передает пакет от одного устройства другому. На рис. 5.2 показана логика инкапсуляции данных в каждом устройстве применительно к примеру на рис. 5.1.

Поскольку маршрутизаторы строят новые канальные заголовки и концевики (на рисунке концевики не показаны) и поскольку новые заголовки содержат канальные адреса, компьютеры и маршрутизаторы должны иметь какой-то способ для определения того, какие канальные адреса использовать. Примером того, как маршрутизатор определяет, какой канальный адрес использовать, является *протокол преобразования IP-адресов* (Address Resolution Protocol — ARP). Протокол ARP используется для динамического определения канального адреса хоста IP, подключенного к локальной сети. Далее в этой главе протокол ARP рассматривается более подробно.

Маршрутизация, как уже было сказано, в своей основе имеет две главные идеи.

- Процесс маршрутизации перенаправляет пакеты третьего уровня, которые также называются *блоками данных протокола уровня 3* (Layer 3 Protocol Data Units — L3 PDU), на основе содержащегося в пакете адреса получателя.
- Процесс маршрутизации использует канальный уровень для инкапсуляции пакетов третьего уровня во фреймы второго уровня для передачи через каждый последующий канал.

Пакеты и заголовки IP

Пакеты IP инкапсулированы в канальные фреймы, показанные на рис. 5.2, и имеют заголовок IP, за которым следуют дополнительные заголовки и данные. На рис. 5.2 показаны обычные для большинства современных сетей обязательные поля в стандартном 20-байтовом заголовке IPv4.

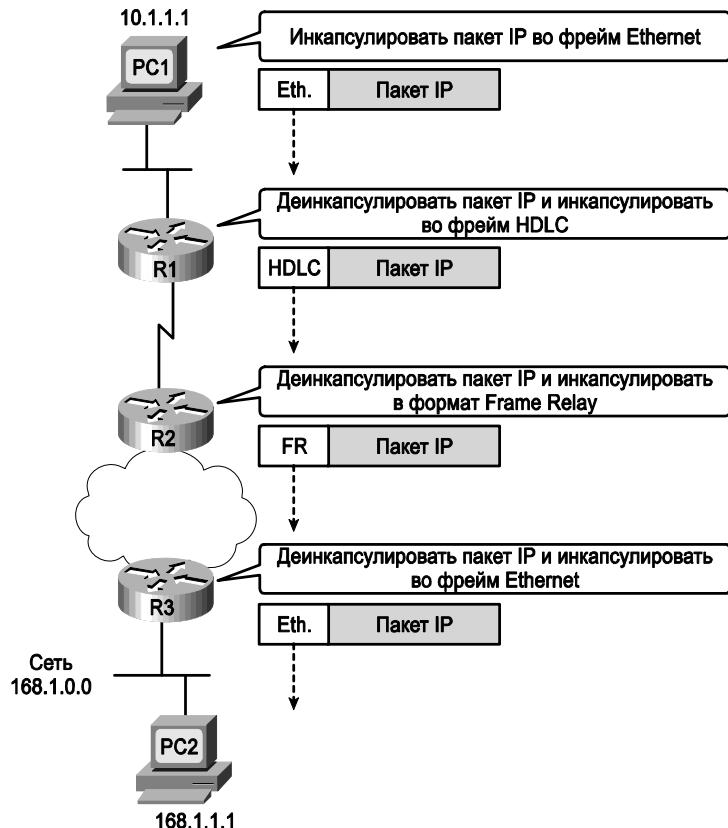


Рис. 5.2. Инкапсуляция сетевого и канального уровней

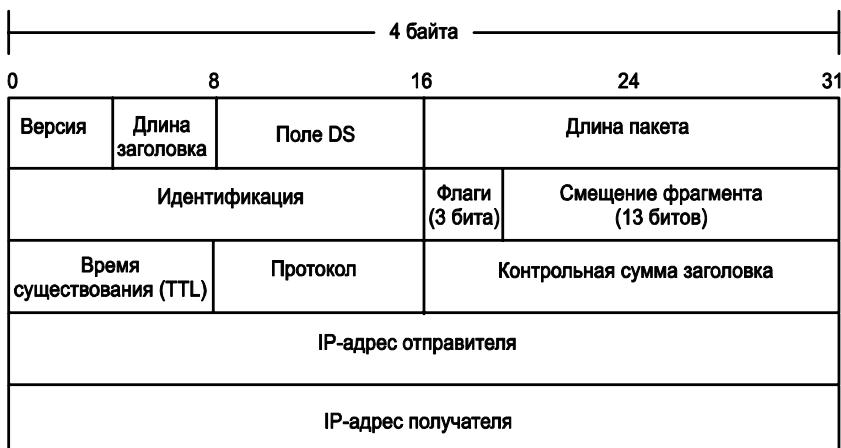


Рис. 5.3. Заголовок IPv4

Из всех полей в заголовке IPv4 в этой книге и во втором томе рассматриваются только поле TTL (Time-To-Live — время существования пакета, оно описано в главе 21), поле протокола (глава 8 второго тома), а также поля IP-адреса отправителя и получателя (которые так или иначе рассматриваются в большинстве глав). Однако для справки в табл. 5.2 кратко описаны все поля.

Таблица 5.2. Поля заголовка IPv4

Поле	Назначение
Версия (version)	Версия протокола IP. В настоящее время в большинстве сетей используется версия 4
Длина заголовка IP (IP Header Length — IHL)	Длина заголовка IP. Определяет длину заголовка IP, включая необязательные поля
Поле DS (differentiated services field)	Поле дифференцированных служб. Используется при маркировании пакетов для применения к разным пакетам различных уровней качества обслуживания (QoS)
Длина пакета (packet length)	Идентифицирует полную длину пакета IP, включая данные
Идентификация (identification)	Используется процессом фрагментации пакета IP; все фрагменты исходного пакета содержат один идентификатор
Флаги (flags)	Три бита, которые используются процессом фрагментации пакета IP
Смещение фрагмента (fragment offset)	Число, которое помогает хосту заново собрать фрагментированные пакеты в один более крупный исходный пакет
Время существования (TTL)	Время существования пакета. Значение, которое используется для предотвращения маршрутных петель
Протокол (protocol)	Поле, которое идентифицирует содержимое порции данных пакета IP. Например, значение 6 означает, что заголовок TCP является первым элементом в поле данных пакета IP
Контрольная сумма заголовка (header checksum)	Поле для хранения значения FCS, для определения битовых ошибок в заголовке IP
IP-адрес отправителя (source IP address)	32-битовый IP-адрес отправителя пакета
IP-адрес получателя (destination IP address)	32-битовый IP-адрес получателя пакета

В следующем разделе рассматривается концепция адресации сетевого уровня и то, как она способствует процессу маршрутизации.

Адресация сетевого (третьего) уровня

Протоколы сетевого уровня определяют формат и назначение логической адресации. (Термин *логический адрес* (logical address) в действительности означает не то, что адрес имеет какую-то особую логику, а скорее противопоставляет эти адреса физическим адресам.) Каждый компьютер, который должен обмениваться данными с другими компьютерами, имеет (по крайней мере) один адрес сетевого уровня, на который другие компьютеры могут отправлять пакеты данных, и ожидать, что сеть доставит эти пакеты по назначению.

Одной из ключевых особенностей адресов сетевого уровня является то, что они позволяют логически группировать адреса. Иначе говоря, часть числового значения адреса подразумевает множество адресов, которые находятся в одной группе. В случае IP-адресов эта группа называется *сетью* (network) или *подсетью* (subnet). Эти группы работают так же, как почтовые индексы, позволяя маршрутизаторам (сортировщикам почты) быстро определять маршрут (сортировать) множества пакетов (писем).

Так же как названия улиц в почтовых адресах, адреса сетевого уровня группируются на основании физического расположения в сети. Правила группировки для некоторых протоколов сетевого уровня отличаются, но в случае IP-адресации первая часть IP-адреса одинакова для всех адресов в одной группе. Например, на рис. 5.1 и 5.2 следующие соглашения IP-адресации определяют группы IP-адресов (сети IP) для всех хостов в этой объединенной сети:

- хосты в верхней сети Ethernet: адреса начинаются с 10;
- хосты на последовательном канале R1-R2: адреса начинаются с 168.10;
- хосты в сети Frame Relay R2-R3: адреса начинаются с 168.11;
- хосты в нижней сети Ethernet: адреса начинаются с 168.1.

ВНИМАНИЕ!

Чтобы избежать путаницы при обсуждении сетей IP, во многих источниках (включая эту книгу) термин *объединенная сеть* (internetwork) или *сетевой комплекс* обозначает сеть в общем, состоящую из маршрутизаторов, коммутаторов, кабелей и другого оборудования, а термин *сеть* (network) обозначает более специфичное понятие сети IP.

Маршрутизация опирается на тот факт, что адреса третьего уровня группируются. Таблицы маршрутизации для каждого протокола сетевого уровня могут иметь одну запись для группы, а не по одной записи для каждого отдельного адреса. Представим сеть Ethernet с сотней хостов TCP/IP. Маршрутизатор, которому нужно перенаправить пакеты любому из этих хостов, должен использовать только одну запись своей таблицы маршрутизации IP, которая представляет всю группу хостов сети Ethernet. Этот факт является одной из основных причин того, что маршрутизаторы способны к масштабированию и поддержке сотен тысяч устройств. Это очень похоже на систему почтовых индексов США. Было бы крайне неудобно, если бы почтовые адреса с одинаковым индексом относились к домам, которые расположены очень далеко друг от друга, или, наоборот, соседние дома имели бы разные индексы. Почтальонам пришлось бы тратить все свое время, пересекая страну вдоль и поперек. Аналогично, протоколы сетевого уровня группируют адреса так, чтобы сделать маршрутизацию более эффективной.

Протоколы маршрутизации

Условно говоря, маршрутизаторы на рис. 5.1 и 5.2 как-то “знают”, что нужно предпринять, чтобы перенаправить пакет от компьютера ПК1 компьютеру ПК2. Чтобы сделать правильный выбор, каждый маршрутизатор должен иметь таблицу маршрутизации с маршрутом, который подходит для пакета, отправленного компьютеру ПК2. Маршруты указывают маршрутизатору, куда нужно отправить пакет дальше.

В большинстве случаев маршрутизаторы строят свои таблицы динамически, используя протокол маршрутизации. Протоколы маршрутизации изучают расположение в сети всех “групп” сетевого уровня и извещают своих соседей о расположении этих групп. В результате каждый маршрутизатор может динамически построить актуальную таблицу маршрутизации. Протоколы маршрутизации, как и любые другие протоколы, определяют форматы сообщений и процедуры. Конечная цель каждого протокола маршрутизации состоит в заполнении таблицы маршрутизации всеми известными группами устройств-получателей с наилучшим маршрутом к каждой из этих групп.

Терминология, связанная с протоколами маршрутизации, иногда может сбивать с толку. *Протокол маршрутизации* (routing protocol) изучает маршруты и записывает их в таблицу маршрутизации. *Маршрутизуемый протокол* (routed protocol) определяет тип маршрутизуемого через сеть пакета. На рис. 5.1 и 5.2 показано, как осуществляется маршрутизация пакетов IP — протокол IP является *маршрутизуемым протоколом*. Если бы маршрутизаторы для изучения маршрутов использовали *протокол маршрутной информации* (Routing Information Protocol — RIP), то протокол RIP был бы *протоколом маршрутизации*. Далее, в разделе “Протоколы маршрутизации IP”, приведен подробный пример того, как протоколы маршрутизации изучают маршруты.

Итак, теперь вы знакомы с главной функцией сетевого уровня модели OSI. В остальной части главы рассматриваются ключевые компоненты процесса сквозной маршрутизации для TCP/IP.

IP-адресация

IP-адресация, безусловно, является самой важной темой экзаменов CCNA. К концу обучения вы должны свободно и уверенно разбираться в IP-адресах, их форматах, понятиях группировки, в том, как группы подразделяются на подсети, как интерпретировать документацию по IP-адресации существующих сетей и т.п. Иными словами, вы должны лучше разбираться в адресации и подсетях.

В этом разделе рассматривается IP-адресация и подсеть, а также концепции, лежащие в основе структуры IP-адреса, включая ее связь с маршрутизацией IP. В части III книги кратко описан математический аппарат, на котором основывается IP-адресация и подсети.

Определения IP-адресации

Чтобы обмениваться данными с другими устройствами по протоколу TCP/IP, устройству необходим IP-адрес. Если устройство имеет IP-адрес и соответствующее программное и аппаратное обеспечение, то оно может отправлять и принимать пакеты IP. Любое устройство, которое может отправлять и принимать пакеты IP, называется *хостом IP* (IP host).

ВНИМАНИЕ!

Четвертая версия (IPv4) в настоящий момент является наиболее распространенной версией протокола IP. В официальном руководстве по подготовке к экзамену ICND2 рассматривается более новая версия этого протокола — IPv6. В этой книге шестая версия рассматривается кратко. Поэтому все упоминания IP-адресов в данной книге относятся к адресам четвертой версии протокола IP.

IP-адрес состоит из 32-битового числа, обычно записанного в *точечно-десятичной нотации*. “Десятичная” часть этого термина связана с тем фактом, что каждый байт (8 бит) 32-битового IP-адреса отображается как десятичное число. Четыре десятичных числа записываются последовательно и разделяются “точками” (десятичными разделителями) — отсюда и название *точечно-десятичная*. Например, 168.1.1.1 — это IP-адрес, записанный в точечно-десятичной форме; двоичная версия этого адреса — 10101000 00000001 00000001 00000001. (Обычно записывать двоичную версию не требуется, но в главе 14 описано преобразование адресов из одного формата в другой.)

Каждое десятичное число в IP-адресе называется *октетом* (octet). Термин *октет* — это просто нейтральный термин для байта (byte). Таким образом, для IP-адреса 168.1.1.1 первый октет равен 168, второй октет равен 1 и т.д. В каждом октете используются десятичные числа в диапазоне от 0 до 255 включительно.

Наконец, следует отметить то, что каждый сетевой интерфейс использует уникальный IP-адрес. Большинство людей склонны считать, что их компьютеры имеют IP-адреса, но на самом деле IP-адреса имеются у компьютерных сетевых плат. Если вставить в компьютер две платы Ethernet, то, чтобы можно было передавать между ними пакеты IP, каждой из них нужно будет назначить уникальный IP-адрес. Если ноутбук одновременно имеет сетевую плату Ethernet и сетевую плату беспроводной сети, то он имеет IP-адрес для каждого из этих сетевых интерфейсов. Аналогично маршрутизаторы, которые обычно имеют множество сетевых интерфейсов (перенаправляющих IP-пакеты), имеют IP-адрес для каждого из этих интерфейсов.

Имея некоторое представление о базовой терминологии, можно переходить к следующему разделу, в котором IP-адресация связывается с концепциями маршрутизации на третьем уровне эталонной модели OSI.

Как группируются IP-адреса

В первоначальных спецификациях стека протоколов TCP/IP IP-адреса группировались в наборы последовательных адресов, которые назывались *сетями IP* (IP network). Все адреса в одной сети имели одинаковое значение первой части. На рис. 5.4 показана простая объединенная сеть, состоящая из трех отдельных сетей IP.

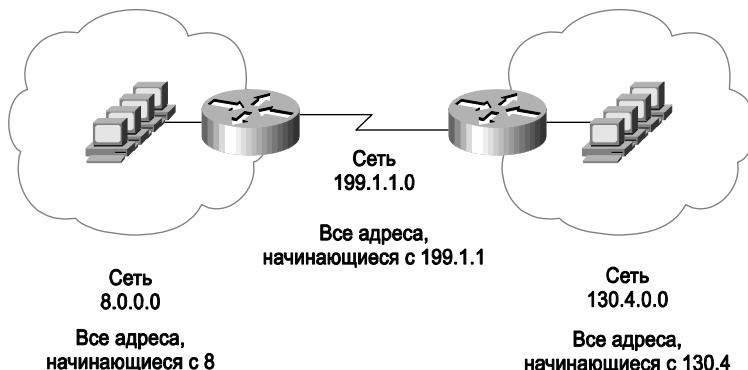


Рис. 5.4. Пример сети с адресами классов A, B и C

Соглашения по IP-адресации и группировке IP-адресов облегчают маршрутизацию. Например, все IP-адреса, которые начинаются с 8, находятся в сети IP, содержащей все узлы сети Ethernet слева. Аналогично все IP-адреса, начинающиеся с 130.4, находятся в другой сети IP, которая состоит из всех узлов в правом сегменте Ethernet. 199.1.1 — префикс всех IP-адресов в сети, которая включает в себя адреса на последовательном канале. (В этой последней группе два IP-адреса принадлежат двум маршрутизаторам.) Следуя этому соглашению, маршрутизаторы строят свои таблицы маршрутизации с тремя записями — по одной для каждого префикса или сетевого номера. Например, маршрутизатор слева может иметь один маршрут, который обозначает все адреса, начинающиеся с 130.4. Этот маршрут заставляет маршрутизатор перенаправлять пакеты маршрутизатору справа.

В примере косвенно подчеркиваются некоторые ключевые моменты организации IP-адресов. Чтобы прояснить эти моменты, необходимо выделить два правила, согласно которым IP-адреса должны входить в одну и ту же группу.



Правила, согласно которым IP-адреса должны входить в ту же группу

- IP-адреса в одной группе не должны разделяться маршрутизатором;
- IP-адреса, разделенные маршрутизатором, должны находиться в разных группах.

Как уже было сказано, IP-адресация работает аналогично системе почтовых индексов. Например, каждый человек, имеющий такой же почтовый индекс, как у меня, живет в маленьком городке в штате Огайо. Если бы кто-то с таким же индексом жил в Калифорнии, то некоторые мои письма могли бы по ошибке приходить в Калифорнию. Аналогично IP-маршрутизация полагается на тот факт, что все IP-адреса в одной группе (которая называется либо сетью, либо подсетью) находятся в одном и том же месте. Если некоторые IP-адреса в моей сети или подсети были бы допустимыми на другой стороне объединенной сети (по отношению к моему компьютеру), то маршрутизаторы в сети могли бы некорректно пересыпал некоторые пакеты (отправленные моему компьютеру) на другую сторону сети.

Классы сетей

На рис. 5.4 показано, что IP-адреса всех устройств, подключенных к левому сегменту Ethernet, начинаются с 8, а IP-адреса устройств, подключенных к правому сегменту Ethernet, — с 130.4. Почему для префикса левой сети используется одна цифра (8), тогда как для префикса правой — две (130 и 4)? Это связано с классами IP-адресов.

Стандарт RFC 791 определяет протокол IP, включая несколько различных классов сетей. Протокол IP определяет три разных класса сетей для адресов, которые используются отдельными хостами, — такие адреса называются *одноадресатными IP-адресами* (unicast IP addresses). Эти три класса сетей называются классами A, B и C. В спецификации TCP/IP определяются также адреса класса D (многоадресатные) и адреса класса E (экспериментальные).

По определению все адреса в одной сети класса A, B или C имеют одинаковое чистовое значение для части адреса, которая соответствует *сети*. Остальная часть адреса называется *частью хоста*.

Используя пример с почтовой службой, можно сказать, что сетевая часть IP-адреса ведет себя как почтовый индекс, а часть хоста — как улица и дом в обычном адресе. Так же как сортировочная машина, находящаяся в трех штатах от вас, принимает во внимание только почтовый индекс на письме, адресованном вам, маршрутизатор, находящийся в трех транзитных переходах от вас, использует только адрес сети, в которой расположен ваш компьютер.

Сети классов А, В и С имеют различную длину той части адреса, которая идентифицирует сеть:

- для сетей класса А длина сетевой части равна 1 байту; 3 оставшихся байта называются частью хоста;
- для сетей класса В длина сетевой части равна 2 байтам; 2 оставшихся байта отводятся для адреса хоста;
- для сетей класса С длина сетевой части равна 3 байтам; для адреса хоста отводится только один байт.

Например, на рис. 5.4 показана сеть 8.0.0.0 в левом сегменте Ethernet. Сеть 8.0.0.0 принадлежит классу сетей А, а это означает, что только один октет (байт) используется для сетевой части адреса. Поэтому адреса всех узлов в этой сети начинаются с 8. Аналогичная ситуация с сетью класса В 130.4.0.0 в правом сегменте Ethernet. Два октета определяют сетевую часть, поэтому все адреса начинаются с 130.4.

Существует соглашение при перечислении адресов сетей записывать их с десятичными нулями в части хоста. Поэтому сеть “8” класса А, содержащая все адреса, которые начинаются с 8, записывается как 8.0.0.0. Аналогично сеть “130.4” класса В, которая содержит все IP-адреса, которые начинаются с 130.4, записывается как 130.4.0.0 и т.д.

Рассмотрим величину сетей каждого класса. Сетям класса А для сетевой части адреса требуется только 1 байт, а 3 байта или 24 бита остаются для части хоста. Таким образом, для любой сети класса А существует 2^{24} различных значений части хоста. Поэтому каждая сеть класса А может иметь 2^{24} IP-адресов — минус два зарезервированных в каждой сети адреса (табл. 5.3). В таблице даны сводные характеристики сетей классов А и С.

Таблица 5.3. Величины частей сети и хоста IP-адресов без подсетей



Класс сети	Количество байт (битов) части сети	Количество байт (битов) части хоста	Количество адресов в сети ¹
A	1 (8)	3 (24)	$2^{24} - 2$
B	2 (16)	2 (16)	$2^{16} - 2$
C	3 (24)	1 (8)	$2^8 - 2$

На основании трех примеров рис. 5.4 в табл. 5.4 в двоичном виде записаны три сетевых адреса: 8.0.0.0, 130.4.0.0 и 199.1.1.0.

¹ В каждой сети существуют два зарезервированных адреса узла. — Примеч. авт.

Таблица 5.4. Десятичные и двоичные адреса сетей

Адрес сети	Двоичное представление. Часть хоста выделена полужирным шрифтом
8.0.0.0	00001000 00000000 00000000 00000000
130.4.0.0	10000010 00000100 00000000 00000000
199.1.1.0	11000111 00000001 00000001 00000000

Несмотря на то что адреса сетей из-за своего точечно-десятичного формата похожи на обычные адреса, их нельзя назначать интерфейсам в качестве IP-адресов. Концептуально адреса сетей представляют группу IP-адресов в сети, так же как почтовый индекс представляет группу адресов в населенном пункте. Возникла бы путаница, если бы один номер представлял целую группу адресов и использовался бы как IP-адрес для одного устройства. Поэтому адреса сетей зарезервированы и не могут использоваться в качестве IP-адресов устройств.



Объяснение концепции сетевых широковещательных или направленных широковещательных адресов

Кроме адреса, в каждой сети зарезервировано второе точечно-десятичное значение. Следует заметить, что первое зарезервированное значение (адрес сети) содержит двоичные нули в части хоста адреса (см. табл. 5.4). Второе зарезервированное значение состоит из двоичных единиц в части хоста. Этот адрес называется *широковещательным адресом сети* (network broadcast), или *направленным широковещательным адресом* (directed broadcast). Этот зарезервированный номер не может быть назначен хосту в качестве IP-адреса. Однако пакеты, направленные на широковещательный адрес сети, перенаправляются всем устройствам этой сети.

Поскольку адрес сети имеет наименьшее числовое значение в этой сети, а широковещательный адрес — наибольшее, все адреса между ними являются корректными и подходят в качестве IP-адресов интерфейсов в этой сети.

Реальные адреса сетей классов А, В и С

Интернет представляет собой множество, в которое входят почти все сети IP и почти все хосты TCP/IP (компьютеры) мира. Первоначальная конструкция сети требовала соблюдения нескольких взаимосвязанных принципов, чтобы обеспечить функционирование Интернета и его управляемость:

- каждый компьютер, подключенный к Интернету, должен иметь уникальный, не повторяющийся IP-адрес;
- центральный орган управления административно назначал сети классов А, В и С компаниям, правительенным учреждениям, школам и провайдерам Интернета в зависимости от размеров их сетей IP (класс А — для крупных сетей, класс В — для средних и класс С — для мелких);
- центральный орган управления назначал каждый адрес сети только одной организации, гарантируя уникальность этого адреса во всем мире;
- каждая организация, получив сеть класса А, В или С, затем назначала отдельные IP-адреса внутри этой сети.

Согласно этим принципам, до тех пор, пока каждая организация назначает каждый IP-адрес только одному компьютеру, каждый компьютер в Интернете имеет глобально уникальный IP-адрес.

ВНИМАНИЕ!

Со временем детали назначения адресов изменились, но общая идея, описанная здесь, поможет понять концепцию различных классов сетей.

Организация, в ведении которой находится всемирное назначение IP-адресов, называется Ассоциация по присвоению имен и номеров портов Интернета (Internet Corporation for Assigned Network and Numbers — ICANN, www.icann.org). (Ранее полномочиями по выделению IP-адресов владело Агентство по выделению имен и уникальных параметров протоколов Интернета (Internet Assigned Numbers Authority — IANA).) Ассоциация ICANN в свою очередь передает свои полномочия на местах другим сотрудничающим организациям. Например, организация Американский регистратор адресов Интернета (American Registry for Internet Numbers — ARIN, www.arin.org) контролирует процесс назначения адресов в Северной Америке.

В табл. 5.5 перечислены возможные адреса сетей, которые могли бы быть выданы ICANN и другими агентствами. Обратите внимание на общее количество хостов для каждого класса сети и количество хостов в каждой сети класса A, B и C.



Таблица 5.5. Все возможные корректные адреса сетей²

Класс сети	Диапазон первого октета	Допустимые адреса сетей	Общее количество адресов для этого класса	Количество хостов в сети
A	от 1 до 126	от 1.0.0.0 до 126.0.0.0	$2^7 - 2$ (126)	$2^{24} - 2$ (16 777 214)
B	от 128 до 191	от 128.0.0.0 до 191.255.0.0	2^{14} (16 384)	$2^{16} - 2$ (65 534)
C	от 192 до 223	от 192.0.0.0 до 223.255.255.0	2^{21} (2 097 152)	$2^8 - 2$ (254)

Запоминание содержимого табл. 5.5 имеет важное значение при подготовке к экзаменам CCNA. Инженеры должны легко определять принадлежность сети к классам A, B или C. Кроме того, следует запомнить количество октетов в сетевой части адресов классов A, B и C (см. табл. 5.4).

Механизм создания подсетей IP

Механизм создания подсетей — одна из наиболее важных тем экзаменов ICND1, ICND2 и CCNA. Необходимо понимать, как он работает и как определять проблемы при использовании подсетей в реальной жизни и на экзамене. В части III этой книги рассматриваются подробности концепции подсетей, мотивировка и математический аппарат, однако базовое понимание этой концепции нужно для изучения тем, которые описаны в главах, предшествующих части III. Меха-

² В столбце “Допустимые адреса сетей” показаны фактические адреса сетей. Сети 0.0.0.0 (этот адрес был первоначально определен для использования в качестве широковещательного адреса) и 127.0.0.0 (этот адрес все еще доступен для проверки обратной петли) зарезервированы. — Примеч. авт.

низм создания подсетей IP подразделяет сеть класса A, B или C на несколько более мелких групп IP-адресов. Правила классов A, B и C остаются, но одна сеть класса A, B или C теперь может подразделяться на множество мелких групп. Механизм создания подсетей рассматривает подразделение одной сети класса A, B или C на меньшие сети. На самом деле название “подсеть” это просто сокращение от “подразделенная сеть”.

Понять концепцию, лежащую в основе механизма создания подсетей, будет не трудно, если сравнить топологию сети без подсетей с той же топологией, но с реализованными подсетями. На рис. 5.5 показана сеть без подсетей.

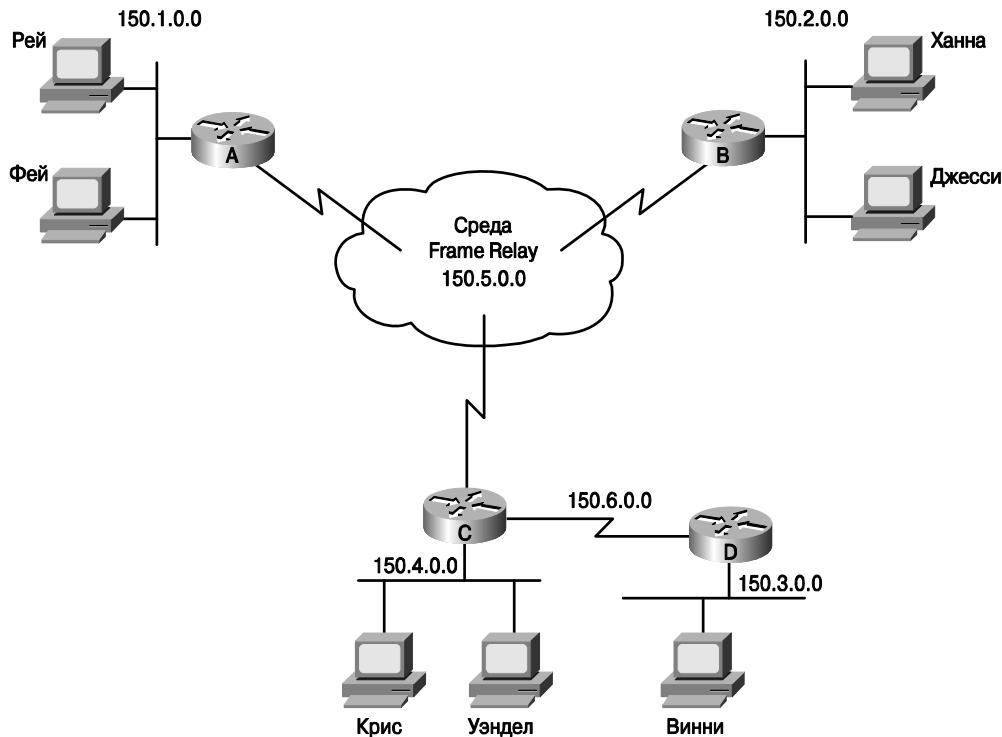


Рис. 5.5. Иллюстрация к обсуждению количества различных сетей и подсетей

Конструкция сети на рис. 5.5 требует шести групп IP-адресов, каждая из которых является в данном примере сетью класса B. Каждая из четырех локальных сетей использует одну сеть класса B. Иначе говоря, каждая локальная сеть, подключенная к маршрутизаторам A, B, C и D, является отдельной сетью IP. В дополнение к этому два последовательных интерфейса, образующих последовательный двухточечный канал между маршрутизаторами C и D, используют одну сеть IP, поскольку эти интерфейсы не разделены маршрутизатором. Наконец, три интерфейса маршрутизатора, составляющих сеть Frame Relay с маршрутизаторами A, B и C, не отделены маршрутизатором IP и используют шестую сеть IP.

Каждая сеть класса B имеет $2^{16} - 2$ адреса хоста — это гораздо больше, чем может понадобиться для локальной сети или канала WAN. Например, левый верхний сег-

мент Ethernet должен содержать все адреса, начинающиеся с 150.1. Следовательно, адреса, которые начинаются с 150.1, не могут быть назначены где-либо, кроме левого верхнего сегмента Ethernet. Поэтому, если где-нибудь в другом месте закончатся IP-адреса, невозможно будет использовать большое количество незадействованных адресов, которые начинаются с 150.1. В результате показанная на рис. 5.5 схема адресации впоследствии расходует множество адресов.

На самом деле такая конструкция при подключении этой сети к Интернету была бы недопустимой. Организация, являющаяся членом ICANN, не назначила бы шесть отдельных зарегистрированных адресов сетей класса B. Скорее всего, не удалось бы получить даже одну сеть класса B, поскольку большинство адресов класса B уже занято. Вероятнее всего, можно было бы получить пару сетей класса C в расчете на использование подсетей. На рис. 5.6 показан более реалистичный пример, в котором используется базовый механизм создания подсетей.

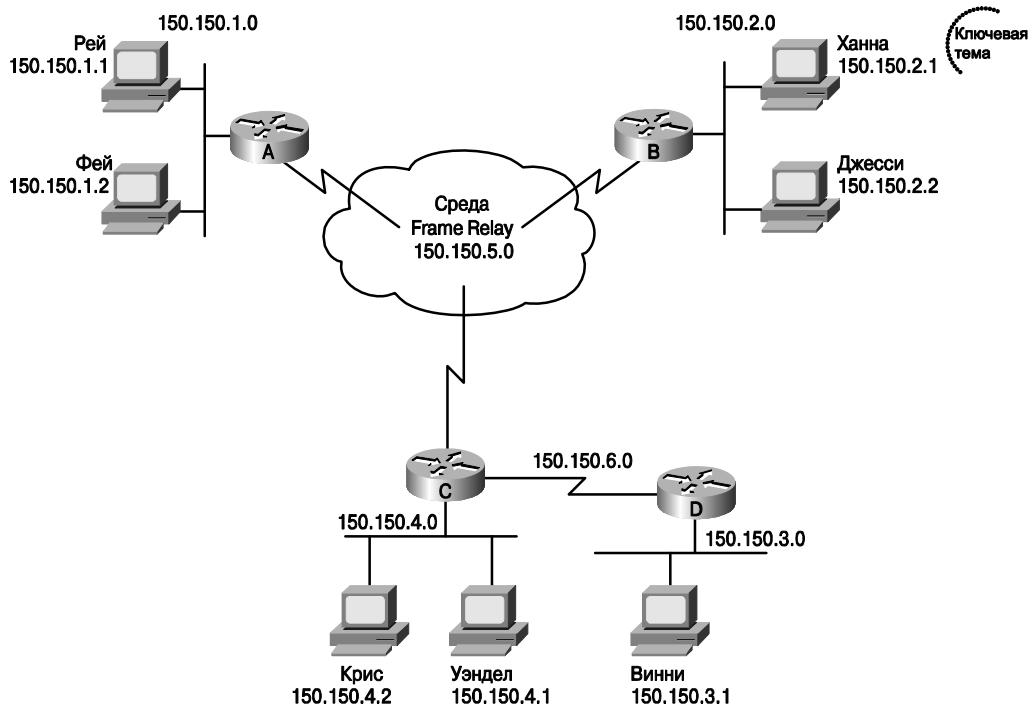


Рис. 5.6. Использование подсетей

Как и на рис. 5.5, в конструкции на рис. 5.6 требуется шесть групп, но в отличие от примера на рис. 5.5 здесь используется шесть подсетей, каждая из которых является подсетью одной сети класса B. В данном случае сеть класса B 150.150.0.0 подразделяется на шесть подсетей. Чтобы реализовать механизм создания подсетей, третий октет (в этом примере) используется для идентификации уникальных подсетей сети 150.150.0.0.

Обратите внимание на то, что в каждом адресе подсети на рисунке используется другое значение третьего октета — другой адрес подсети. Иначе говоря, в этой конструкции подсети нумеруются или идентифицируются с помощью третьего октета.

При использовании подсетей третья часть IP-адреса, т.е. *часть подсети*, оказывается между сетевой частью адреса и частью хоста. Это поле создается заимствованием битов части хоста адреса. Размер сетевой части адреса не сокращается. Другими словами, для определения размера сетевой части адреса все также применяются правила классов А, В и С. Пространство для части подсети адреса освобождается за счет сокращения части хоста. На рис. 5.7 показан формат адресов при использовании подсетей с указанием количества битов в каждой из трех частей IP-адреса.

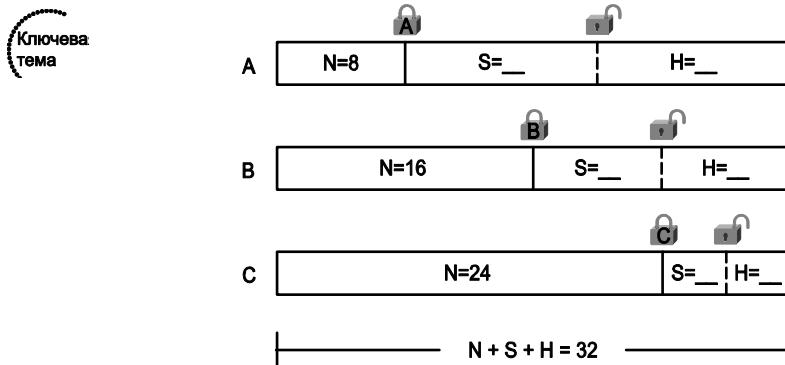


Рис. 5.7. Форматы классовых адресов при использовании подсетей

Вместо маршрутизации на основе сетевой части адреса маршрутизаторы могут осуществлять маршрутизацию на основе комбинации сетевой части адреса и части хоста. Например, когда компьютер Криса (150.150.4.2) отправляет пакет компьютеру Ханны (150.150.2.1), маршрутизатор С имеет информацию о маршруте, в которой упоминаются “все адреса, начинающиеся с 150.150.2”. Этот же маршрут предписывает маршрутизатору С перенаправить пакет маршрутизатору В. Следует отметить, что информация в таблице маршрутизации включает как сетевую часть адреса, так и часть подсети, поскольку обе эти части вместе идентифицируют группу.

Следует также отметить, что показанная на рис. 5.7 концепция с тремя частями IP-адреса (сети, подсети и хоста) называется *классовой адресацией* (classful addressing). Термин *классовая адресация* относится к тому, как можно описывать IP-адреса, а именно то, что они имеют три части. В частности, классовая адресация означает, что адрес можно рассматривать как имеющий сетевую часть, которая определяется на основании правил адресации для сетей классов А, В и С, — отсюда и слово “классовая” в названии.

Поскольку процесс маршрутизации рассматривает сетевую часть адреса и часть подсети вместе, можно выделить альтернативный подход к IP-адресам, который называется *бесклассовая адресация* (classless addressing). Вместо трех частей каждый адрес содержит две части:

- часть, на основе которой осуществляется маршрутизация;
- часть хоста.

Первая часть, на которой основывается маршрутизация, — это комбинация сетевой части и части подсети с точки зрения классовой адресации. Эта первая часть зачастую называется просто частью подсети, или иногда *префиксом*. На рис. 5.8 показаны концепция и термины, относящиеся к бесклассовой IP-адресации.

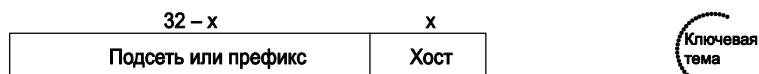


Рис. 5.8. Формат бесклассовых адресов при использовании подсетей

Наконец, в IP-адресации с механизмом создания подсетей используется понятие *маски подсети* (subnet mask). Мaska подсети способствует определению структуры IP-адреса, как показано на рис. 5.7 и 5.8. Подробнее маски подсетей рассматриваются в главах 14–16.

Маршрутизация IP

В первом разделе этой главы рассматривались основы маршрутизации на примере сети с тремя маршрутизаторами и двумя персональными компьютерами. Теперь, зная об IP-адресации больше, можно рассмотреть процесс маршрутизации IP подробней. В этом разделе основное внимание уделено тому, как хост-отправитель определяет, куда следует направить пакет, а также тому, как маршрутизаторы выбирают, куда следует перенаправлять пакеты, чтобы они достигли хоста-получателя.

Маршрутизация в хостах

Хости при определении того, куда отправлять пакет, фактически используют некоторую простую логику маршрутизации. Эта двухэтапная логика описана ниже.

Двухэтапный процесс маршрутизации пакетов

- Этап 1** Если IP-адрес получателя находится в той же подсети, что и адрес отправителя, пакет отправляется непосредственно хосту-получателю.
- Этап 2** Если IP-адрес получателя находится в другой подсети, пакет отправляется стандартному шлюзу. *Стандартный шлюз* (default gateway) — это интерфейс Ethernet маршрутизатора в данной подсети.

Например, рассмотрим рис. 5.9, в частности локальную сеть Ethernet в верхней его части. В верхнем сегменте Ethernet имеются два персональных компьютера, ПК1 и ПК11, а также маршрутизатор R1. Если ПК1 отправляет пакет на адрес 150.150.1.11 (IP-адрес ПК11), то пакет отправляется компьютеру ПК11 через сеть Ethernet — нет необходимости использовать маршрутизатор.

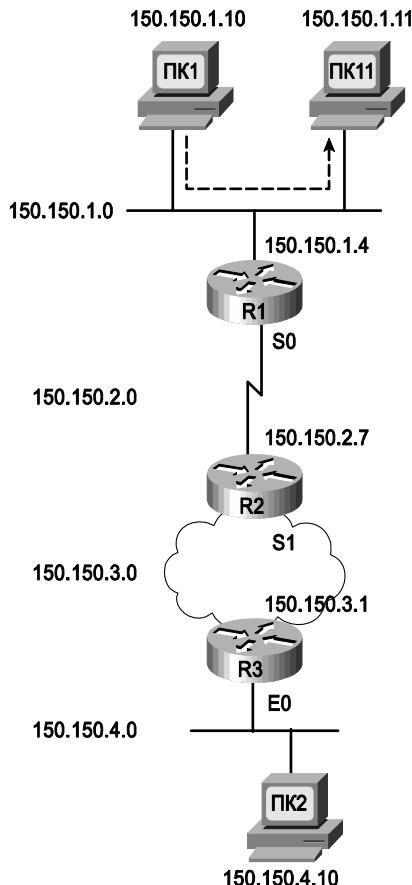


Рис. 5.9. Альтернативы маршрутизации в хостах

Однако если ПК1 отправляет пакет компьютеру ПК2 (150.150.4.10), то согласно второму этапу логики маршрутизации в хостах пакет направляется стандартному шлюзу, т.е. на адрес 150.150.1.4, IP-адрес интерфейса Ethernet маршрутизатора R1. В следующем разделе описан пример, в котором компьютер ПК1 использует свой стандартный шлюз.

Решения о перенаправлении, принимаемые маршрутизатором, и таблица маршрутизации IP

Ранее в этой главе на рис. 5.1 и 5.2 (и в соответствующих разделах) в общих чертах описывалось, как маршрутизаторы перенаправляют пакеты, используя каждую последующую физическую сеть для передачи пакетов следующему устройству. Чтобы лучше оценить решение о перенаправлении, принимаемое маршрутизатором, в этом разделе используется пример с тремя различными маршрутизаторами, перенаправляющими пакеты.

Получая фрейм канального уровня, т.е. фрейм, в котором инкапсулирован пакет IP, маршрутизатор использует следующую логику.



Четырехэтапный процесс маршрутизации пакетов

- Этап 1** Используется поле FCS для проверки ошибок фрейма; если ошибки есть, фрейм отбрасывается.
- Этап 2** Если пакет не был отброшен на предыдущем этапе, отбрасывается старый канальный заголовок и концевик и остается только пакет IP.
- Этап 3** IP-адрес отправителя пакета IP сопоставляется с таблицей маршрутизации и определяется маршрут, который соответствует этому адресу; маршрут идентифицирует исходящий интерфейс маршрутизатора и, возможно, маршрутизатор следующего перехода.
- Этап 4** Пакет IP инкапсулируется в новый канальный заголовок и концевик, подходящий для исходящего интерфейса, и фрейм отправляется.

Каждый маршрутизатор, выполняя описанные выше этапы, отправляет пакет следующему устройству до тех пор, пока пакет не достигнет получателя.

Отдельно следует рассмотреть третий этап — процесс поиска адреса в таблице маршрутизации. В заголовке пакета содержится IP-адрес получателя, а в таблице маршрутизации обычно имеется список сетей и подсетей. Для поиска записи в таблице маршрутизации маршрутизатор “рассуждает” так: *адреса сетей и подсетей представляют группу адресов, которые начинаются с одинакового префикса. В какой из групп таблицы маршрутизации находится адрес получателя?*

Естественно, маршрутизаторы на самом деле превращают эту логику в математическую задачу, но текст весьма точно описывает происходящее. Например, на рис. 5.10 показана та же топология, что и на рис. 5.9, но теперь компьютер ПК1 отправляет пакет компьютеру ПК2.

ВНИМАНИЕ!

В данном случае все маршрутизаторы “знают”, что “подсеть” 150.150.4.0 означает “все адреса, которые начинаются с 150.150.4”.

Ниже поясняется логика перенаправления на каждом этапе, показанном на рисунке. (Следует отметить, что все упоминания этапов 1–4 относятся к описанию логики маршрутизации, которое приведено выше в этом разделе.)

- Этап А** **ПК1 отправляет пакет своему стандартному шлюзу.** Сначала ПК1 создает пакет IP, в котором в качестве адреса получателя указан IP-адрес ПК2 (150.150.4.10). ПК1 должен отправить пакет маршрутизатору R1 (это его стандартный шлюз), поскольку получатель находится в другой подсети. ПК1 помещает пакет IP во фрейм Ethernet, в котором адрес Ethernet получателя соответствует адресу Ethernet маршрутизатора R1. ПК1 отправляет этот фрейм по Ethernet.
- Этап Б** **Маршрутизатор R1 обрабатывает входящий фрейм и перенаправляет пакет маршрутизатору R2.** Так как указанный во входящем фрейме Ethernet MAC-адрес получателя является MAC-адресом маршрутизатора R1, этот маршрутизатор копирует фрейм для обработки. Маршрутизатор проверяет поле FCS фрейма и убеждается, что ошибок нет (этап 1). Затем маршрутизатор отбрасывает заголовок и концевик Ethernet (этап 2). После этого маршрутизатор R1 сравнивает указанный в пакете адрес получателя (150.150.4.10) с таблицей маршрутизации и находит запись для подсети 150.150.4.0. Эта подсеть содержит адреса с 150.150.4.0 по 150.150.4.255 (этап 3). Поскольку адрес получателя находится в этой группе, маршрутизатор R1 после инкапсуляции пакета во фрейм HDLC перенаправляет пакет через исходящий интерфейс Serial0 следующему маршрутизатору R2 (150.150.2.7) (этап 4).

- Этап В** Маршрутизатор R2 обрабатывает входящий фрейм и перенаправляет пакет маршрутизатору R3.
Получив фрейм HDLC, маршрутизатор R2 повторяет тот же общий процесс, что и маршрутизатор R1. Маршрутизатор R2 проверяет поле FCS и обнаруживает, что ошибок нет (этап 1). Затем он отбрасывает заголовок HDLC и концевик (этап 2). После этого R2 находит в своей таблице маршрутизации маршрут для подсети 150.150.4.0, которая включает в себя диапазон адресов 150.150.4.0–150.150.4.255, и “понимает”, что адрес 150.150.4.10 соответствует этому маршруту (этап 3). Наконец, маршрутизатор R2 отправляет пакет через интерфейс Serial1 следующему маршрутизатору R3 (150.150.3.1), предварительно инкапсулировав пакет в заголовок Frame Relay (этап 4).
- Этап Г** Маршрутизатор R3 обрабатывает входящий фрейм и перенаправляет пакет компьютеру ПК2.
Маршрутизатор R3, как и R1 и R2, проверяет поле FCS, отбрасывает старый заголовок и концевик канального уровня и находит свой маршрут для подсети 150.150.4.0. Запись для этой подсети в его (маршрутизатора R3) таблице маршрутизации показывает, что исходящим интерфейсом является интерфейс Ethernet маршрутизатора R3, но маршрутизатора следующего перехода нет, поскольку маршрутизатор R3 подключен непосредственно к подсети 150.150.4.0. Маршрутизатору R3 остается только инкапсулировать пакет в заголовок Ethernet и концевике, указав в качестве адреса Ethernet получателя MAC-адрес компьютера ПК2, и передать фрейм.

Ключевая тема

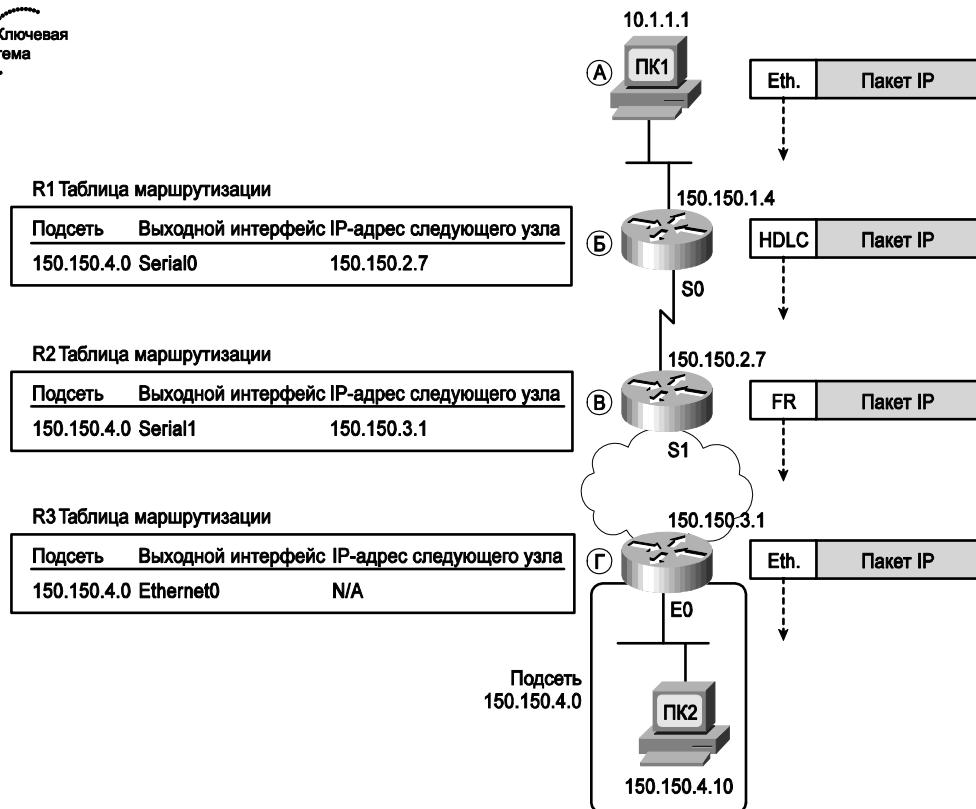


Рис. 5.10. Простой пример маршрутизации с подсетями IP

Процесс маршрутизации опирается на правила, касающиеся IP-адресации. Например, почему компьютер ПК1 (150.150.1.4) считает, что компьютер ПК2 (150.150.4.10) находится в другом сегменте Ethernet? Потому, что у них разные под-

сети 150.150.4.0 (для ПК2) и 150.150.1.0 (для ПК1). Из-за того, что IP-адреса в разных подсетях должны быть отделены маршрутизатором, ПК1 должен отправить пакет маршрутизатору, что он и делает. Аналогично все три маршрутизатора содержат маршрут к подсети 150.150.4.0, которая в данном примере включает в себя IP-адреса с 150.150.4.1 по 150.150.4.254. Что произойдет, если кто-нибудь попытается перенести ПК2 в какое-нибудь другое место сети, сохранив при этом адрес 150.150.4.10? В таком случае маршрутизаторы неправильно перенаправляли бы пакеты. Поэтому, чтобы маршруты строились более эффективно, маршрутизация третьего уровня полагается на структуру адресации третьего уровня.

В части III IP-адресация рассматривается более подробно. Далее в этой главе представлено краткое введение в концепции, лежащие в основе протоколов маршрутизации.

Протоколы маршрутизации IP

Процесс маршрутизации (перенаправления) сильно зависит от наличия в каждом маршрутизаторе актуальной таблицы маршрутизации IP. Протоколы маршрутизации IP заполняют таблицы маршрутизации правильными, беспетельными маршрутами. Каждый маршрут содержит адрес подсети, интерфейс, через который пакеты перенаправляются к этой подсети, а также IP-адрес следующего маршрутизатора. Маршрутизатор должен (по необходимости) получить адресуемые этой подсети пакеты (см. рис. 5.10).

Прежде чем рассмотреть логику, лежащую в основе протоколов маршрутизации, следует уяснить их цели. Описанные ниже цели являются общими для всех протоколов маршрутизации IP независимо от их базовой логики.

- Динамически определять маршруты ко всем подсетям в сети и заполнять эти-ми маршрутами таблицу маршрутизации.
- Если доступно несколько маршрутов к какой-либо подсети, поместить в таб-лицу наилучший из них.
- Определять, когда маршруты в таблице оказываются неправильными, и уда-лять их из таблицы маршрутизации.
- Если маршрут удаляется из таблицы и доступен маршрут через соседний мар-шрутизатор, то добавлять такой маршрут в таблицу. (Многие считают эту цель частью предыдущей.)
- Как можно быстрее добавлять новые маршруты или заменять потерянные маршруты наилучшими из доступных в текущий момент. Время между поте-рьей маршрута и нахождением другого работающего маршрута называется *вре-менем конвергенции* (convergence time).
- Предотвращать маршрутные петли.

Протоколы маршрутизации могут быть довольно сложными, но базовая логика, которая в них используется, сравнительно проста. Маршрутизаторы выполняют сле-дующие общие действия для оповещения сети о маршрутах.

Этап 1 Каждый маршрутизатор добавляет маршрут в свою таблицу маршрутизации для каждой подсети, непосредственно подключенной к этому маршрутизатору.

- Этап 2** Каждый протокол маршрутизации маршрутизатора сообщает своим соседям обо всех маршрутах в его таблице, включая непосредственно подключенные к нему маршруты, а также маршруты, о которых ему сообщили другие маршрутизаторы.
- Этап 3** После получения нового маршрута от соседа протокол маршрутизации маршрутизатора добавляет маршрут в свою таблицу маршрутизации. При этом в качестве маршрутизатора следующего перехода обычно записывается соседний маршрутизатор, от которого был получен этот маршрут.

Например, на рис. 5.11 показана та же сеть, что и на рис. 5.9 и 5.10, но основное внимание в данном случае уделено тому, как три маршрутизатора узнают о подсети 150.150.4.0. Следует заметить, что протоколы маршрутизации выполняют больше работы, чем показано на рисунке. В данном случае важно то, как маршрутизаторы узнают о подсети 150.150.4.0.

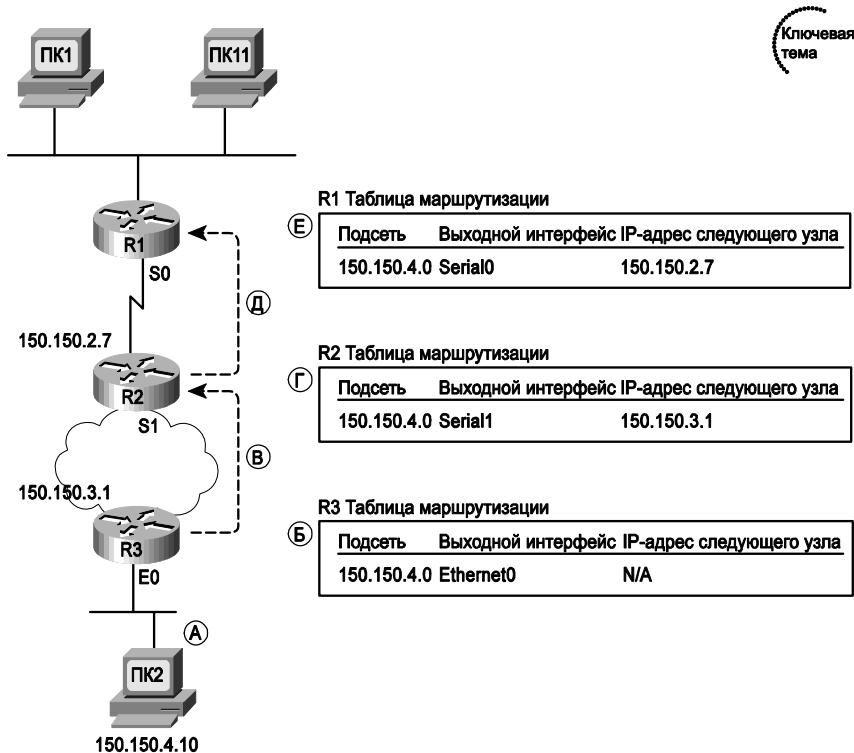


Рис. 5.11. Маршрутизатор R1 узнает о подсети 150.150.4.0

Ниже описаны этапы А, Б, В и Г, отмеченные на рисунке для того, чтобы показать, как каждый маршрутизатор изучает свой маршрут к подсети 150.150.4.0.

- Этапы А, Б** Маршрутизатор R3 узнает маршрут для подсети 150.150.4.0, непосредственно подключенной к его собственному интерфейсу E0, и добавляет этот маршрут в свою таблицу маршрутизации.
- Этап В** Маршрутизатор R3 отправляет сообщение протокола маршрутизации, которое называется *анонсом маршрутизации* (routing update), маршрутизатору R2, и этот маршрутизатор узнает о подсети 150.150.4.0 (этап 2).

-
- Этап Г** Маршрутизатор R3 добавляет маршрут для подсети 150.150.4.0 к своей таблице маршрутизации (этап 3).
- Этап Д** Маршрутизатор R2 отправляет аналогичную информацию маршрутизатору R1, сообщая ему о подсети 150.150.4.0 (этап 2).
- Этап Е** Маршрутизатор R1 добавляет маршрут для подсети 150.150.4.0 к своей таблице маршрутизации (этап 3). Маршрут указывает Serial0 в качестве исходящего интерфейса R1, и IP-адрес R2 (150.150.2.7) — как следующий транзитный маршрутизатор.

В главе 20 протоколы маршрутизации рассматриваются более подробно. Далее в последнем важном разделе этой главы коротко описаны дополнительные функции, связанные с тем, как сетевой уровень перенаправляет пакеты от отправителя получателю через объединенную сеть.

Утилиты сетевого уровня

До сих пор в этой главе описывались главные функции сетевого уровня эталонной модели OSI — в частности, уровень межсетевого взаимодействия TCP/IP, который определяет те же общие функции, что и третий уровень модели OSI. В завершение этой главы в данном разделе рассматриваются четыре инструмента, которые используются почти каждый день практически в каждой сети TCP/IP мира и помогают сетевому уровню решать его задачу по сквозной маршрутизации пакетов в объединенной сети:

- *протокол преобразования адресов* (Address Resolution Protocol — ARP);
- *система доменных имен* (Domain Name System — DNS);
- *протокол динамического конфигурирования хоста* (Dynamic Host Configuration Protocol — DHCP);
- утилита ping.

Протокол преобразования адресов и система доменных имен

Конструкторы сетей должны стараться сделать их использование как можно проще. Главным образом пользователи запоминают имя другого компьютера, к которому они хотят подключиться, так же как они помнят имя веб-сайта. Они определенно не хотят запоминать ни IP-адрес, ни MAC-адрес. Поэтому стеку TCP/IP нужен протокол, который динамически определяет всю необходимую информацию, позволяя обмениваться данными, не заставляя при этом пользователя запоминать что-то кроме имени хоста.

Может показаться, что запоминать имя другого компьютера не нужно. Например, в браузерах многих пользователей настроены домашние страницы по умолчанию, которые открываются сразу после запуска браузера. Можно подумать, что строка универсального локатора ресурса (Universal Resource Locator — URL) не является именем. На самом деле URL домашней страницы содержит имя этой страницы. Например, в URL <http://www.cisco.com/go/ccna> часть www.cisco.com представляет собой имя веб-сервера корпорации Cisco. Поэтому всякий раз, вводя имя другого компьютера в сети или видя его на экране, пользователь обычно идентифицирует дистанционный компьютер по имени.

Таким образом, протоколу TCP/IP нужен способ, который позволит компьютеру определять IP-адрес другого компьютера по его имени. Также нужен способ определять MAC-адреса, связанные с другими компьютерами в той же локальной подсети. Схематически эта проблема показана на рис. 5.12.

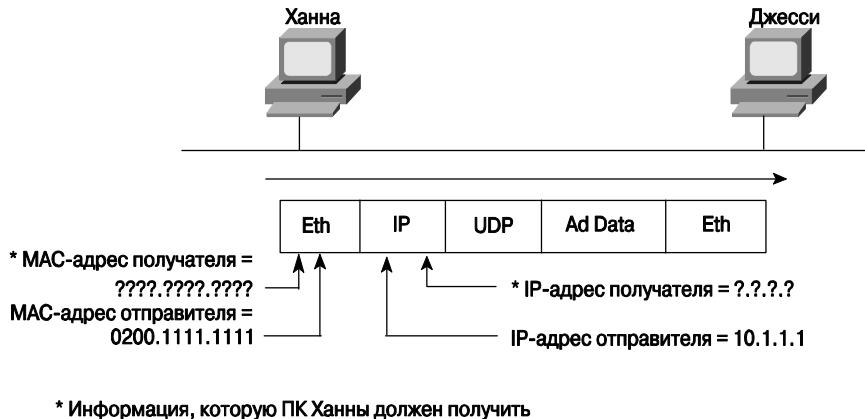


Рис. 5.12. Компьютер Ханны знает имя компьютера Джесси, но нужно получить еще IP- и MAC-адрес этого компьютера

В данном случае компьютер Ханны должен обмениваться данными с сервером, который установлен на ПК Джесси. Компьютер Ханны знает свое имя, свой IP- и MAC-адрес. Ханна не знает IP- и MAC-адреса компьютера Джесси. Для определения этих адресов Ханна использует службу DNS, чтобы найти IP-адрес ПК Джесси, и протокол ARP — чтобы определить MAC-адрес этого компьютера.

Преобразование имен DNS

Компьютер Ханны знает IP-адрес сервера DNS, потому что этот адрес либо заранее записан в конфигурации ПК Ханны, либо был получен с помощью протокола DHCP (эта тема рассматривается в данной главе позднее). Как только пользователь Ханна так или иначе идентифицирует имя другого компьютера (например, jessie.example.com), компьютер отправляет серверу DNS *запрос* на IP-адрес компьютера Джесси. Сервер DNS в ответ отправляет адрес 10.1.1.2. Этот простой процесс показан на рис. 5.13.

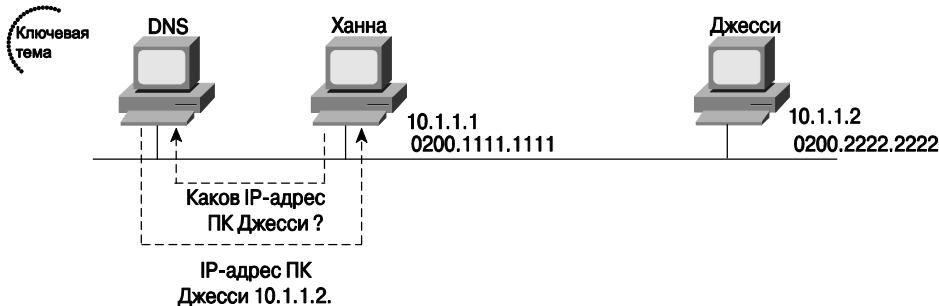


Рис. 5.13. Запрос DNS и ответ

Компьютер Ханны просто отправляет серверу запрос DNS, указывая в нем имя jessie или jessie.example.com, а сервер DNS в ответ отправляет IP-адрес (в данном случае 10.1.1.2). Фактически то же самое происходит, когда вы подключаетесь к какому-нибудь веб-сайту. Ваш ПК отправляет запрос, такой же, как компьютер Ханны отправляет для того, чтобы сервер DNS преобразовал имя компьютера Джесси в IP-адрес. После этого ПК начинает запрашивать веб-страницу.

Процесс ARP

Как только хост узнает IP-адрес другого хоста, хосту отправителя может понадобиться MAC-адрес другого компьютера. Например, компьютер Ханны должен знать MAC-адрес Ethernet, который соответствует IP-адресу 10.1.1.2, поэтому ПК Ханны начинает *рассылку ARP* (ARP broadcast). Рассылка ARP отправляется на широковещательный адрес Ethernet, поэтому ее получает каждый компьютер в локальной сети. Поскольку ПК Джесси находится в той же локальной сети, что и ПК Ханны, он получает рассылку ARP. Поскольку IP-адрес компьютера Джесси 10.1.1.2, а целью рассылки ARP является поиск MAC-адреса, связанного с этим IP-адресом, Джесси отвечает, отправляя свой MAC-адрес. Этот процесс показан на рис. 5.14.

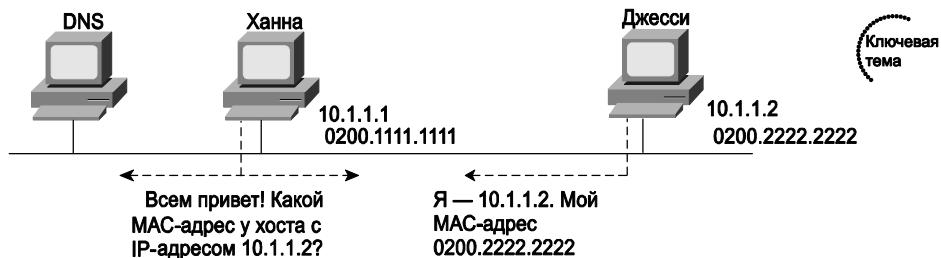


Рис. 5.14. Пример процесса ARP

Теперь компьютер Ханны знает IP-адрес получателя и адрес Ethernet, который нужно использовать для отправки фреймов компьютеру Джесси, и пакет, показанный на рис. 5.12, можно успешно отправить.

Для определения MAC-адреса получателя хосты могут использовать (а могут и не использовать) протокол ARP. Это зависит от логики двухэтапной маршрутизации, которую использует хост. Если хост получателя находится в той же подсети, то хост отправителя посылает запрос ARP, пытаясь определить MAC-адрес получателя, как показано на рис. 5.14. Но если получатель и отправитель находятся в разных подсетях, то в результате логики маршрутизации отправляющего хоста пакет нужно перенаправить на стандартный шлюз отправителя. Например, если компьютеры Ханны и Джесси расположены в разных подсетях (см. рис. 5.12–5.14), логика маршрутизации ПК Ханны заставляет этот компьютер отправлять пакеты на стандартный шлюз (маршрутизатор). В таком случае ПК Ханны, используя ARP, будет определять MAC-адреса маршрутизатора вместо MAC-адреса Джесси.

Кроме того, хостам приходится использовать ARP для определения MAC-адресов только однажды. Любое устройство, использующее протокол IP, должно сохранить или кешировать информацию, которая была получена с помощью ARP, поместив ее в свой кеш ARP. Каждый раз, собираясь отправить пакет, инкапсулированный во фрейм

Ethernet, хост сначала проверяет свой кеш ARP и использует найденный там MAC-адрес. Если в кеше ARP отсутствует корректная информация, хост может использовать ARP для определения MAC-адреса по известному IP-адресу. Кроме того, хост получает информацию ARP, получая запрос ARP. Например, процесс ARP, показанный на рис. 5.14, приводит к тому, что и Ханна, и Джесси узнают MAC-адреса друг друга.

ВНИМАНИЕ!

Содержимое кеша ARP можно просмотреть в большинстве операционных систем, используя в командной строке команду `arp -a`.

Назначение адресов и протокол DHCP

Правильный IP-адрес нужен каждому устройству, использующему TCP/IP, а точнее, каждому интерфейсу в каждом устройстве, которое использует стек TCP/IP. Для некоторых устройств адрес можно и нужно задавать статически. Например, большинство широко распространенных компьютерных операционных систем, которые поддерживают протокол TCP/IP, позволяют пользователю статически задать IP-адрес на каждом интерфейсе. Маршрутизаторы и коммутаторы также используют статически заданные IP-адреса.

Серверы также обычно используют статически заданные IP-адреса. Использование статического и редко изменяемого IP-адреса удобно потому, что все ссылки на этот сервер могут долгое время оставаться неизменными. Очень удобно, если расположение любимого гастронома не меняется и мы всегда знаем, где можно купить продукты и что можно доставить их домой по дороге с работы. Аналогичная концепция действует и для IP-адресов. Если серверы имеют статические, не изменяемые IP-адреса, то пользователи этих серверов знают, как единообразно подключаться к этим серверам из любой точки.

В то же время среднему пользовательскому компьютеру не нужно использовать один и тот же IP-адрес каждый день. Продолжая аналогию с гастрономом, можно сказать, что покупатели могут каждую неделю переезжать на новую квартиру и все равно будут знать, где находится гастроном, в то время как работникам гастронома не нужно знать, где живут покупатели. Точно так же и серверы обычно не заботятся о том, что персональные компьютеры каждый день получают другие IP-адреса. Машины конечных пользователей могут динамически получать IP-адреса и даже изменять их со временем, потому что изменение IP-адреса ни на что не влияет.

DHCP определяет протоколы, которые используются для того, чтобы выделять компьютерам IP-адреса. DHCP использует сервер, на котором хранится список диапазонов IP-адресов, доступных в каждой подсети. Клиент DHCP может отправить серверу DHCP сообщение, запрашивая выделение или аренду IP-адреса. В ответ сервер предлагает IP-адрес. Если этот адрес приемлемый, сервер отмечает, что данный адрес более не доступен для назначения другим хостам, а клиент получает в использование IP-адрес.



Наиболее важная информация, которую получает хост, работающий как клиент DHCP

Протокол DHCP предоставляет клиентам IP-адреса, а также другую информацию. Например, хост должен знать свой IP-адрес, используемую маску подсети, стандартный шлюз, а также IP-адрес (или адреса) серверов DNS. В большинстве современных сетей DHCP предоставляет конечным хостам всю эту информацию.

На рис. 5.15 показан типичный набор из четырех сообщений, которые используются между сервером и клиентом DHCP для назначения IP-адреса и передачи другой информации. Следует заметить, что два первых сообщения являются широковещательными в своей топологии.

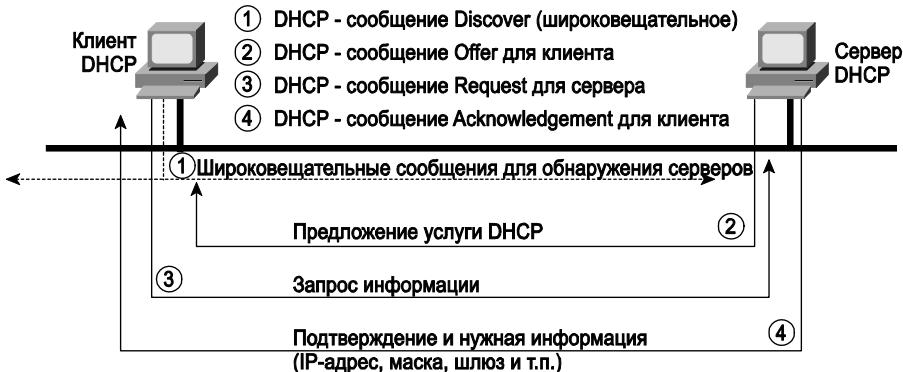


Рис. 5.15. Сообщения DHCP для получения IP-адреса

На рис. 5.15 сервер DHCP показан как компьютер, что является обычным в корпоративной сети. Однако, как будет сказано в главе 23, маршрутизаторы также могут обеспечивать службу DHCP и делают это. На самом деле маршрутизаторы могут обеспечивать функции сервера DHCP, динамически назначая IP-адреса компьютерам в небольшой домашней или офисной сети, а также использовать функции клиентов DHCP для динамического получения IP-адресов от провайдера служб Интернета (ISP). Однако необходимость использования этих функций тесно связана с подключением к Интернету. Поэтому рассмотрение подробностей реализации маршрутизаторами функций серверов и клиентов DHCP отложено до главы 23.

Протокол DHCP стал весьма распространенным. Большинство хостов конечных пользователей локальных корпоративных сетей получает свои IP-адреса и другую базовую информацию через DHCP.

Протокол ICMP эхо-запросов и команда ping

После того как сеть установлена, необходимо проверить базовую связь IP, не полагаясь на какие-либо приложения. Основным средством для проверки базовой сетевой связи является команда **ping**. Утилита **ping** (Packet Internet Groper) использует протокол управляющих сообщений Интернета (Internet Control Message Protocol — ICMP). Она отправляет на другой IP-адрес сообщение, которое называется **эхо-запрос ICMP** (ICMP echo request). Ожидается, что компьютер с этим IP-адресом пришлет **эхо-ответ ICMP** (ICMP echo reply). Если это так, то сеть успешно проверена. Иными словами, после этого можно утверждать, что сеть может доставить пакет от одного хоста к другому и обратно. Протокол ICMP не полагается на какие-либо приложения, он лишь проверяет базовую связь IP — уровни 1–3 эталонной модели OSI. Этот процесс показан на рис. 5.16.

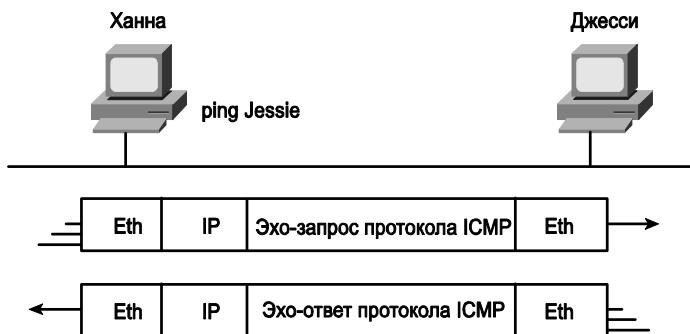


Рис. 5.16. Команда ping в сети

В главе 21 приведены более подробные сведения и примеры использования команды ping и протокола ICMP.

Подготовка к экзамену

Повторите все ключевые темы

Повторите все ключевые темы данной главы, помеченные пиктограммой “Ключевая тема”. Ключевые темы и соответствующие им страницы перечислены в табл. 5.6.

Таблица 5.6. Ключевые темы главы 5

Элемент	Описание	Страница
Список	Правила, согласно которым IP-адреса должны входить в ту же группу	150
Табл. 5.3	Величины частей сети и хоста IP-адресов без подсетей	151
Абзац	Объяснение концепции сетевых широковещательных или направленных широковещательных адресов	152
Табл. 5.5	Все возможные корректные адреса сетей	153
Рис. 5.6	Использование подсетей	155
Рис. 5.7	Форматы классовых адресов при использовании подсетей	156
Рис. 5.8	Формат бесклассовых адресов при использовании подсетей	157
Список	Двухэтапный процесс маршрутизации пакетов	157
Список	Четырехэтапный процесс маршрутизации пакетов	159
Рис. 5.10	Простой пример маршрутизации с подсетями IP	160
Рис. 5.11	Маршрутизатор R1 узнает о подсети 150.150.4.0	162
Рис. 5.13	Запрос DNS и ответ	164
Рис. 5.14	Пример процесса ARP	165
Абзац	Наиболее важная информация, которую получает хост, работающий как клиент DHCP	166

Заполните таблицы и списки по памяти

Распечатайте приложение М (Appendix L) с компакт-диска или его раздел, относящийся к этой главе, и заполните таблицы и списки по памяти. В приложении Н (Appendix M) приведены заполненные таблицы и списки для самоконтроля.

Ключевые термины

Дайте определения перечисленных ниже терминов и проверьте правильность их написания в списке терминов:

протокол ARP (ARP), стандартный шлюз и стандартный маршрутизатор (default gateway/default router), DHCP, DNS, часть хоста (host part), IP-адрес (IP address), логический адрес (logical address), широковещательный адрес сети (network broadcast address), адрес сети (network number и network address), часть сети (network part), таблица маршрутизации (routing table), широковещательный адрес подсети (subnet broadcast address), адрес подсети (subnet number и subnet address), часть подсети (subnet part).

В этой главе...

- **Протоколы 4-го уровня стека TCP/IP: TCP и UDP.** Описываются функции и механизмы, используемые протоколами TCP и UDP, включая восстановление данных после ошибок передачи и использование номеров портов.
- **Приложения TCP/IP.** Описывается назначение протоколов TCP/IP уровня приложений; в качестве примера более подробно рассматривается протокол HTTP.
- **Безопасность сети.** Рассматриваются возникающие в настоящее время угрозы безопасности сети; описаны некоторые важнейшие меры для предотвращения таких угроз и уменьшения их последствий.

ГЛАВА 6

Основы протокола TCP/IP: передача данных, приложения и безопасность

На сертификационном экзамене CCNA основное внимание уделяется углубленному и расширенному изучению тем, рассмотренных в главе 3 (локальные сети LAN), главе 4 (распределенные сети WAN) и в главе 5 (маршрутизация). В настоящей главе рассматриваются базовые положения некоторых тем, которым уделяется меньше внимания на экзамене: транспортный уровень протокола TCP/IP, уровень приложений протокола TCP/IP и обеспечение безопасности сети. Хотя эти три темы входят в программу курса CCNA, вопросов по ним в экзамене значительно меньше, чем по сетям LAN, WAN и маршрутизации.

Контрольные вопросы: знаете ли вы уже темы главы

Этот раздел предназначен для того, чтобы читатель мог предварительно оценить свои знания и решить, нужно ли ему читать главу целиком. Если ответы на девять из десяти вопросов даны правильно, то можно сразу же перейти к последнему разделу “Подготовка к экзамену”. В табл. 6.1 перечислены основные темы этой главы и номера предварительных контрольных вопросов, относящихся к соответствующим темам. Используя эту таблицу и отвечая на контрольные вопросы, читатель сможет достаточно точно оценить свои знания в той или иной области. Ответы на вопросы приведены в приложении А.

Таблица 6.1. Темы контрольных вопросов

Основная тема	Номера вопросов
Протоколы 4-го уровня стека TCP/IP: TCP и UDP	1–6
Приложения TCP/IP	7, 8
Безопасность сети	9, 10

1. Компьютер ПК1 использует протокол TCP и имеет окно размером 4000. ПК1 посыпает компьютеру ПК2 четыре сегмента, каждый из которых имеет размер 1000 байтов, с последовательными номерами 2000, 3000, 4000 и 5000. Компьютер ПК2 не получает подтверждения на протяжении установленного периода для данного соединения. Что должен после этого сделать компьютер ПК1?

- а) Увеличить размер своего окна до 5000 или более сегментов.
- б) Отправить следующий сегмент с последовательным номером 6000.
- в) Повторно отправить сегмент с номером 5000.
- г) Повторить отправку всех четырех ранее отправленных сегментов.

2. Какие из перечисленных ниже функций не являются необходимыми для протокола, который считается соответствующим 4-му уровню эталонной модели OSI?
 - а) Восстановление после ошибок передачи.
 - б) Управление потоком.
 - в) Сегментация данных приложений.
 - г) Преобразование из бинарной формы в формат ASCII.
3. Какие из приведенных ниже полей заголовка указывают, какому из приложений TCP/IP следует передать данные, полученные компьютером? (Выберите несколько ответов.)
 - а) Тип сети Ethernet (Ethernet Type).
 - б) Тип протокола SNAP.
 - в) Поле протокола IP.
 - г) Номер порта TCP.
 - д) Номер порта UDP.
 - е) Идентификатор (ID) приложения.
4. Какие из перечисленных ниже функций не являются типичными для протокола TCP? (Выберите несколько ответов.)
 - а) Использование оконного механизма (windowing).
 - б) Восстановление данных после ошибок.
 - в) Мультиплексирование с использованием номеров портов.
 - г) Маршрутизация.
 - д) Шифрование данных.
 - е) Упорядоченная передача данных.
5. Какая из перечисленных ниже функций поддерживается как протоколом TCP, так и протоколом UDP?
 - а) Использование оконного механизма (windowing).
 - б) Восстановление после ошибок.
 - в) Мультиплексирование с использованием номеров портов.
 - г) Маршрутизация.
 - д) Шифрование данных.
 - е) Упорядоченная передача данных.
6. Как называются данные, которые включают в себя заголовок протокола 4-го уровня, и данные, переданные 4-му уровню вышележащими уровнями, но не включают в себя заголовки и концевики уровней 1–3? (Выберите несколько ответов.)
 - а) Биты.
 - б) Блок (chunk).
 - в) Сегмент.
 - г) Пакет.

- д) Фрейм.
е) L4PDU.
ж) L3PDU.
7. Какая часть адреса URL <http://www.certskills.com/name.html> указывает имя веб-сервера?
- а) http.
б) www.certskills.com.
в) certskills.com.
г) <http://www.certskills.com>.
д) Имя файла name.html включает в себя имя хоста.
8. При сравнении приложения VoIP с критически важным коммерческим приложением HTTP какое из приведенных ниже утверждений точно характеризует качество обслуживания, требуемое от сети? (Выберите несколько ответов.)
- а) VoIP требует меньшего уровня утери пакетов.
б) Протоколу HTTP требуется меньшая полоса пропускания.
в) Протокол HTTP требует более низкого уровня флуктуации задержки.
г) VoIP требует меньшей величины задержки.
9. Что из перечисленного ниже является устройством или функцией, важнейшей задачей которой является отслеживание во времени тенденций, чтобы распознать различные известные атаки по списку общих сигнатур атак?
- а) VPN.
б) Брандмауэр.
в) IDS.
г) NAC.
10. Для какого из перечисленных ниже устройств или функции важнейшей задачей является шифрование пакетов перед передачей их через Интернет?
- а) VPN.
б) Брандмауэр.
в) IDS.
г) NAC.

Основные темы

Данная глава начинается с рассмотрения функций *протокола управления передачей* (Transmission Control Protocol — TCP), которые весьма многочисленны по сравнению с функциями *протокола пользовательских дейтаграмм* (User Datagram Protocol — UDP). Во втором разделе главы рассматривается уровень приложений протокола TCP/IP, в частности обсуждается работа службы DNS. В третьем разделе обсуждаются важность сетевой безопасности и методы ее обеспечения, включая некоторые базовые концепции, терминологию и функции, важные для современного подхода к обеспечению безопасности.

Протоколы 4-го уровня стека TCP/IP: TCP и UDP

Транспортный уровень эталонной модели OSI (4-й уровень) определяет несколько функций, наиболее важными из которых являются восстановление данных при ошибках передачи и управление потоком. Протоколы TCP/IP транспортного уровня реализуют эти функции. Следует обратить внимание на то, что как в эталонной модели OSI, так и в модели TCP/IP этот уровень называется транспортным. Однако, как обычно, когда речь идет о модели TCP/IP, имя и номер уровня базируются на эталонной модели OSI, поэтому все протоколы TCP/IP транспортного уровня рассматриваются как протоколы 4-го уровня.

Принципиальное различие между протоколами TCP и UDP состоит в том, что по сравнению с UDP протокол TCP обеспечивает приложениям значительно более широкий диапазон служб. Например, маршрутизаторы по многим причинам могут отбрасывать пакеты, включая битовые ошибки, переполнение и ситуации, в которых правильный маршрут неизвестен. Как уже говорилось, большинство протоколов канального уровня фиксирует факт ошибки при передаче (этот процесс называется *обнаружением ошибок* (error detection)), а затем отбрасывают фреймы с ошибками. Протокол TCP обеспечивает повторную передачу (восстановление после ошибок передачи) и помогает избежать переполнения (управление потоком), в то время как протокол UDP таких функций не имеет. Вследствие этого во многих протоколах приложений предпочтительным оказывается использование протокола TCP.

Однако из-за недостатка служб в протоколе UDP не следует делать вывод, что этот протокол уступает протоколу TCP. Меньшее количество служб позволяет протоколу UDP использовать меньше байтов в заголовке, чем протоколу TCP, что приводит к уменьшению служебной нагрузки в сети. Программное обеспечение протокола UDP не вызывает замедления передачи данных в тех случаях, когда работа TCP целенаправленно замедляется. К этому следует добавить, что некоторые приложения, особенно современные технологии *передачи голоса по сети IP* (Voice Over IP — VoIP), не требуют восстановления данных после ошибок и поэтому в них используется протокол UDP. Вследствие этого протокол UDP по-прежнему играет большую роль в современных сетях TCP/IP.

В табл. 6.2 перечислены основные функции, которые поддерживаются протоколами TCP и/или UDP. Следует обратить внимание на то, что лишь первый пункт таблицы поддерживается протоколом UDP, в то время как протоколом TCP поддерживаются все перечисленные в таблице функции.



Таблица 6.2. Функции транспортного уровня модели TCP/IP

Функция	Описание
Мультиплексирование с использованием портов	Функция, позволяющая хосту-получателю по номеру порта выбрать приложение, для которого предназначены полученные данные
Восстановление после ошибок (надежность)	<i>Нумерация</i> (numbering) и подтверждение получения данных с помощью полей заголовка Sequence (Последовательный номер) и Acknowledgment (Подтверждение)
Управление потоком с использованием окон	Использование размеров окон для защиты от переполнения буфера в маршрутизаторах и хостах
Установка и прекращение соединения	Процесс инициализации номеров портов и полей Sequence (Последовательный номер) и Acknowledgment (Подтверждение)
Упорядоченная передача данных и их сегментация	Непрерывный поток байтов от процесса более высокого уровня “сегментируется” для передачи и передается процессам верхних уровней принимающего устройства с тем же самым порядком следования байтов

Далее в настоящем разделе описываются функции протокола TCP и выполняется их сравнение с функциями протокола UDP.

Протокол управления передачей

В каждом приложении TCP/IP обычно выбирается протокол TCP или UDP, в зависимости от требований приложения. Например, протокол TCP обеспечивает восстановление после ошибок, однако для этого требуется большая полоса пропускания и используется большее количество циклов обработки. Протокол UDP не осуществляет коррекцию ошибок, но требует меньшую полосу пропускания и использует меньшее количество циклов обработки. Независимо от того, какой из двух протоколов транспортного уровня TCP/IP выбран для использования приложением, требуется понимать базовые принципы работы каждого из этих протоколов транспортного уровня.

Протокол TCP, описанный в документе RFC 793, выполняет свои функции, перечисленные в табл. 6.2, используя механизмы конечных компьютеров. Работа протокола TCP базируется на протоколе IP для сквозной (end-to-end) доставки данных, включая вопросы маршрутизации. Иными словами, протокол TCP выполняет лишь часть функций, необходимых для доставки данных от одного приложения к другому. Кроме того, выполняемая им роль направлена на обеспечение служб для приложений, которые располагаются на конечном компьютере. Независимо от того, находятся ли оба компьютера в локальной сети Ethernet или разделены огромными участками в Интернете, протокол TCP выполняет свои функции одним и тем же образом.

На рис. 6.1 показаны поля заголовка протокола TCP. Хотя нет необходимости запоминать все имена полей или их расположение, в оставшейся части раздела будут упоминаться некоторые из этих полей, поэтому в справочных целях ниже приводится весь заголовок.



Рис. 6.1. Поля заголовка протокола TCP

Мультиплексирование с использованием номеров портов протокола TCP

Протокол TCP предоставляет приложениям множество функций, хотя для этого требуются несколько больший объем обработки данных и увеличенная по сравнению с UDP служебная нагрузка. Однако оба протокола — TCP и UDP — используют метод, называемый *мультиплексированием* (multiplexing). Поэтому данный раздел начинается с описания мультиплексирования в протоколах TCP и UDP. Далее будут рассмотрены функции, уникальные только для протокола TCP.

Мультиплексирование в протоколах TCP и UDP включает в себя процесс принятия решения компьютером при получении данных. Возможны ситуации, когда на компьютере работает несколько приложений, таких как веб-браузер, электронная почта или приложение VoIP (например, Skype). Мультиплексирование в протоколах TCP и UDP позволяет получающему данные компьютеру определять, какому из работающих приложений следует передать полученные данные.

Приведенные ниже примеры помогут понять необходимость мультиплексирования. В рассматриваемом ниже примере сеть состоит из двух персональных компьютеров (ПК), с именами Ханна и Джесси. Компьютер Ханны использует приложение, предназначенное для рассылки рекламных сообщений, которые появляются на экране компьютера Джесси. Это приложение каждые 10 секунд посылает Джесси новое рекламное сообщение. На компьютере Ханны используется другое приложение, осуществляющее перевод денег для их пересылки компьютеру Джесси. Кроме того, на компьютере Ханны работает веб-браузер, используемый для доступа к веб-серверу, работающему на компьютере Джесси. Рекламное приложение и приложение перевода денег используются в данном примере лишь для иллюстрации. Веб-приложение работает точно так же, как это было бы в реальной жизни.

На рис. 6.2 показан пример такой сети, в которой на компьютере Джесси работают три приложения.

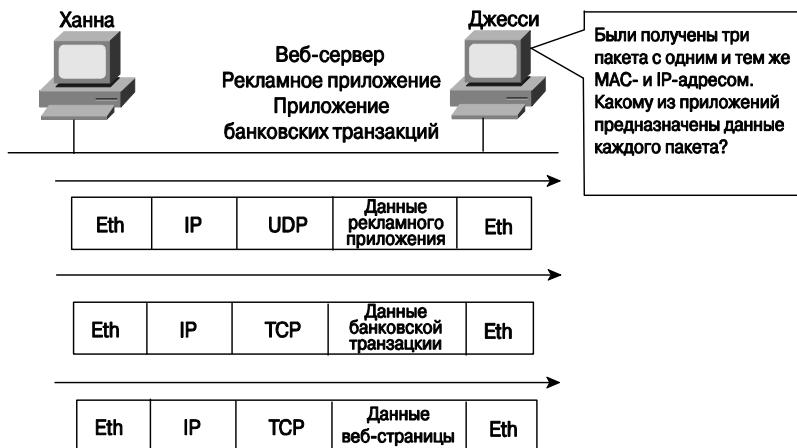


Рис. 6.2. Компьютер Ханны отправляет пакеты компьютеру Джесси с использованием трех приложений

- Рекламное приложение на основе протокола UDP.
- Приложение по переводу денег на основе протокола TCP.
- Веб-сервер на основе протокола TCP.

Компьютеру Джесси требуется знать, какому приложению следует передать данные, однако все три пакета пришли с одних и тех же адресов Ethernet и IP. Может показаться, что компьютер Джесси может решить эту проблему на основе заголовка UDP или TCP в пакете, однако, как показано на рисунке, два из трех приложений используют один и тот же протокол TCP.

Протоколы TCP и UDP решают эту проблему, используя поле номера порта в заголовке протокола TCP или протокола UDP соответственно. Каждый из сегментов TCP и UDP компьютера Ханны использует отличный от других *номер порта получателя* (*destination port number*), поэтому компьютер Джесси знает, какому приложению следует передать данные. На рис. 6.3 показан пример такой ситуации.

Мультиплексирование базируется на понятии *сокета* (socket). Сокет состоит из трех частей:

- IP-адрес;
- транспортный протокол;
- номер порта.

Поэтому для веб-сервера на компьютере Джесси сокет будет иметь вид (10.1.1.2, TCP, порт 80), поскольку стандартно веб-серверы используют общеизвестный порт 80. При подключении веб-браузера на компьютере Ханны к веб-серверу также используется сокет — вероятно, имеющий вид (10.1.1.1, TCP, 1030). Почему 1030? Просто потому, что компьютеру Ханны требуется номер порта, который был бы уникальным для компьютера Ханны, и, поскольку порт 1030 доступен, использует

его. На самом деле хосты обычно выделяют для использования динамические номера портов, начинающиеся с 1024, поскольку порты с номерами, меньшими 1024, зарезервированы для общеизвестных приложений, таких, например, как веб-службы.

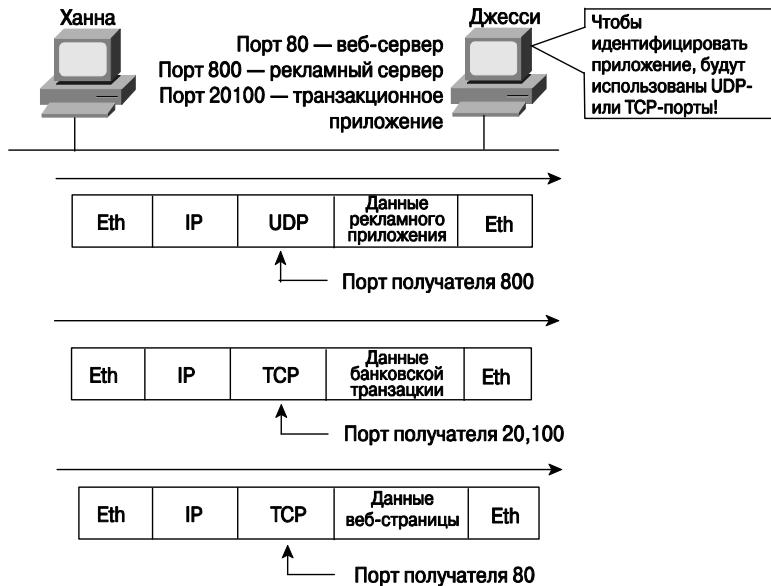


Рис. 6.3. Компьютер Ханны посылает пакеты компьютеру Джесси; при этом три приложения для мультиплексирования используют номера портов

На рис. 6.3 Ханна и Джесси используют одновременно три приложения, следовательно, при этом открыты три сокета соединений. Поскольку сокет на каждом отдельном компьютере должен быть уникальным, соединение между двумя сокетами должно уникальным образом идентифицировать соединение между двумя компьютерами. Эта уникальность означает, что можно использовать несколько приложений одновременно, обращаясь к приложениям, работающим на одном и том же компьютере или на различных компьютерах. Мультиплексирование на базе сокетов обеспечивает доставку данных требуемым приложениям. На рис. 6.4 показаны три сокета соединений между компьютерами Ханны и Джесси.

Номера портов являются важнейшей частью концепции сокетов. Общеизвестные номера портов используются серверами, остальные номера портов используются клиентами. Приложения, поддерживающие службы, такие как FTP, Telnet и веб-серверы, открывают сокет, используя общеизвестные порты, и прослушивают их на предмет запросов на соединение. Поскольку от этих запросов на соединение требуется, чтобы они включали в себя номера портов как отправителя, так и получателя, номера портов, используемые серверами, должны быть общеизвестными. Поэтому стандартные службы используют общеизвестные номера портов. Общеизвестные порты перечислены на странице сайта <http://www.iana.org/assignments/port-numbers>.

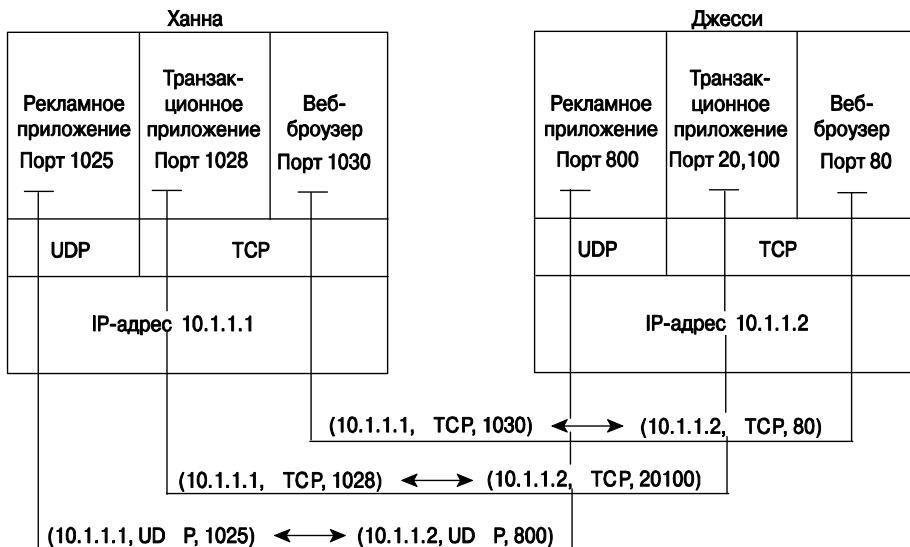


Рис. 6.4. Соединения между сокетами

На клиентских машинах, где инициируются запросы, для сокета может быть выделен любой неиспользуемый порт. В результате каждый клиент на одном и том же хосте использует отличный от других номер порта, однако сервер использует для всех соединений один и тот же номер порта. Например, 100 веб-браузеров на одном и том же компьютере могут иметь каждый свое соединение с одним и тем же веб-сервером, однако этот веб-сервер с подсоединенными к нему 100 клиентами будет использовать только один сокет и, соответственно, только один номер порта (в данном случае номер 80). Сервер может отличить пакеты любого из 100 клиентов друг от друга, просматривая порт отправителя в полученных сегментах TCP. Сервер может посыпать данные требуемому клиенту (браузеру) отправляя данные на тот номер порта, который был указан в качестве порта получателя. Комбинация сокетов отправителя и получателя позволяет всем хостам, участвующим в обмене данными, отличать отправителей от получателей передаваемых данных. Хотя в данном примере концепция мультиплексирования была проиллюстрирована на примере 100 соединений протокола TCP, этот же метод нумерации портов относится равным образом и к сеансам протокола UDP.

ВНИМАНИЕ!

Все документы RFC можно найти на сайте по адресу <http://www.isi.edu/in-notes/rfcxxxx.txt>, где xxxx — номер документа RFC. Если вы не знаете номер документа RFC, то можно выполнить тематический поиск на сайте по адресу <http://www.rfc-editor.org/rfcsearch.html>.

Популярные приложения протокола TCP/IP

На протяжении всей подготовки к экзамену CCNA вы встретите ряд приложений TCP/IP. Вы должны по меньшей мере знать о тех из них, которые могут быть использованы для управления и контроля сети.

Приложения World Wide Web (WWW) работают через веб-браузеры, получая таким образом содержимое, доступное на веб-серверах. Хотя WWW часто рассматривается как приложение конечного пользователя, в действительности возможно использование WWW для управления маршрутизатором или коммутатором. Для этого на маршрутизаторе или коммутаторе включается функция веб-сервера, а браузер используется для получения доступа к этим устройствам.

Система доменных имен (Domain Name System — DNS) позволяет пользователю использовать имена для ссылки на компьютеры, а служба DNS используется для нахождения соответствующих IP-адресов. Система DNS использует также модель “клиент–сервер”; при этом серверы DNS управляются сетевым персоналом, а клиентские функции DNS, как правило, являются в настоящее время частью любого устройства, использующего протокол TCP/IP. Клиент просто запрашивает у сервера DNS IP-адрес, соответствующий указанному имени.

Простой протокол управления сетью (Simple Network Management Protocol — SNMP) является протоколом уровня приложений, специально предназначенным для управления сетевыми устройствами. Например, компания Cisco поставляет на рынок разнообразные продукты управления сетью, многие из которых являются частью семейства CiscoWorks — программных продуктов управления сетью. Они могут использоваться для запроса, компиляции (сбора), хранения и отображения информации о работе сети. Для выполнения запросов к сетевым устройствам программное обеспечение CiscoWorks использует главным образом протоколы SNMP.

Для перемещения файлов на маршрутизатор, или коммутатор, или в обратном направлении программное обеспечение Cisco традиционно использовало *простейший протокол передачи файлов* (Trivial File Transfer Protocol — TFTP). TFTP определяет протокол для базовой передачи — этим и объясняется термин “простейший” (trivial). Альтернативным вариантом является использование маршрутизаторами и коммутаторами *протокола передачи файлов* (File Transfer Protocol — FTP), который имеет значительно больше функций для передачи файлов. Оба протокола успешно выполняют задачи передачи файлов на устройства Cisco и от них. Протокол FTP имеет значительно больше функций, что делает его наилучшим выбором для обычного (general) конечного пользователя. Клиентские и серверные приложения протокола TFTP очень просты и поэтому являются удобными инструментами в качестве встроенных частей сетевых устройств.

Одни из этих приложений используют протокол TCP, другие — протокол UDP. Как будет показано далее, протокол TCP осуществляет восстановление после ошибок передачи, в то время как протокол UDP не выполняет такой функции. Например, *простой протокол передачи почты* (Simple Mail Transport Protocol — SMTP) и *почтовый протокол версии 3* (Post Office Protocol 3 — POP3), используемые для передачи электронной почты, требуют гарантированной доставки, поэтому в них используется протокол TCP. Независимо от того, какой протокол транспортного уровня используется, приложения используют общеизвестный номер порта, поэтому клиенты знают, к какому порту следует подключиться. В табл. 6.3 перечислены некоторые популярные приложения и их общеизвестные номера портов.

Таблица 6.3. Популярные приложения и их общеизвестные номера портов



Номер порта	Протокол	Приложение
20	TCP	Передача данных протокола FTP
21	TCP	Управление протоколом FTP
22	TCP	SSH
23	TCP	Telnet
25	TCP	SMTP
53	UDP, TCP	DNS
67, 68	UDP	DHCP
69	UDP	TFTP
80	TCP	HTTP (WWW)
110	TCP	POP3
161	UDP	SNMP
443	TCP	SSL
16 384–32 767	UDP	Передача голоса по сети IP (VoIP)

Восстановление после ошибок (надежность)

Протокол TCP обеспечивает надежную передачу данных. В различных документах она называется *надежностью* (reliability), или *восстановлением данных после ошибок передачи* (error recovery). Для обеспечения надежности протокол TCP нумерует блоки данных, используя для этого поля последовательного номера (SEQ) и подтверждения (ACK) в заголовке TCP. На рис. 6.5 показана типичная операция передачи данных.

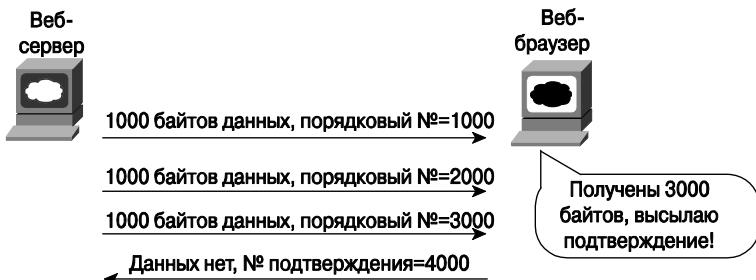


Рис. 6.5. Подтверждение безошибочной передачи данных в протоколе TCP

На рис. 6.5 поле подтверждения в заголовке TCP, отправленном веб-клиентом (4000), указывает на готовность принять следующий байт; такая ситуация называется *прямым подтверждением* (forward acknowledgment). Последовательный номер указывает номер первого байта в сегменте. В данном случае каждый сегмент TCP имеет длину 1000 байтов; количество байтов подсчитывается в полях последовательного номера и подтверждения.

На рис. 6.6 отображена аналогичная ситуация, однако второй сегмент TCP оказался утерянным или был передан с ошибками. В ответе веб-клиента в поле подтверждения содержится значение 2000, указывающее на то, что веб-клиент ожидает

следующий байт с номером 2000. В этом случае функция протокола TCP на веб-сервере может восстановить утерянные данные повторной отправкой второго сегмента TCP. Протокол TCP позволяет повторно отправить только этот сегмент и ожидать ответа веб-клиента с подтверждением, равным 4000.

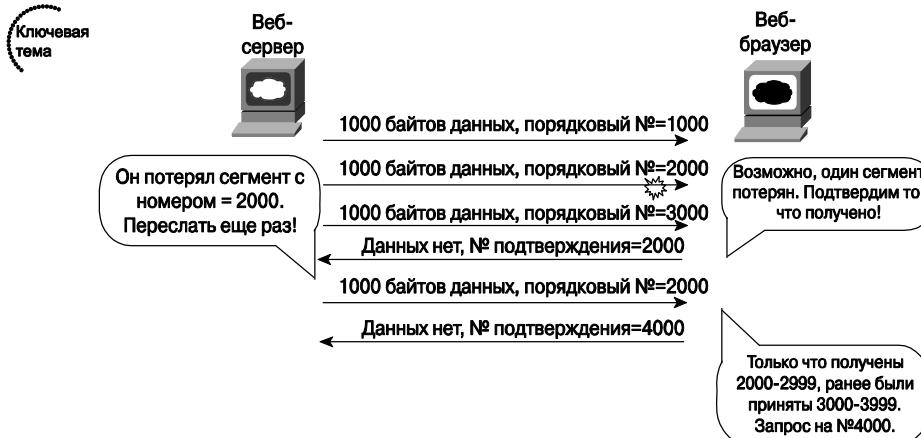


Рис. 6.6. Подтверждение протокола TCP в случае ошибки передачи

Хотя это и не показано на рисунке, отправитель также устанавливает таймер повторной передачи для сегмента, ожидая подтверждения, на случай, если подтверждение утеряно или утеряны все переданные сегменты. Если время таймера истекло, то отправитель TCP отправляет этот сегмент повторно.

Управление потоком с использованием окон

Протокол TCP выполняет управление потоком с помощью полей последовательного номера и подтверждения в заголовке TCP, а также поля, называемого размером окна. Это поле указывает максимальное количество неподтвержденных байтов, которое допускается в любой момент времени. Сначала окно имеет небольшой размер и постепенно увеличивается до тех пор, пока не появятся ошибки передачи. Размер окна изменяется с течением времени, поэтому оно иногда называется *динамическим окном* (dynamic window). Кроме того, поскольку порядковый номер и номер подтверждения с течением времени возрастают, это окно иногда называют *скользящим окном* (sliding window), номера которого “скользят” в сторону увеличения. Когда окно заполнено, отправитель прекращает передачу, что позволяет управлять потоком данных. На рис. 6.7 показано использование окна с текущим размером, равным 3000. Каждый сегмент TCP содержит 1000 байт данных.

Следует обратить внимание на то, что веб-сервер должен перейти в режим ожидания после отправки третьего сегмента, поскольку окно уже заполнено. Следующее окно может быть отправлено после получения подтверждения. Поскольку при передаче не было ошибок, веб-клиент предоставляет серверу окно большего размера, поэтому можно отправить 4000 байт до получения сервером подтверждения. Иными словами, получатель использует поле размера окна для того, чтобы сообщить отправителю, какое количество данных последний может отправить перед тем, как прекратить передачу и ожидать следующего подтверждения.

Как и в отношении других функций TCP, оконный механизм передачи используется в обоих направлениях. Обе стороны отправляют и получают данные, и в каждом случае получатель согласовывает количество передаваемых данных, используя поле размера окна.

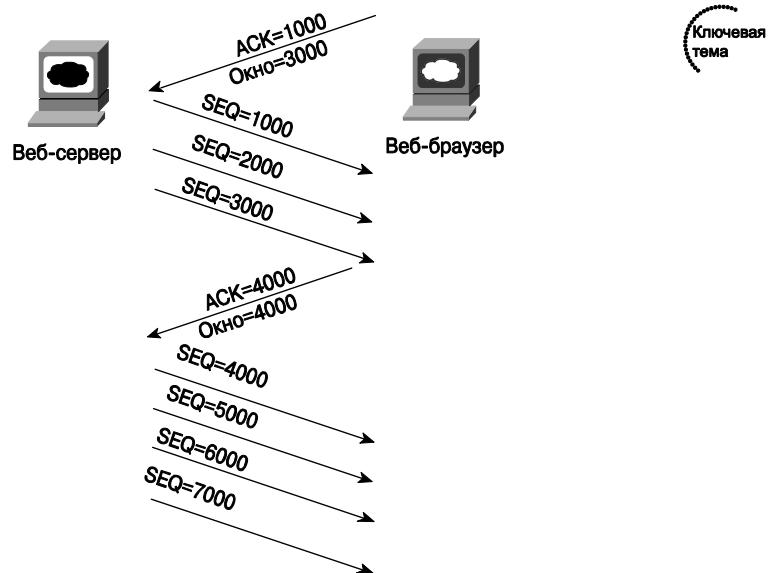


Рис. 6.7. Использование окон в протоколе TCP

Использование оконного механизма не обязательно требует прекращения передачи данных. Если подтверждение получено до того, как окно оказалось заполненным, то открывается новое окно, и отправитель продолжает передачу до тех пор, пока текущее окно не окажется заполненным. (Для описания функций восстановления после ошибок и использования окон, реализуемых протоколом TCP, иногда используется термин *позитивное подтверждение и повторная передача* (Positive Acknowledgment and Retransmission — PAR).)

Установка и разрыв соединения

Перед тем как начнет работать какая-либо из функций протокола TCP, происходит установка соединения. Под установкой соединения понимается процесс инициализации полей последовательного номера и подтверждения, а также согласование номеров используемых портов. На рис. 6.8 приведен пример потока передаваемых данных при установке соединения.

Этот трехэтапный обмен данными при установке соединения должен закончиться перед тем, как начнется передача данных. Соединение существует между двумя сокетами, хотя в заголовке TCP нет отдельного поля сокета. Предполагается, что из трех частей сокета IP-адреса могут быть получены из полей IP-адресов отправителя и получателя в заголовке протокола IP. Подразумевается протокол TCP, поскольку используется заголовок протокола TCP, который указан в поле протокола в заголовке IP. Поэтому единственной частью сокета, которая должна быть закодирована в заголовке TCP, являются номера портов.

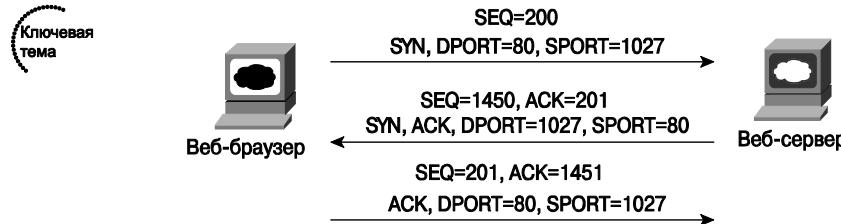


Рис. 6.8. Установка соединения протокола TCP

Протокол TCP сообщает об установке соединения, используя 2 бита в полях флагов заголовка TCP. Эти биты называются флагами SYN и ACK и имеют особо важное значение. Аббревиатура SYN означает “Синхронизировать последовательные номера”, что является необходимым компонентом инициализации для протокола TCP. Аббревиатура ACK означает “Поле подтверждения в данном заголовке является действительным”. До тех пор пока порядковые номера не инициализированы, поле подтверждения не приносит пользы. Отметим также, что в первоначальном сегменте TCP на рис. 6.8 номер подтверждения не показан; это связано с тем, что данный номер пока недействителен. Поскольку поле подтверждения (ACK) должно присутствовать во всех последующих сегментах, бит подтверждения будет устанавливаться до тех пор, пока соединение не будет прекращено.

Протокол TCP инициализирует поля порядкового номера (SEQ) и номера подтверждения (ACK) любым числом, которое умещается в 4-байтовом поле; значения, приведенные на рис. 6.8, являются произвольными и используются для примера. Предполагается, что в каждом потоке при инициализации передается по одному байту данных, как показано в полях номеров подтверждений в приведенном примере.

На рис. 6.9 показан разрыв соединения протокола TCP. Эта четырехэтапная последовательность является достаточно простой и использует дополнительный флаг, называемый *битом FIN* (FIN bit) (как, вероятно, догадался читатель, аббревиатура FIN является сокращением от “finished”). Хотелось бы сделать одно интересное замечание: перед тем, как устройство, расположенное на рисунке справа, отправит третий сегмент TCP в данной последовательности, оно уведомляет приложение о том, что соединение отключается. После этого оно ожидает подтверждения от приложения и лишь затем отправляет третий из показанных на рисунке сегментов. В случае, если приложению требуется некоторое время для ответа, компьютер ПК справа отправляет второй из показанных на рисунке потоков данных, подтверждая то, что другой компьютер намерен разорвать соединение. В противном случае компьютер, показанный на рисунке слева, может повторно отправить первый сегмент.

Ключевая тема Определения протоколов, ориентированных и не ориентированных на соединение

- *Протокол с установлением соединения.* Протокол, которому перед началом передачи данных необходим обмен сообщениями между устройствами.
- *Протокол без установления соединения.* Протокол, которому не требуется обмен сообщениями между устройствами и заранее установленной связи между конечными точками.

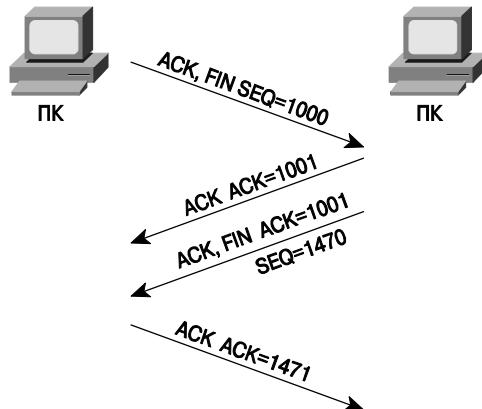


Рис. 6.9. Разрыв соединения в протоколе TCP

Сегментация данных и упорядоченная передача данных

Приложениям требуется отправлять данные. Иногда эти данные имеют небольшой объем — в некоторых случаях всего один байт. В других случаях, например, при передаче файлов, объем данных может достигать миллионов байтов.

Каждый тип протокола канального уровня обычно имеет ограничение на размер *максимального блока передачи* (Maximum Transmission Unit — MTU), который может быть отправлен во фрейме канального уровня. Иными словами, блок MTU определяет максимальный размер пакета 3-го уровня, который может быть размещен в поле данных фрейма. Для многих протоколов канального уровня, в частности для Ethernet, размер блока MTU составляет 1500 байтов.

Поскольку приложению может потребоваться передача миллионов байтов, протокол TCP сегментирует данные в блоки меньшего размера, называемые *сегментами* (segment). Так как пакет протокола IP может иметь размер не более 1500 байтов (из-за ограничений MTU), а заголовки IP и TCP имеют размер 20 байтов каждый, TCP обычно сегментирует данные в *блоки* (chunk) размером 1460 байтов.

При получении сегментов получатель TCP осуществляет *сборку* (reassembly) данных. Для этого протокол TCP должен восстановить утерянные сегменты, как это было описано ранее. Однако получатель TCP должен также восстановить первоначальный порядок сегментов, который может нарушаться при передаче. Поскольку при маршрутизации IP возможно балансирование потоков данных по нескольким каналам, на практике сегменты могут доставляться не в том порядке, в каком они были отправлены. Поэтому получатель протокола TCP должен также обеспечивать *упорядоченную передачу данных* (ordered data transfer) за счет восстановления первоначального порядка следования сегментов. Этот процесс легко себе представить: если сегменты поступают в последовательности 1000, 3000 и 2000 и каждый из них содержит 1000 байтов данных, то получатель может изменить их порядок, и повторной передачи не потребуется.

С сегментацией TCP связаны некоторые специальные термины, которые рассматриваются ниже. Заголовок протокола TCP вместе с полем данных называется *сегментом TCP* (TCP segment). Этот термин аналогичен понятию фрейма канального уровня или пакета IP в том смысле, что он относится к заголовкам и концевикам со-

ответствующих уровней вместе с инкапсулированными данными. Вместо термина *сегмент TCP* может также использоваться аббревиатура L4PDU, поскольку TCP является протоколом 4-го уровня.

Протокол пользовательских дейтаграмм

Протокол UDP обеспечивает для приложений службу обмена сообщениями. В отличие от протокола TCP, этот протокол не ориентирован на соединение и не обеспечивает надежности, не использует окон и не восстанавливает порядок полученных данных. Он также не сегментирует крупные блоки данных в блоки подходящего для передачи размера.

Однако протокол UDP обеспечивает выполнение некоторых функций протокола TCP, таких как передача данных и мультиплексирование с использованием номеров портов. Для этого ему требуется меньшее количество байтов служебной нагрузки и меньше времени для обработки, чем протоколу TCP.

Передача данных по протоколу UDP отличается от передачи по протоколу TCP тем, что при этом не происходит упорядочения данных или их восстановления. Приложения, использующие протокол UDP, должны быть толерантны к утере данных или иметь какие-либо собственные механизмы восстановления утерянных данных. Например, в технологии VoIP используется протокол UDP, поскольку в случае утери пакета к моменту обнаружения этой потери и возможной повторной передачи накопится задержка и голос станет плохо различимым. В службе доменных имен DNS также используется протокол UDP, поскольку в случае неудачной операции по преобразованию имени пользователь может повторить попытку. Еще одним примером может служить *сетевая файловая система* (Network File System — NFS), приложение дистанционной файловой системы, которое восстанавливает данные с помощью кода уровня приложений, поэтому набор функций протокола UDP для NFS является приемлемым.

На рис. 6.10 показаны форматы заголовков для протоколов TCP и UDP. Следует обратить внимание на то, что поля порта отправителя (Source Port) и порта получателя (Destination Port) присутствуют как в заголовке TCP, так и в заголовке UDP, однако в заголовке UDP отсутствуют поля последовательного номера и подтверждения. Протоколу UDP эти поля не требуются, так как он не пытается пронумеровать данные для подтверждения или упорядочения.

2	2	4	4	4 бита	6 битов	6 битов	2	2	2	3	1
Порт отправителя	Порт получателя	Порядковый номер	Номер подтверждения	Смещение	Зарезервировано	Флаги	Размер окна	Контрольная сумма	Срочность	Опции	Заполнение
TCP-заголовок											
2	2	2	2								
Порт отправителя	Порт получателя	Длина	Контрольная сумма								

UDP-заголовок

* Если не указано явно, то длина поля измеряется в байтах

Рис. 6.10. Заголовки протоколов TCP и UDP

Не используя поля последовательного номера и подтверждения, протокол UDP получает некоторые преимущества в сравнении с протоколом TCP. Наиболее важным из них является то, что UDP использует меньшее количество байтов служебной нагрузки. Не столь очевидным является то, что протоколу UDP не требуется ожидать подтверждений и до их получения удерживать данные в памяти. Это означает, что приложения, использующие протокол UDP, не испытывают искусственной задержки, вызываемой процессом подтверждения, и их память быстрее освобождается.

Приложения TCP/IP

Вообще говоря, целью построения корпоративной сети, подключения небольшой домашней сети или офисной сети к Интернету является использование приложений, таких, как просмотр веб-сайтов, обмен текстовыми сообщениями, электронная почта, загрузка файлов, передача голосовых данных и видеоданных. В настоящем разделе рассматриваются некоторые вопросы проектирования сети в свете использования приложений, которые будут работать в данной сети. Далее будет более подробно рассмотрена работа одного конкретного приложения — веб-браузера, использующего протокол передачи гипертекста (Hypertext Transfer Protocol — HTTP).

Качество обслуживания в приложениях TCP/IP

За последние годы потребности работающих в сети приложений значительно возросли. Когда в 1970-х годах стали популярными корпоративные сети, типичные сети поддерживали только приложения, работающие с обычными данными, главным образом текстовые терминалы и принтеры, которые могли работать только с текстами. В таких ситуациях отдельный пользователь может передавать в сеть несколько сот байтов данных при каждом нажатии клавиши <Enter>, что происходит примерно каждые 10 секунд.

Термин *качество обслуживания* (Quality of Service — QoS) описывает в целом требования приложения к работе сетевой службы. Каждый тип приложения может быть проанализирован в отношении требований QoS, предъявляемых им к сети, и если сеть удовлетворяет этим требованиям, то приложение может эффективно работать. Например, типичные для того времени интерактивные приложения, работающие только с текстом, требовали незначительной полосы пропускания, однако для них было весьма желательным уменьшение задержки. Если тогдашняя сеть поддерживала передачу данных к получателю и обратно (round-trip) с задержкой менее одной секунды, то пользователь оставался удовлетворенным, поскольку ему приходилось ждать ответа не более одной секунды.

Однако за прошедшие годы требования к качеству обслуживания QoS значительно изменились. Говоря в целом, приложениям требовалась все большая полоса пропускания и все меньшая задержка. С тех пор на рынке появились следующие приложения, оказавшие существенное влияние на характер работы в сети.

- Работающие с графикой терминалы и принтеры, которые по сравнению с аналогичными прежними текстовыми устройствами требуют значительно большего количества байтов для выполнения тех же действий.
- Приложения для передачи файлов, которые используют значительно большие объемы данных, однако не требуют значительно более быстрого ответа.

- Файловые серверы, которые позволяют пользователю хранить файлы на сервере, — эти приложения требуют передачи больших объемов данных, но не требуют быстрого ответа.
- Развитые технологии баз данных, делающие доступными для обычных пользователей большие объемы данных, значительно увеличивают количество пользователей, которые ожидают возможности доступа к данным.
- Смещение обычных приложений в направлении работы по принципу веб-браузеров, которое увеличивает количество пользователей, желающих получить доступ к данным.
- Всеобщее признание электронной почты в качестве службы коммуникации как в рамках одной компании, так и с другими компаниями.
- Быстрая коммерциализация Интернета, позволяющая компаниям предоставлять потребителям данные непосредственно, а не с помощью телефонных вызовов.

Кроме вышеупомянутых и многих других тенденций в развитии приложений, работающих с данными, следует отметить также то, что голосовые и видеоприложения тоже находятся в процессе перехода в сети данных. До середины 1990-х годов голосовые и видеоприложения обычно использовали сетевые средства, полностью отделенные от сетей передачи обычных данных. Передача голоса по сети данных еще больше увеличивает нагрузку на сети данных, поскольку им требуется обеспечить требуемое качество сетевой службы. В настоящее время большинство компаний уже начали или планируют переход на использование IP-телефонии, в которой голосовые данные передаются по сети обычных данных в пакетах IP с использованием протоколов приложений, в целом называемых *передачей голоса по сети IP* (Voice over IP — VoIP). В дополнение к этому некоторые компании предоставляют телефонные услуги по Интернету, в котором голосовые данные передаются с использованием пакетов VoIP. На рис. 6.11 показаны некоторые подробности работы технологии VoIP из домашнего высокоскоростного соединения Интернета с общим голосовым адаптером (Voice Adapter — VA), преобразующим аналоговый сигнал обычного телефона в пакеты протокола IP.

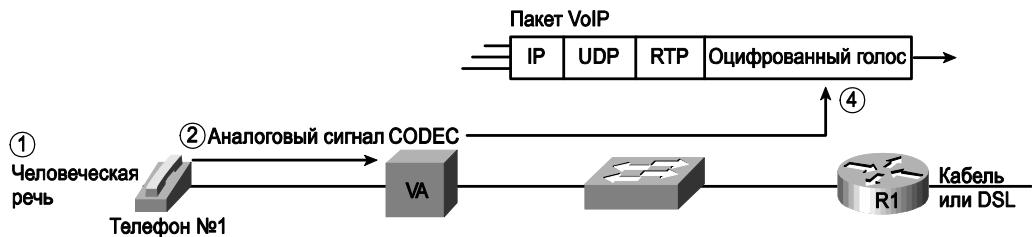


Рис. 6.11. Преобразование звука в пакеты IP с помощью голосового адаптера

Один вызов VoIP, проходящий по сети WAN, обычно занимает не более 30 Кбит/с полосы пропускания, что не так уж много по сравнению со многими современными приложениями для передачи данных. Фактически большинство приложений, работающих с данными, потребляет столько полосы пропускания, сколько им удается захватить. Однако технология VoIP предъявляет к сети и дополнительные требования:

тельные требования, выполнение которых обеспечивает удовлетворительное звучание голосовых данных VoIP.

Требования качества обслуживания QoS для технологии VoIP



- *Малая величина задержки.* VoIP требует очень низкого уровня задержки между отправляющим и принимающим телефонами — как правило, эта задержка не должна превышать 200 мс (0,2 с). Этот уровень задержки значительно ниже, чем тот, которого требует типичное приложение, работающее с данными.
- *Низкий уровень флуктуации задержки.* Под флуктуацией понимается изменение (вариация) задержки. Технология VoIP требует также очень низкого уровня отклонения задержки, в то время как приложения обычных данных допускают значительно более высокий уровень. Например, для последовательных пакетов VoIP вариация задержки не должна превышать 30 мс (0,03 с); в противном случае качество звука значительно ухудшается.
- *Утеря пакетов.* Если при передаче пакет VoIP теряется вследствие ошибок передачи или недостатка места на маршрутизаторе при ожидании пересылки, то доставки этого пакета VoIP не происходит. Вследствие проблем задержки и дребезжания нет необходимости в восстановлении этого утерянного пакета. К моменту, когда пакет может быть восстановлен, его использование потеряло смысл. Утерянные пакеты могут восприниматься как перерыв в звуковом потоке вызова VoIP.

При передаче видеоданных по VoIP возникают такие же проблемы производительности, с тем лишь отличием, что видео требует либо просто большей полосы пропускания (часто от 300 до 400 Кбит/с), либо значительно большей (от 3 до 10 Мбит/с для каждого видеопотока). В мире видео по VoIP также происходит определенная трансформация, вызванная появлением видео высокого разрешения по VoIP, которое еще больше увеличивает требования к полосе пропускания сети.

В табл. 6.4 обобщены некоторые данные о потребностях различных типов приложений в отношении четырех главных параметров QoS: полосы пропускания, задержки, дребезжания и утери пакетов. Нет необходимости заучивать данные этой таблицы, однако важно отметить, что хотя технология VoIP требует относительно небольшой полосы пропускания, для достижения высокого качества она предъявляет высокие требования к задержке, уровню дребезжания и количеству утерянных пакетов. Отметим, что передача видеоданных по протоколу IP предъявляет такие же требования с тем отличием, что при этом требуется средняя или большая ширина полосы пропускания.

Таблица 6.4. Сравнение минимальных потребностей различных типов приложений

Тип приложения	Полоса пропускания	Задержка	Дребезжание	Потери пакетов
VoIP	Низкая	Низкая	Низкая	Низкая
Двусторонняя передача видеоданных по IP (например, видеоконференции)	Средняя и широкая	Низкая	Низкая	Низкая
Односторонняя передача видеоданных по IP (например, камеры видеонаблюдения)	Средняя	Средняя	Средняя	Низкая

Окончание табл. 6.4

Тип приложения	Полоса пропускания	Задержка	Дребезжание	Потери пакетов
Интерактивные критически важные данные (например, заполняемые через веб-платежные ведомости)	Средняя	Средняя	Высокая	Высокая
Интерактивные коммерческие данные (например, разговор с другими сотрудниками компании)	Низкая и средняя	Средняя	Высокая	Высокая
Передача файлов (например, создание резервных копий дисковых носителей)	Широкая	Высокая	Высокая	Высокая
Некоммерческие приложения (например, просмотр последних спортивных результатов)	Средняя	Высокая	Высокая	Высокая

Для поддержки требований качества обслуживания QoS различных приложений на маршрутизаторах и коммутаторах могут быть настроены различные средства обеспечения QoS. Рассмотрение этих средств выходит за рамки программы экзаменов CCNA (однако эти вопросы входят в программу нескольких сертификатов Cisco профессионального уровня). Эти инструменты QoS следует использовать в современных сетях, для поддержки высокого качества службы VoIP и видео по протоколу IP.

Далее будет рассмотрен самый популярный протокол для интерактивных приложений работы с данными — протокол HTTP и “всемирная паутина” (World Wide Web, WWW). Целью этого рассмотрения является иллюстрация работы протокола уровня приложений.

“Всемирная паутина”, протоколы HTTP и SSL

“Всемирная паутина” (World Wide Web — WWW) включает в себя подключенные к глобальному Интернету веб-серверы всего мира и все подсоединенные к нему хосты, на которых работают веб-браузеры. Веб-сервер представляет собой службу, запущенную на некотором компьютере. Он хранит информацию (в виде веб-страниц), которая представляет интерес для многочисленных пользователей. Веб-браузер представляет собой программное обеспечение, установленное на компьютере конечного пользователя, позволяющее подключиться к веб-серверу и отобразить хранящиеся на нем веб-страницы.

Чтобы такой процесс стал возможным, должны быть доступны некоторые особые функции уровня приложений. Пользователь должен каким-либо образом указать сервер, конкретную веб-страницу и протокол, который будет использоваться для получения данных от сервера. Клиент должен узнать IP-адрес сервера, зная имя сервера; обычно для этого используется служба доменных имен DNS. Клиент должен запросить веб-страницу, состоящую из множества отдельных файлов, которые сервер должен отправить веб-браузеру. В заключение отметим, что для приложений электронной коммерции (e-commerce) передача данных, в частности конфиденциальных финансовых данных, должна сопровождаться особыми мерами безопасности, которые также обеспечиваются функциями уровня приложений. Все эти функции рассматриваются в последующих разделах данной главы.

ВНИМАНИЕ!

Большинство пользователей используют термин *веб-браузер*, или просто *браузер*. Веб-браузеры также называются веб-клиентами, поскольку они получают службу от веб-сервера.

Универсальный указатель ресурса

Чтобы в браузере отображалась какая-либо веб-страница, он должен указать сервер, на котором она хранится, а также другую информацию, идентифицирующую конкретную веб-страницу. Как правило, на веб-сервере хранится большое количество веб-страниц. Например, если веб-браузер используется для навигации по серверу <http://www.cisco.com> и пользователь щелкнет мышью на соответствующей гиперссылке, то отобразится другая веб-страница. После нового щелчка отображается еще одна новая страница. В каждом случае щелчок мышью идентифицирует IP-адрес сервера и конкретную веб-страницу; при этом большинство деталей процесса скрыто от пользователя. Позиции на веб-странице, на которых можно щелкнуть мышью и вызвать другую веб-страницу, называются гиперссылками, или просто *ссылками* (*link*).

Пользователь браузера может указать веб-страницу, щелкнув на ее гиперссылке на отображаемой в данный момент странице, или ввести в поле адреса браузера *универсальный указатель ресурсов* (*Universal Resource Locator* — URL), зачастую называемый веб-адресом. Оба способа — щелчок на гиперссылке или ввод URL — указывают на URL, поскольку при щелчке на ссылке веб-страницы ссылка в действительности указывает на URL.

ВНИМАНИЕ!

Чтобы увидеть скрытый под гиперссылкой соответствующий адрес URL, следует открыть веб-страницу в браузере, навести указатель мыши на гиперссылку, щелкнуть правой кнопкой мыши и выбрать в появившемся контекстном меню пункт *Properties* (*Свойства*). В появившемся окне должен отобразиться URL, к которому обратится браузер при щелчке мышью на данной гиперссылке.

Каждый URL определяет протокол, используемый для передачи данных, имя сервера и конкретную веб-страницу на этом сервере. URL можно разделить на три части:

- протокол, указываемый перед символами //;
- название хоста, которое находится между символами // и /;
- имя веб-страницы, которое находится после символа /;

Например: <http://www.certskills.com/ICND1>.

В данном случае используется *протокол передачи гипертекста* (*Hypertext Transfer Protocol* — HTTP), именем хоста является www.certskills.com, а имя веб-страницы — ICND1. (Этот URL особенно полезен, поскольку он указывает на веб-страницу со справочной информацией, связанной с главами настоящей книги.)

Поиск веб-сервера с помощью службы доменных имен DNS

Как уже говорилось в главе 5, хост может использовать службу DNS для того, чтобы узнать IP-адрес, соответствующий конкретному имени хоста. Хотя URL может включать в себя IP-адрес веб-сервера вместо его имени, обычно в URL указывается имя хоста. Таким образом, перед тем как браузер сможет отправить пакет на веб-сервер, ему обычно требуется преобразовать указанное в URL имя сервера в соответствующий этому имени IP-адрес.

Чтобы обобщить вышеизложенные концепции, на рис. 6.12 показан процесс службы DNS, инициированный веб-браузером, а также приведена другая связанная с этим

процессом информация. В целом можно сказать, что пользователь вводит URL (<http://www.cisco.com/go/learningnetwork>), а браузер преобразует имя `www.cisco.com` в корректный IP-адрес и начинает отправку пакетов на веб-сервер.

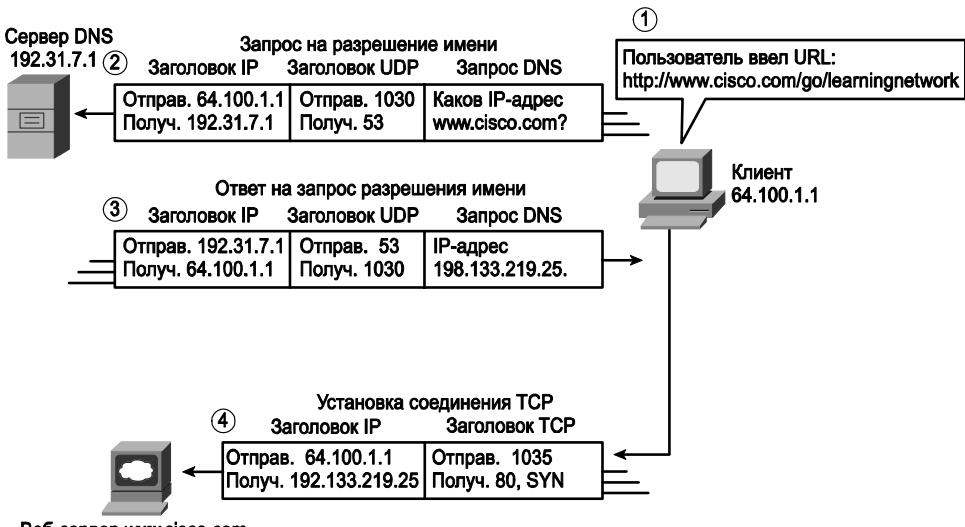


Рис. 6.12. Работа службы DNS и запрос веб-страницы

На рисунке показаны следующие этапы процесса.

- Пользователь вводит URL <http://www.cisco.com/go/learningnetwork> в адресной строке браузера.
- Клиент посылает запрос DNS на сервер DNS. Как правило, клиент узнает IP-адрес сервера DNS с помощью протокола DHCP. Отметим, что запрос DNS использует заголовок протокола UDP с портом получателя, равным общезвестному порту 53 (список популярных общезвестных портов см. в табл. 6.3).
- Сервер DNS посыпает ответ, приводя IP-адрес 198.133.219.25 в качестве IP-адреса для <http://www.cisco.com>. Отметим также, что в ответе содержится адрес 64.100.1.1 в качестве IP-адреса получателя, т.е. IP-адрес клиента. В нем также содержится заголовок UDP с портом отправителя 53; это вызвано тем, что данные посыпаются сервером DNS.
- Клиент начинает установку нового соединения TCP с веб-сервером. Отметим, что IP-адресом получателя является только что ставший известным IP-адрес веб-сервера. Пакет включает в себя заголовок TCP, так как протокол HTTP использует протокол TCP. Отметим также, что портом TCP получателя является порт 80, т.е. общезвестный порт HTTP. В заключение отметим, что на рисунке показан бит SYN — это напоминает о том, что процесс установки соединения TCP начинается с сегмента TCP, в котором установлен бит SYN (бинарная единица, 1).

На этой стадии процесса веб-браузер почти полностью закончил установку соединения TCP с веб-сервером. В следующем разделе показано, как веб-браузер получает файлы, которые образуют запрашиваемую веб-страницу.

Передача файлов с помощью протокола HTTP

После того как веб-клиент (браузер) создал соединение TCP с веб-сервером, клиент может запрашивать у сервера веб-страницы. Чаще всего для передачи веб-страниц используется протокол HTTP. Этот протокол уровня приложений, описанный в документе RFC 2616, определяет способ передачи файлов между двумя компьютерами. Протокол HTTP был специально создан для передачи файлов между веб-серверами и веб-клиентами.

В протоколе HTTP определено несколько команд и ответов; при этом наиболее часто используется запрос HTTP GET. Для получения файла с веб-сервера клиент посыпает серверу HTTP запрос GET с указанием имени файла. Если сервер принимает решение послать файл, то он отправляет ответ на запрос GET с кодом ответа 200 (означающим “OK”), а также содержимое файла.

ВНИМАНИЕ!

Для запросов HTTP имеется множество кодов ответов. Например, когда сервер не имеет запрашиваемого файла, он возвращает код 404, означающий “файл не найден”. Большинство веб-браузеров, получая в ответ на запрос код 404, отображают пользователю не код HTTP, а сообщение вроде “страница не найдена”.

Веб-страницы обычно состоят из нескольких файлов, называемых *объектами* (objects). Большинство веб-страниц содержат текст, а также графические изображения, анимированную рекламу и, возможно, файлы голосовых или видеоданных.

Каждый из этих компонентов хранится как отдельный объект (файл) на веб-сервере. Для получения всех этих файлов веб-браузер сначала получает первый файл, который может включать в себя (и обычно включает) ссылки на другие URL, поэтому браузер после этого запрашивает другие объекты. На рис. 6.13 показана общая картина этого процесса, в котором браузер получает первый файл, а затем два других файла.

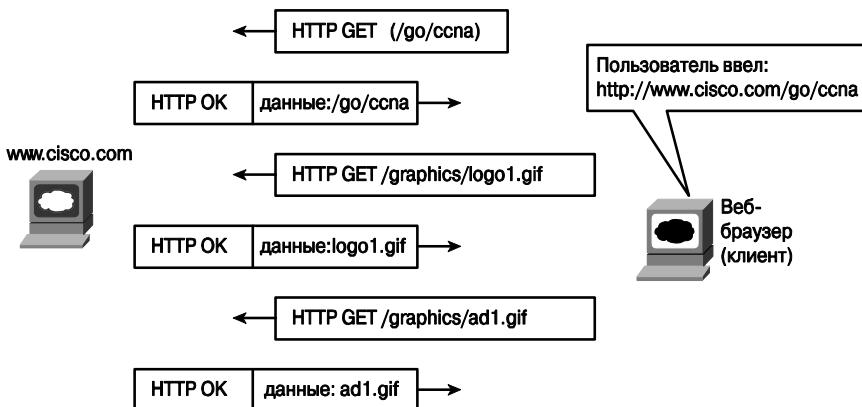


Рис. 6.13. Несколько запросов GET и ответов протокола HTTP

В данном случае после получения первого файла, обозначенного в URL как /go/ccna, браузер читает и интерпретирует этот файл. Кроме элементов страницы, полученный файл содержит ссылки на два других файла, поэтому браузер создает и отправляет два дополнительных запроса GET протокола HTTP.

Отметим, что, хотя это и не показано на рисунке, все эти команды передаются по одному (или нескольким) соединению TCP между клиентом и сервером. Это означает, что протокол TCP обеспечивает восстановление после ошибок, гарантируя доставку данных.

В заключение в данной главе приводятся начальные сведения по обеспечению безопасности сети.

Безопасность сети

Раньше угрозы безопасности сети приходили в основном от гениев или “ботаников”, которые не знали, как убить время. Их количество было относительно невелико. Главным их мотивом было желание доказать, что они могут проникнуть в чужую сеть. С тех пор количество потенциальных взломщиков и сложность атакросли экспоненциально. Атаки, которые некогда требовали от взломщика высокого уровня владения компьютером, сейчас совершаются с помощью легко загружаемых и свободно доступных инструментов, воспользоваться которыми могут даже студенты младших курсов. Каждая компания и почти каждый человек подключаются к Интернету, что, по существу, делает уязвимым весь мир.

Наибольшую опасность, однако, представляют изменения в мотивации лиц, совершающих атаки. Вместо честолюбивых помыслов или попытки украсть миллионы современные взломщики могут быть значительно более организованы и мотивированы. Организованная преступность пытается украсть миллиарды, занимаясь вымогательством у крупных компаний, угрожая атаками на *отказ в обслуживании* (Denial of Service — DoS) на публичные серверы компаний. Они могут похитить идентификационную информацию или данные кредитных карточек у сотен тысяч людей в ходе одной изощренной атаки. Атаки могут исходить от государств или от террористов. Преступники не только совершают атаки на военные или правительственные сети, но и пытаются вывести из строя инфраструктурные службы коммунальных предприятий и транспорта, а также нанести ущерб экономике.

Проблема безопасности действительно серьезна и требует пристального внимания. В рамках изучения данной книги и подготовки к сдаче экзамена ICND1 ниже рассматриваются основы терминологии, типы проблем безопасности и некоторые типичные средства, используемые для уменьшения возможных рисков для безопасности сети. Для этого в данном заключительном разделе представлен общий обзор возможных атак, а затем описаны четыре класса средств, используемых для защиты сети от возможных угроз. Кроме этих предварительных сведений, также рассматриваются вопросы защиты устройств, в данном случае маршрутизаторов и коммутаторов, как часть материала главы 8 и главы 13.

Обзор источников и типов угроз сети

На рис. 6.14 показана типичная топология сети с брандмауэром (межсетевым экраном). Брандмауэр, вероятно, является наиболее известным устройством защиты сети, которое располагается между корпоративной сетью и небезопасным Интернетом. Задача брандмауэра состоит в том, чтобы остановить пакеты, которые сетевой инженер или менеджер безопасности счел небезопасными. Брандмауэр главным образом просматривает номера портов транспортного уровня и заголовки уровня приложений для того, чтобы предотвратить проникновение в корпоративную сеть пакетов, исходящих от определенных портов или приложений.

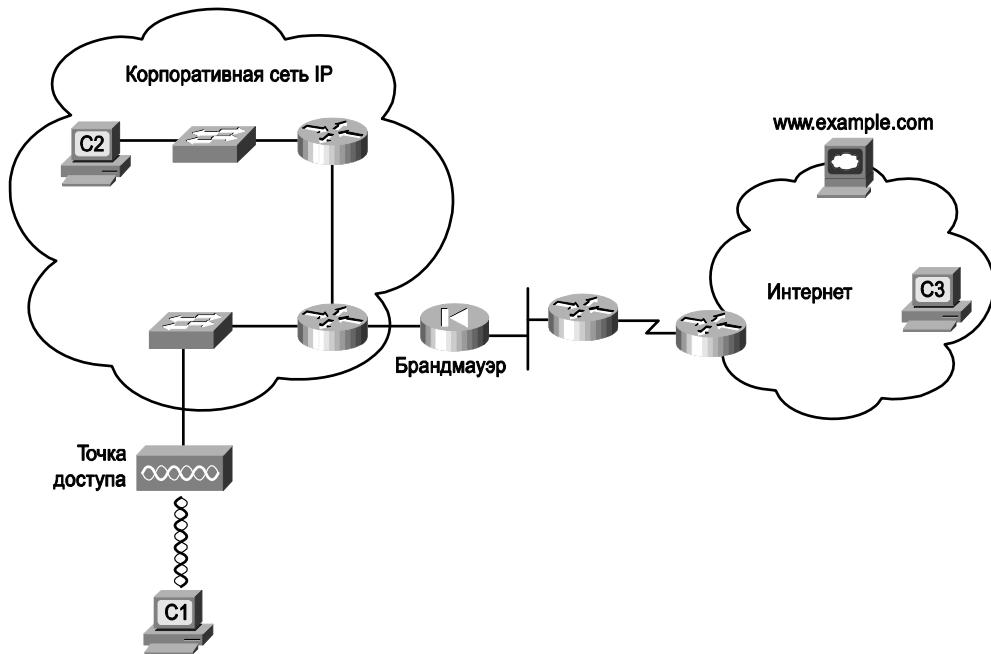


Рис. 6.14. Типичное подключение корпоративной сети к Интернету через брандмауэр

Однако ситуация, показанная на рисунке, может создать у обычного сотрудника неправильное представление о проблемах безопасности. Ему может показаться, что брандмауэр обеспечивает защиту от всех угроз, связанных с подключением к Интернету.

Границочный брандмауэр корпоративной сети (брандмауэр на границе или на периметре сети) защищает не от всех угроз, связанных с подключением к Интернету. Более того, большая часть угроз безопасности в действительности исходит из самой корпоративной сети, а брандмауэр этих пакетов даже не видит.

Чтобы лучше оценить угрозы, исходящие из самой корпоративной сети, следует несколько подробнее ознакомиться с различными возможными типами атак.

Три типа атак



- Атака типа “отказ в обслуживании” (Denial of Service — DoS). Целью этой атаки является взлом. Атаки DoS называемые *разрушителями* (destroyers), пытаются повредить хост сети, уничтожая данные и программное обеспечение. Атаки DoS, называемые *взломщиками* (crashers), наносят вред, вызывая сбои на хосте или делая невозможным подсоединение устройств к сети. Атаки DoS, называемые *заполнителями* (flooders), переполняют сеть пакетами, делая ее непригодной для использования и лишая пользователей возможности связи с серверами.
- *Разведывательные* (reconnaissance) атаки. Этот тип атаки может вызывать разрушения в качестве побочного эффекта, однако основной целью атаки является сбор информации для последующей атаки доступа. Примером такой атаки может служить попытка выяснения IP-адреса с последующим обнаружением сервера, который не требует шифрования при подключении.

- *Атака доступа.* Попытка выкрасть данные, обычно относящиеся к финансовой сфере, чтобы другая компания получила преимущества в конкурентной борьбе, или даже для международного шпионажа.

Компьютерные вирусы являются лишь одним из средств, которые могут быть использованы для осуществления таких атак. Под вирусом понимается программа, которая незаметно проникает в компьютер, например, через приложение к электронному письму или при загрузке файлов с веб-сайта. Вирус может вызвать нарушение работы компьютера или переслать информацию пользователя лицу, совершившему атаку.

В настоящее время большинство компьютеров использует какое-либо антивирусное программное обеспечение для обнаружения известных вирусов и предотвращения заражения ими компьютера. Кроме других действий (функций), антивирусное программное обеспечение загружает базу данных с характеристиками всех известных вирусов; эти характеристики называются *сигнатурами* (signatures). Периодически загружая из сети самые последние сигнатуры вирусов, антивирусное программное обеспечение имеет информацию обо всех последних вирусах. Программой сканирования пакеты, поступающие на компьютер, антивирусная программа может распознать известные вирусы и не допустить заражения ими компьютера. Эти программы также периодически выполняют автоматическое сканирование всех жестких дисков компьютера для поиска известных вирусов.

На рис. 6.15 приведены возможные риски и угрозы для корпоративной сети, в которой уже установлен граничный брандмауэр. После рисунка приведен список трех возможных ситуаций, в которых корпоративная сеть оказывается уязвимой для атак из самой сети.

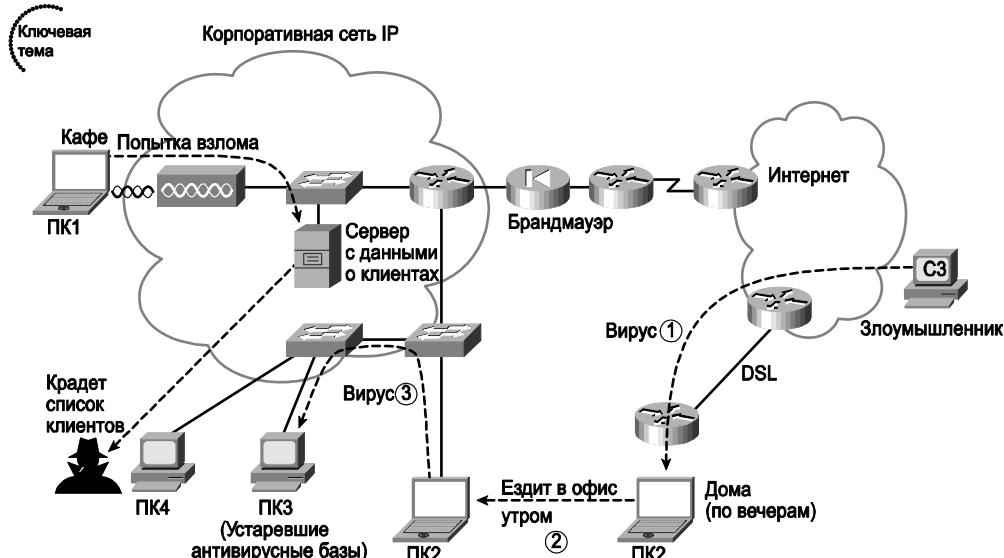


Рис. 6.15. Распространенные проблемы безопасности в корпоративной сети

В такой корпоративной сети могут возникнуть следующие типичные проблемы.

- *Доступ из беспроводной сети LAN.* Беспроводные сети LAN позволяют пользователю получить доступ к другим устройствам корпоративной сети. Радиосигналы

такой сети выходят за пределы здания, поэтому в такую незащищенную сеть может войти пользователь, находящийся, например, в кафе на другой стороне улицы, что позволяет злоумышленнику (компьютер ПК1) перейти к следующему этапу — попытке получить доступ к компьютерам компании.

- *Инфицированные вирусом переносные компьютеры.* Когда сотрудник компании приносит свой переносной компьютер (ПК2) домой, без брандмауэра и других средств безопасности, его компьютер может оказаться зараженным вирусом. Когда сотрудник возвращается на работу в офис, его компьютер подключается к корпоративной сети и вирус распространяется на другие компьютеры, например на компьютер ПК3. Компьютер ПК3 может частично оказаться уязвимым, поскольку пользователи могут не делать ежедневного антивирусного сканирования, которое, хотя и полезно, может раздражать.
- *Обиженные сотрудники.* Пользователь компьютера ПК4 планирует перейти в другую компанию. Он крадет информацию из корпоративной сети и загружает ее в MP3-плеер или во флеш-память. Это позволяет ему ввести всю базу данных пользователей в устройство, которое может легко быть скрыто и вынесено из здания.

Выше было описано несколько основных видов атаки на сеть; в действительности существует большое количество их вариаций и других методов. Для решения подобных проблем корпорация Cisco предложила модель обеспечения безопасности сети, в которой используются различные средства, автоматически предпринимающие меры по защите сети, а функции безопасности работают во всей сети. В модели Cisco используется термин *эшелонированная безопасность* (security in depth), который относится ко всем используемым в сети средствам защиты, включая функции защиты на маршрутизаторах и коммутаторах. Cisco также использует термин *самозашитающаяся сеть* (self-defending network), под которым понимается автоматизация защиты, когда сетевые устройства автоматически реагируют на проблемы в сети.

Например, *управление доступом к сети* (Network Admission Control — NAC) является средством защиты, которое помогает предотвратить две из описанных выше атак. Кроме всех прочих функций, NAC может регистрировать первое подключение устройства к локальной сети LAN, независимо от того, является оно проводным или беспроводным. Эта функция NAC, частично реализуемая на коммутаторах LAN, не допускает подключения компьютера к сети LAN до тех пор, пока не будет обновлена его антивирусная база (определения вирусов), и требует полного сканирования жестких дисков на наличие вирусов. NAC также требует, чтобы пользователь ввел свое имя и пароль перед тем, как он сможет посыпать другие данные в сеть LAN, что предотвращает получение доступа злоумышленником, сидящим в соседнем кафе. Однако NAC не может предотвратить нанесение ущерба обиженным сотрудником, поскольку обычно у него есть имя и пароль, которые проходят аутентификацию системой NAC.

Кроме вирусов, существует много других средств, которые могут быть использованы для совершения атаки.

- *Сканер сети* (scanner). Инструмент, который посылает запросы на соединение портам UDP и TCP для различных приложений, пытаясь выяснить, какие службы IP работают на различных хостах, и по возможности узнать тип операционной системы на каждом хосте.

- *Шпионское ПО* (spyware). Вирус, который ищет личную или конфиденциальную информацию, отслеживая действия пользователя на компьютере и передавая через Интернет информацию атакующему.
- *Червь* (worm). Самораспространяющаяся программа, которая может быстро воспроизводить саму себя в корпоративной сети и в Интернете, часто совершая атаки DoS, особенно на серверы.
- *Регистратор нажатия клавиш на клавиатуре* (keystroke logger — логгер). Вирус, который записывает все нажатия клавиш на клавиатуре или только нажатия, с помощью которых обеспечивается доступ к безопасным (зашитенным) сайтам, и передающий эту информацию лицу, совершающему атаку. Логгеры в действительности могут перехватить имя пользователя и его пароль для доступа к защищенным сайтам еще до того, как информация покинет компьютер, что дает атакующему доступ к вашим наиболее важным финансовым веб-сайтам.
- *Мошенничество* (phishing). Взломщик создает веб-сайт, который внешне выглядит как реальный сайт банка или кредитной компании. Мошенник рассыпает электронные письма с указанием URL поддельного сайта, который, однако, выглядит как настоящий URL сайта компании (например: “Щелкните здесь для обновления записей вашей кредитной карты и повышения уровня ее защиты”). Мошенник надеется, что найдутся пользователи, которые “проглотят наживку”, подключаясь к этому незаконному сайту и введут личную информацию: имя, адрес, номер кредитной карты, код социального страхования (social security number в США) или другой социальный идентификатор. Наилучшей защитой от такого рода атак, вероятно, является обучение пользователей и лучшее понимание ими проблем открытости сети.
- *Вредоносное ПО* (malware). Этот термин относится к широкому классу разрушительных вирусов, включая вирусы-шилоны (spyware).

Решение этих и многих других не упомянутых здесь проблем безопасности состоит в обеспечении многоуровневой безопасности сети. Ниже описываются некоторые средства, которые могут быть использованы для обеспечения такой эшелонированной безопасности.

Брандмауэры и адаптивные средства безопасности Cisco (ASA)

Брандмауэры исследуют все входящие в сеть и выходящие из нее пакеты, чтобы отфильтровать нежелательный трафик. Брандмауэры отделяют допустимые данные от недопустимых на основе многих характеристик пакетов, в частности IP-адресов отправителя и получателя, а также номеров портов TCP и UDP (в которых косвенно указан протокол приложения). Брандмауэры также анализируют заголовки уровня приложений.

Термин *брандмауэр* относится к области строительства и архитектуры. К брандмауэру здания предъявляются два основных требования: он должен быть сделан из огнеупорных материалов, и архитектор ограничивает количество проемов в стене (двери, каналы для проводки и трубопровода), ограничивая тем самым пути распространения огня. Аналогичным образом брандмауэр в сети должен быть “закаленным” против атак на сеть. Он должен запрещать доступ всем пакетам, кроме тех, которым доступ был разрешен сетевым инженером в соответствии с установленными в сети правилами. Этот процесс по аналогии с брандмауэром здания часто называют “открытием дыры”.

Брандмауэры находятся на пути пересылки пакетов между двумя сетями, при этом часто один интерфейс LAN подключен к безопасной локальной сети, а другой интерфейс — к менее безопасной сети (часто Интернету). Кроме того, поскольку некоторые корпоративные хосты должны быть доступны из Интернета, по сути, наиболее опасная ситуация — когда брандмауэр обычно имеет интерфейс, подключенный к другой небольшой части корпоративной сети, которая называется *демилитаризованной зоной* (Demilitarized Zone — DMZ). Зона DMZ локальной сети представляет собой место, где расположены устройства, которые должны быть доступны извне, но этот доступ подвергает их серьезному риску. На рис. 6.16 показан пример проектирования сети, имеющей один брандмауэр с тремя интерфейсами.

Для выполнения своих задач брандмауэр должен быть настроен таким образом, чтобы он “знал”, какие его интерфейсы подключены к внутренней, внешней и демилитаризованной частям сети. Кроме того, должны быть заданы правила, которые указывают брандмауэру, какие типы трафика являются допустимыми, а какие — нет. На рисунке показаны два типичных допустимых потока и один, который обычно является запрещенным (потоки показаны пунктирными линиями).

- Разрешить веб-клиентам внутренней сети (таким, как компьютер ПК1) отправлять пакеты веб-серверу (в данном случае серверу www.example.com)
- Запретить веб-клиентам внешней сети (таким, как ПК5) отправку пакетов веб-серверам внутренней части сети (таким, как внутренний сервер int.fredesco.com).
- Разрешить веб-клиентам внешней сети (таким, как компьютер ПК5) подключаться к веб-серверам демилитаризованной зоны DMZ (таким, как веб-сервер www.fredesco.com).

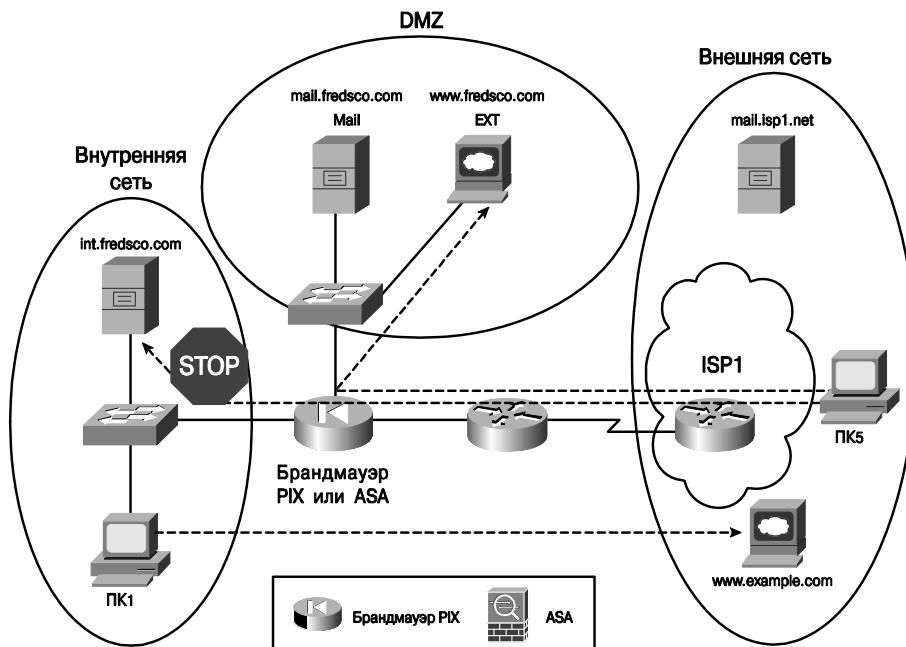


Рис. 6.16. Общая схема сети с брандмауэром

Ранее корпорация Cisco выпускала брандмауэры под торговой маркой PIX. Несколько лет назад она выпустила на рынок целое поколение новых аппаратных средств обеспечения сетевой безопасности, используя торговую марку ASA (Adaptive Security Appliance — *адаптивные устройства безопасности*). Аппаратные средства ASA могут играть роль брандмауэра и выполнять другие функции обеспечения безопасности, в том числе комбинации этих ролей. Поэтому, когда речь идет о безопасности сети, термин *брандмауэр* по-прежнему применяется к этим функциям, хотя в настоящее время устройство Cisco может быть установленным ранее устаревшим брандмауэром PIX или более новым ASA (см. на рис. 6.16, снизу, пиктограмму устройства ASA).

“Анти-х”

Всеобъемлющий план защиты сети требует использования нескольких функций, которые предотвращают возникновение известных типов проблем. Например, установленное на хосте антивирусное обеспечение помогает предотвратить заражение компьютера вирусами. Средства Cisco ASA обеспечивают или помогают создать эшелонированную защиту, которая включает в себя ряд средств, предотвращающих такие проблемы, как заражение вирусами. Поскольку названия нескольких отдельных инструментов начинаются с приставки “анти-”, специалисты Cisco используют термин *анти-х* (anti-x) для обозначения целого класса инструментов защиты, которые предотвращают возникновение различных проблем, включая следующие.

- *Антивирусные средства* (anti-virus). Используются для сканирования потока данных в сети и предотвращения передачи известных вирусов на основе их сигнатур.
- *Антишипион* (anti-spyware). Сканирует сетевой поток для предотвращения передачи программ-шпионов.
- *Антиспам* (anti-spam). Анализирует почтовые сообщения до того, как они попадут к пользователям, уничтожая или отделяя нежелательную корреспонденцию.
- *Антифиッシнг* (anti-phishing). Осуществляет мониторинг URL, отправленных в сообщениях по сети, для поиска URL, которым свойственны фишинговые атаки, предотвращая похищение пользовательских данных.
- *Фильтрация URL* (URL filtering). Фильтрует веб-трафик на основе URL для предотвращения подключений пользователей к нежелательным сайтам.
- *Фильтрация электронной почты* (E-mail filtering). Предоставляет средства антиспама. Также фильтрует почтовые сообщения, содержащие оскорбительные материалы, потенциально защищая предприятие от судебного преследования.

Средства Cisco ASA могут быть использованы для всех перечисленных выше функций “анти-х”.

Обнаружение вторжений в сеть и их предотвращение

Некоторые типы атак трудно обнаружить средствами “анти-х”. Например, если известный вирус заражает компьютер только через приложение к электронному письму файла *this-is-aviruse.exe*, то ASA или антивирусное программное обеспечение компьютера сможет легко идентифицировать и уничтожить этот вирус. Однако некоторые виды атак имеют значительно более изощренный характер. Атаки

могут даже не включать в себя передачу файлов, используя вместо этого множество других, более сложных методов, часто пользуясь недавно обнаруженными дефектами в операционной системе.

В мире сетевой безопасности есть два типа средств защиты, которые могут быть использованы для предотвращения изощренных атак: *система обнаружения вторжений* (Intrusion Detection Systems — IDS) и *система предотвращения вторжений* (Intrusion Prevention Systems — IPS). Средства систем IDS и IPS обнаруживают эти угрозы, анализируя тенденции в поисках атак, которые используют особые шаблоны сообщений и другие факторы. Например, системы IDS и IPS могут следить за последовательностями пакетов, пересылаемых между хостами в поисках файлов, отправляемых на все большее количество хостов, что может свидетельствовать о наличии “червя”, который пытается распространяться по сети.

Системы IDS и IPS различаются главным образом тем, как они следят за трафиком в сети, и тем, как они реагируют в случае подозрений на угрозы. Средства IDS обычно получают копии пакетов через порт мониторинга, не становясь частью маршрута пересылки пакетов. Система IDS может после этого оценить уровень каждой потенциальной угрозы и в случае необходимости запросить помочь в предотвращении атаки у других устройств, таких как маршрутизаторы и брандмауэры (если они в состоянии это сделать). Средства IPS часто находятся на пути пересылки пакетов, что позволяет IPS выполнять такие же функции, как и функции IDS, но в дополнение к ним IPS имеет возможность реагировать на трафик и фильтровать его. Способность быстро реагировать весьма важна для предотвращения некоторых атак, таких, например, как “червь” Slammer, появившийся в 2003 году, который удваивал число зараженных хостов примерно каждые 9 секунд и смог заразить 75000 хостов за первые 10 минут атаки. При такой скорости атаки требуется использование быстро реагирующих на угрозу средств, вместо ожидания прихода инженера, который просмотрит отчет и предпримет какие-либо действия.

Виртуальные частные сети

Последним классом средств защиты сети, который будет рассмотрен в данной главе, будет *виртуальная частная сеть* (Virtual Private Network — VPN), которую, возможно, точнее было бы назвать виртуальной частной распределенной сетью WAN. Выделенная линия по своей природе является безопасной и в действительности выступает в качестве электрической цепи между двумя маршрутизаторами. Сеть VPN пересыпает пакеты через Интернет, который является общедоступным. Однако использование виртуальной частной сети VPN делает такую связь безопасной, как частную выделенную линию.

Без использования технологии VPN пакеты, пересылаемые между двумя устройствами, потенциально уязвимы. Проходящие по Интернету пакеты могут быть перехвачены атакующими. В реальности с ростом Интернета атакующие нашли способы перенаправлять пакеты и исследовать их содержимое как для просмотра передаваемых данных, так и для получения персональной информации (такой, как имена пользователей и пароли), что может быть частью разведывательной атаки. Кроме того, пользователи и серверы могут оказаться неспособными отличить законный пакет действительного пользователя от пакета атакующего, который пытается получить еще больше информации и возможность доступа.

Сети VPN позволяют решать эти проблемы, используя Интернет и не подвергаясь при этом риску случайно принять данные от атакующих хостов или позволить другим прочитать ваши данные. Сети VPN аутентифицируют конечные точки — это означает, что оба окончных устройства, участвующих в обмене данными, проверили идентичность друг друга. Кроме этого, сети VPN шифруют первоначальные пакеты IP, поэтому даже если атакующему удастся получить копии пакетов во время их прохождения по сети, то он не сможет прочитать их данные. На рис. 6.17 проиллюстрированы общие принципы работы сети VPN, с сетью интранет VPN и сетью доступа VPN.

На рисунке приведен пример двух типов сетей VPN: сеть VPN доступа и сеть интранет VPN между двумя подразделениями. Сеть VPN доступа поддерживает работу домашнего пользователя или пользователя филиала (малого офиса), а пакеты обычно шифрует компьютер дистанционного офиса. Сеть интранет VPN обычно соединяет между собой два подразделения одного и того же предприятия, фактически создавая безопасное соединение между двумя различными частями внутри интранета. Для сетей интранет VPN шифрование может выполняться для всех устройств с использованием различных аппаратных средств, таких как маршрутизаторы, брандмауэры, специально созданное встроенное аппаратное обеспечение VPN концентратора или средства ASA (см. рис. 6.17).

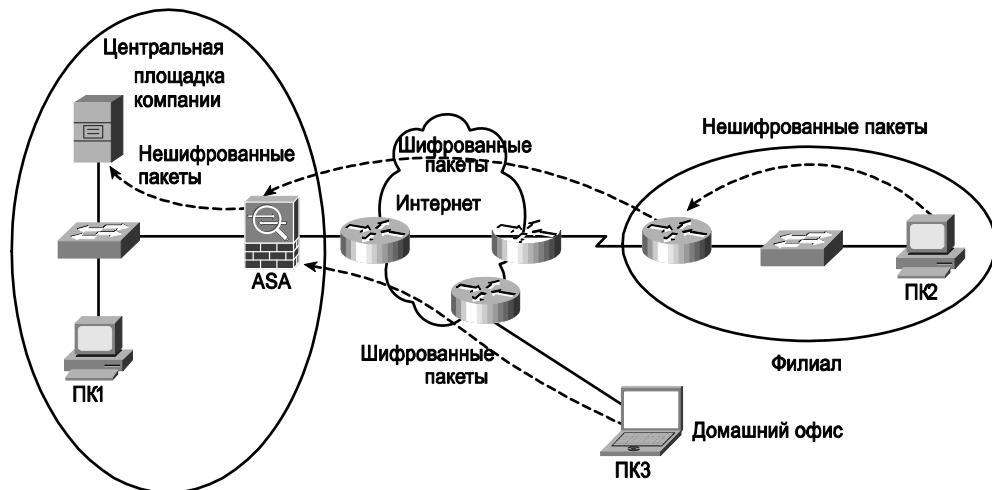


Рис. 6.17. Примеры сетей VPN

На рис. 6.17 показано, как сети VPN могут использовать сквозное (end-to-end) шифрование, при использовании которого данные остаются в зашифрованном состоянии, пока они передаются через один или несколько маршрутизаторов. Кроме того, канальное шифрование может быть использовано для шифрования данных на канальном уровне, поэтому данные шифруются только при прохождении по одному каналу данных. Пример канального шифрования приведен в главе 11.

Подготовка к экзамену

Повторите все ключевые темы

Повторите все ключевые темы данной главы, помеченные пиктограммой “Ключевая тема”. Ключевые темы и соответствующие им страницы перечислены в табл. 6.5.

Таблица 6.5. Ключевые темы главы 6

Элемент	Описание	Страница
Табл. 6.2	Функции транспортного уровня модели TCP/IP	175
Табл. 6.3	Популярные приложения и их общеизвестные номера портов	181
Рис. 6.6	Подтверждение протокола TCP в случае ошибки передачи	182
Рис. 6.7	Использование окон в протоколе TCP	183
Рис. 6.8	Установка соединения протокола TCP	184
Список	Определения протоколов, ориентированных и не ориентированных на соединение	184
Список	Требования качества обслуживания QoS для технологии VoIP	189
Список	Три типа атак	195
Рис. 6.15	Распространенные проблемы безопасности в корпоративной сети	196

Заполните таблицы и списки по памяти

Распечатайте приложение М (Appendix L) с компакт-диска или его раздел, относящийся к этой главе, и заполните таблицы и списки по памяти. В приложении Н (Appendix M) приведены заполненные таблицы и списки для самоконтроля.

Ключевые термины

Дайте определения перечисленных ниже терминов и проверьте правильность их написания в списке терминов:

анти-х (Anti-x), установка соединения (connection establishment), атака DoS (DoS), обнаружение ошибок (error detection), восстановлением данных после ошибок передачи (error recovery), брандмауэр (firewall), управление потоком (flow control), прямое подтверждение (forward acknowledgment), протокол HTTP (HTTP), система обнаружения вторжений (Intrusion Detection System — IDS), система предотвращения вторжений (Intrusion Prevention System — IPS), упорядоченная передача данных (ordered data transfer), порт (port), позитивное подтверждение и повторная передача (Positive Acknowledgment and Retransmission — PAR), сегмент (segment), скользящие окна (sliding windows), URL, виртуальная частная сеть (Virtual Private Network — VPN), технология VoIP (VoIP), веб-сервер (web server).

В этой части рассмотрены следующие темы экзамена Cisco ICND1¹...

Принципы работы сетей передачи данных:

- показано, как использовать модели OSI и TCP/IP, а также связанные с ними протоколы для объяснения процесса передачи потоков данных в сети;
- рассказано, как интерпретировать диаграммы сетей;
- объяснено, как определить маршрут между двумя хостами в сети;
- рассказано, как правильно определить наиболее распространенные сетевые проблемы на уровнях 1, 2, 3 и 7 с использованием многоуровневого подхода;
- описаны различия локальных (LAN) и распределенных (WAN) сетей и их функций.

Внедрение небольшой коммутируемой сети:

- описан процесс выбора правильной среды, кабелей, портов и разъемов для подключения коммутаторов к другим сетевым устройствам и хостам;
- объяснены технологии и методы контроля среды передачи данных для сетей Ethernet;
- объяснены фундаментальные концепции сегментирования сетей и базовых средств управления трафиком;
- объяснены базовые концепции коммутации и принцип работы коммутаторов компании Cisco;
- рассказано, как выполнять базовое конфигурирование коммутаторов Cisco, сохранять и проверять конфигурационные файлы, а также как использовать средства дистанционного администрирования;
- рассказано, как проверять состояние сети и работу коммутатора с помощью базовых сетевых утилит (ping, traceroute, Telnet, SSH, ARP, ipconfig), а также с помощью команд групп show и debug;
- показано, как внедрить базовые средства безопасности в коммутаторе (технология port security, отключение портов);
- рассказало, как идентифицировать, изолировать и решить наиболее распространенные проблемы с сетевой средой, конфигурацией, автоматическим согласованием и исправить стандартные аппаратные отказы коммутаторов.

Объяснение основных задач при построении беспроводных сетей:

- описаны стандарты беспроводных сетей (в том числе IEEE, Альянса Wi-Fi, ITU и FCC);
- рассказано, для чего используются основные компоненты небольших беспроводных сетей (в том числе параметры SSID, сети BSS и ESS);
- описаны типичные параметры конфигураций беспроводных сетей, которые необходимы для взаимодействия устройств;
- проанализированы функции безопасности беспроводных сетей, а также возможности технологии WPA (в том числе открытые сети и стандарты WEP и WPA-1/2);
- описаны основные проблемы при развертывании беспроводных сетей.

Поиск недостатков в системе безопасности и распространенные методы их устранения:

- описаны рекомендуемые действия по улучшению безопасности сети и рассказано о минимальных мерах по обеспечению безопасности устройств.

¹ Текущие темы сертификационного экзамена приведены на сайте <http://www.cisco.com>. — Примеч. авт.

Часть II. Коммутация в локальных сетях

Глава 7. “Базовые концепции коммутации Ethernet”

Глава 8. “Работа с коммутаторами компании Cisco”

Глава 9. “Настройка коммутаторов Ethernet”

Глава 10. “Поиск и устранение неисправностей в коммутаторах Ethernet”

Глава 11. “Беспроводные локальные сети”

В этой главе...

- **Концепции коммутации в локальных сетях.** Объяснены основные процессы, связанные с коммутацией в локальных сетях.
- **Принципы построения локальных сетей.** Описана терминология и методы построения корректно работающих локальных сетей.

ГЛАВА 7

Базовые концепции коммутации Ethernet

В главе 3 были достаточно подробно рассмотрены основные концепции и атрибуты технологии Ethernet для локальных сетей. В ней были описаны как основы технологии, так и кабельная система на основе кабеля UTP, принципы работы концентраторов и коммутаторов, а также приведено сравнение различных стандартов Ethernet, описаны механизмы передачи на канальном уровне, адресация и фреймирование.

В этой части продолжено описание локальных сетей (LAN) на основе технологии Ethernet, а в главе 11 описаны беспроводные сети. В текущей главе подробно объясняются темы, оставшиеся за рамками рассмотрения предыдущих глав, например главы 3. В частности, в этой главе более детально описаны принципы работы коммутаторов, методы построения сетей с использованием концентраторов, мостов, коммутаторов и маршрутизаторов. В главах 8–10 рассказано, как подключиться к коммутаторам компании Cisco и как их настроить. В главе 8 подробно описан интерфейс командной строки пользователя, в главе 9 рассмотрена базовая конфигурация коммутаторов, а в главе 10 рассказано, как проверять сеть и устранять неисправности в коммутаторах компании Cisco. В главе 11, завершающей вторую часть первого тома книги, описаны основные концепции беспроводных локальных сетей.

Контрольные вопросы: знаете ли вы уже темы главы

Этот раздел предназначен для того, чтобы читатель мог предварительно оценить свои знания и решить, нужно ли ему читать главу целиком. Если ответы на девять из десяти вопросов даны правильно, можно сразу же перейти к последнему разделу “Подготовка к экзамену”. Основные темы этой главы и предварительных контрольных вопросов перечислены в табл. 7.1. Отвечая на контрольные вопросы и используя таблицу, читатель сможет достаточно точно определить свои знания в той или иной области. Ответы на вопросы приведены в приложении А.

Таблица 7.1. Темы контрольных вопросов

Основная тема	Номера вопросов
Концепции коммутации в локальных сетях	1–5
Принципы построения локальных сетей	6–8

1. Какое из утверждений правильно описывает принимаемое коммутатором решение об отправке фрейма для известного ему одноадресатного (unicast) MAC-адреса получателя?

- а) Коммутатор сравнивает адрес получателя с таблицей коммутации (т.е. таблицей MAC-адресов).
 - б) Коммутатор сравнивает адрес отправителя с таблицей коммутации (т.е. таблицей MAC-адресов).
 - в) Устройство рассыпает фрейм через все интерфейсы в данной сети VLAN, кроме того, через который он был получен.
 - г) Коммутатор сравнивает IP-адрес получателя с MAC-адресом получателя.
2. Какое из утверждений правильно описывает принимаемое коммутатором решение об отправке фрейма для широковещательного (broadcast) MAC-адреса получателя?
- а) Коммутатор сравнивает адрес получателя с таблицей коммутации (т.е. таблицей MAC-адресов).
 - б) Коммутатор сравнивает адрес отправителя с таблицей коммутации (т.е. таблицей MAC-адресов).
 - в) Устройство рассыпает фрейм через все интерфейсы в данной сети VLAN, кроме того, через который он был получен.
 - г) Коммутатор сравнивает IP-адрес получателя с MAC-адресом получателя.
 - д) Устройство сравнивает идентификатор входного интерфейса с MAC-адресом отправителя в таблице MAC-адресов.
3. Какое из утверждений правильно описывает принимаемое коммутатором решение об отправке фрейма для неизвестного ему одноадресатного (unicast) MAC-адреса получателя?
- а) Устройство рассыпает фрейм через все интерфейсы в данной сети VLAN, кроме того, через который он был получен.
 - б) Устройство пересыпает фрейм через один интерфейс, для которого есть соответствующая запись в таблице MAC-адресов.
 - в) Коммутатор сравнивает IP-адрес получателя с MAC-адресом получателя.
 - г) Устройство сравнивает идентификатор входного интерфейса с MAC-адресом отправителя в таблице MAC-адресов.
4. Какие действия выполняет коммутатор, если ему нужно принять решение о том, добавлять или нет новый MAC-адрес в таблицу коммутации?
- а) Устройство сравнивает одноадресатный адрес получателя с записями в таблице коммутации (MAC-адресов).
 - б) Устройство сравнивает одноадресатный адрес отправителя с записями в таблице коммутации (MAC-адресов).
 - в) Устройство сравнивает идентификатор сети VLAN (ID) с записями в таблице коммутации (MAC-адресов).
 - г) Устройство сравнивает IP-адрес получателя из записи в кеше ARP с записями в таблице коммутации (MAC-адресов).

5. Персональный компьютер ПК1 с MAC-адресом 1111.1111.1111 подключен к интерфейсу Fa0/1 коммутатора SW1. Компьютер ПК2 с MAC-адресом 2222.2222.2222 подключен к интерфейсу Fa0/2 коммутатора SW1, а компьютер ПК3 с MAC-адресом 2222.2222.2222 подключен к интерфейсу Fa0/3 того же коммутатора. Изначально в таблице коммутатора нет никаких динамических записей о MAC-адресах. ПК1 пересыпает фрейм с адресом получателя 2222.2222.2222. Если после этого ПК3 пересыпает фрейм компьютеру ПК2 с адресом получателя 2222.2222.2222, что будет происходить в коммутаторе? (Выберите несколько ответов.)

- а) Коммутатор перешлет фрейм через интерфейс Fa0/1.
- б) Коммутатор перешлет фрейм через интерфейс Fa0/2.
- в) Коммутатор перешлет фрейм через интерфейс Fa0/3.
- г) Коммутатор отбросит (или отфильтрует) такой фрейм.

В каком случае два компьютера будут в одном и том же домене коллизий?

- а) Если компьютеры разделены концентратором Ethernet.
- б) Если компьютеры разделены прозрачным мостом.
- в) Если компьютеры разделены коммутатором Ethernet.
- г) Если компьютеры разделены маршрутизатором.

6. В каком случае два компьютера будут в одном и том же широковещательном домене? (Выберите несколько ответов.)

- а) Если компьютеры разделены концентратором Ethernet.
- б) Если компьютеры разделены прозрачным мостом.
- в) Если компьютеры разделены коммутатором Ethernet.
- г) Если компьютеры разделены маршрутизатором.

В каком из стандартов Ethernet максимальная длина кабеля не может превышать 100 м? (Выберите несколько ответов.)

- а) 100BASE-TX.
- б) 1000BASE-LX.
- в) 1000BASE-T.
- г) 100BASE-FX.

Основные темы

Эта глава начинается с описания концепций локальных сетей (Local Area Network — LAN), в частности, подробного описания процесса передачи фреймов Ethernet коммутаторами. Затем подробно рассмотрены основные принципы дизайна сети и приведена соответствующая терминология. В текущей главе представлен также небольшой обзор оптоволоконных вариантов технологии Ethernet, позволяющей реализовывать сегменты большей длины, чем среда UTP.

Концепции коммутации в локальных сетях

В главе 3 была подробно описана технология Ethernet, а также принцип работы коммутаторов и концентраторов локальных сетей. Чтобы разобраться в принципах работы коммутаторов LAN, следует хорошо разбираться в принципах более старых устройств: *концентраторов* (hub) и *мостов* (bridge). В первой части этого раздела рассказано, зачем вообще были разработаны коммутаторы, а во второй описаны три их основные функции и некоторые другие детали устройств.

Развитие сетевых устройств: концентраторы, мосты и коммутаторы

Как уже говорилось в главе 3, первым вариантом технологии Ethernet была физическая шинная топология на основе коаксиального кабеля. Следующим распространенным вариантом технологии был стандарт 10BASE-T, надежность которого была значительно выше, поскольку проблемы в одном кабеле не влияли на всю сеть (характерная ситуация для сетей 10BASE2 и 10BASE5 с топологией разделяемой шины). В технологии 10BASE-T использовалась неэкранированная витая пара (Unshielded Twisted-Pair — UTP), которая значительно дешевле, чем коаксиальный кабель. Кроме того, во многих организациях витая пара использовалась для телефонии, поэтому стандарт 10BASE-T очень быстро стал разумной альтернативой сетям Ethernet стандартов 10BASE2 и 10BASE5. Типичные топологии для сети стандарта 10BASE2 и сети 10BASE-T с использованием концентратора показаны на рис. 7.1.

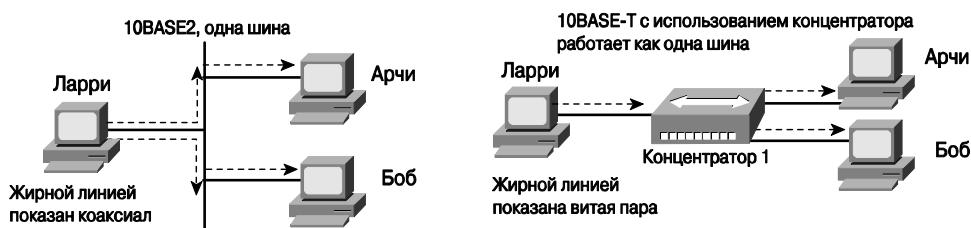


Рис. 7.1. Физические топологии для сети 10BASE2 и сети 10BASE-T с использованием концентратора

Несмотря на то что технология 10BASE-T была заметным шагом вперед в развитии сетевых технологий, у нее все же было несколько существенных недостатков, связанных с использованием концентраторов:

- фрейм, пересылаемый любым устройством, может послужить причиной коллизии в сети, если он “столкнется” с фреймом от другого устройства в том же самом сегменте;
- только одно устройство может пересылать фрейм в один момент времени, т.е. устройства в сегменте работают в режиме конкуренции и разделяют общую полосу пропускания (в 10 Мбит/с);
- широковещательные фреймы, отправляемые одним устройством, будут получены и обработаны всеми устройствами в локальной сети.

Когда были разработаны три указанных выше стандарта Ethernet, разделяемая полоса пропускания в 10 Мбит казалась просто огромной величиной! До того как появились локальные сети (LAN), для работы зачастую использовались упрощенные терминалы, подключенные через канал в 56 Кбит/с к центральному серверу в сети, и множество таких терминалов использовали эту полосу пропускания (всего 56 Кбит/с!) в режиме разделения. Когда появилась технология 10BASE-T Ethernet, ее скорость была просто невероятной для того времени, например, как если бы вы из дома подключались к Интернету через модем, а потом вдруг стали использовать гигабитовое подключение. Поэтому инженерам и пользователям казалось, что такая высокая скорость никогда не понадобится.

С течением времени производительность сетей Ethernet стала заметно ухудшаться. Производители программного обеспечения стали разрабатывать приложения, использующие большую полосу пропускания в локальной сети. В сетях появилось многое больше устройств, чем было изначально. В локальных сетях стали появляться затормозы трафика, поскольку устройства в одном и том же сегменте Ethernet не могут пересыпать больше чем 10 Мбит/с потоков данных, кроме того, они разделяют эту полосу пропускания между собой. Увеличение объемов трафика привело к росту числа коллизий в локальных сетях. Фактически задолго до того, как загрузка сетей Ethernet достигла 10 Мбит/с, в ней появились проблемы из-за большого числа коллизий.

Чтобы решить проблемы с производительностью сети, были разработаны мосты, которые решали проблемы затормозов в сетях Ethernet двумя методами:

- уменьшали количество коллизий в сети;
- увеличивали в сегменте доступную полосу пропускания.

Структура сети с использованием *прозрачного моста* (transparent bridge) показана на рис. 7.2. В верхней части рисунка показана сеть 10BASE-T без использования моста, а в нижней — *сегментированная* с помощью прозрачного моста. Такой мост создает два *домена коллизий*, поскольку фреймы от компьютера Фреда могут вступать в коллизии с фреймами от компьютера Барни, но не с фреймами от компьютеров Вилмы или Бетти. Если один из сегментов локальной сети перегружен и мост не сможет передать в него фрейм, то он просто буферизирует его (хранит в памяти) до тех пор, пока среда передачи данных не освободится. Несмотря на то что количество устройств в сети, а также ее загруженность потоками данных не изменилась, уменьшение количества коллизий приводит к заметному увеличению производительности телекоммуникационной инфраструктуры.

За счет установки *моста* (bridge) между двумя *концентраторами* (hub) сеть разделяется на две независимые сети 10BASE-T: одна слева и одна справа. В сети слева

есть собственные разделяемые сети 10BASE-T 10 Мбит/с, аналогично и в сети справа, поэтому в рассмотренном примере фактически полоса пропускания вырастет почти до 20 Мбит/с по сравнению с сетью, показанной в верхней части рис. 7.2.

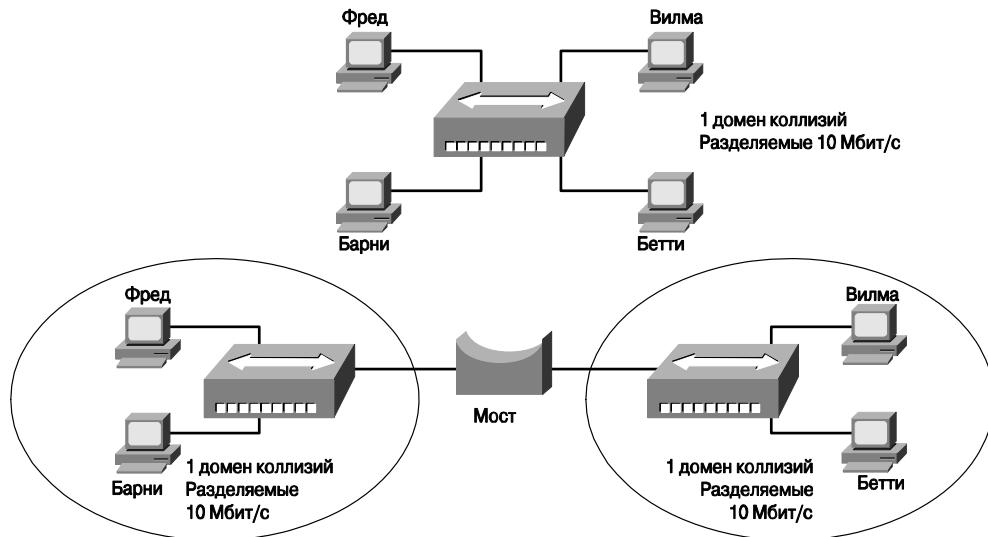


Рис. 7.2. Мост создает два домена коллизий и два разделяемых сегмента Ethernet

Коммутаторы локальных сетей (LAN switches) выполняют те же базовые функции, что и мосты, но у них есть множество дополнительных функций. Как и мосты, коммутаторы сегментируют сеть на различные участки, каждый сегмент представляет собой отдельный домен коллизий. В коммутаторах может быть очень большое количество интерфейсов, специально оптимизированное аппаратное обеспечение, поэтому даже младшие модели коммутаторов Ethernet могут коммутировать миллионы фреймов в секунду. За счет того, что коммутаторы создают отдельный домен коллизий для каждого своего интерфейса и виртуальный маршрут для потока данных между двумя портами, они фактически увеличивают скорость передачи данных. Как было показано в главе 3, если порт коммутатора подключен к одному какому-либо устройству, в таком сегменте Ethernet будет использоваться *дуплексный режим* (full-duplex), поэтому скорость передачи данных удвоится.

ВНИМАНИЕ!

Разделение домена коллизий коммутатором в локальной сети на меньшие домены для каждого интерфейса называется *микросегментацией* сети.

Рассмотренные выше ключевые концепции приведены на рис. 7.3. На нем показаны те же рабочие станции, что и на рис. 7.2, но теперь они соединены коммутатором, интерфейсы которого работают со скоростью 100 Мбит/с и создают четыре домена коллизий. Следует также запомнить, что все интерфейсы работают в дуплексном режиме, поскольку только один компьютер включен в каждый порт, а также что в такой структуре сети вообще не будет коллизий.

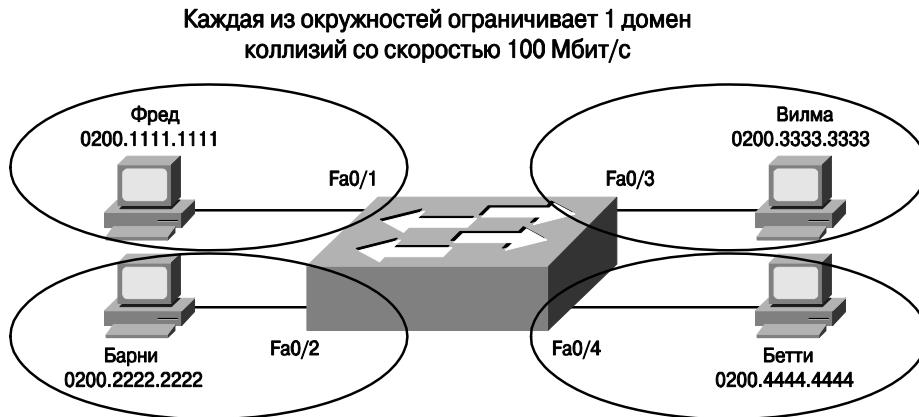


Рис. 7.3. Коммутатор разделяет четыре сегмента Ethernet и создает четыре домена коллизий

В следующем разделе описан процесс пересылки фреймов Ethernet коммутаторами.

Принципы коммутации фреймов

Вполне очевидно, что основная задача коммутатора в локальной сети состоит в пересылке фреймов Ethernet. Для выполнения такой функции устройство использует определенные алгоритмы, основанные на анализе MAC-адресов отправителя и получателя в заголовках Ethernet фреймов. Чтобы понять, как именно работает коммутатор, сначала следует запомнить основные типы адресов, используемые в современных сетях.

Согласно стандартам IEEE MAC-адреса технологии Ethernet можно разделить на три категории:

- **одноадресатные** (unicast addresses), или те, которые идентифицирует один интерфейс, сетевую плату или порт локальной сети;
- **широковещательные** (broadcast addresses) — фрейм с широковещательным адресом в качестве получателя (FFFF.FFFF.FFFF) должен быть принят и обработан всеми устройствами в сегменте локальной сети (LAN);
- **многоадресатные** (multicast addresses) позволяют одновременно принимать трафик некоторой динамически изменяющейся группе сетевых устройств в локальной сети.

ВНИМАНИЕ!

В протоколе IP поддерживается многоадресатная рассылка пакетов. Когда многоадресатный пакет IP передается в среде Ethernet, используется специализированный многоадресатный MAC-адрес определенного формата. Адрес выглядит таким образом: 0100.5exxx.xxxx, где значение от 00.0000 до 7f.ffff может быть использовано во второй половине адреса вместо символов “x”.

Многоадресатные MAC-адреса среды Ethernet выходят за рамки рассмотрения данной книги.

Итак, основная задача любого коммутатора Ethernet заключается в получении фреймов из локальной сети и последующем принятии решения: следует ли такой фрейм переслать через какой-либо порт (порты) или проигнорировать (т.е. отбросить) его. Чтобы выполнить эту задачу, коммутаторы (как, впрочем, и прозрачные мосты) выполняют следующие действия.



Действия, выполняемые коммутаторами

1. Принимают решение о том, следует ли пересыпать фрейм или отфильтровать (не пересыпать) на основании MAC-адреса устройства получателя.
2. Изучают MAC-адреса и строят таблицу коммутации на основании MAC-адресов устройств отправителей фреймов.
3. Поддерживают топологию второго уровня без петель с другими коммутаторами за счет использования протокола распределенного связующего дерева (Spanning Tree Protocol — STP).

Первое из указанных выше действий — это основная задача любого коммутатора, два остальных являются второстепенными, но необходимыми. В последующих разделах подробно описаны указанные выше главные функции коммутаторов.

Фильтрация и передача фрейма

Чтобы принять решение о том, следует ли пересыпать фрейм, коммутатор использует динамически создаваемую таблицу коммутации, в которой содержатся MAC-адреса и идентификаторы выходных интерфейсов. Коммутатор сравнивает MAC-адрес получателя фрейма с записью в такой таблице, чтобы принять решение о том, следует ли передать фрейм дальше или проигнорировать его. Например, обратимся к сети, показанной на рис. 7.4, и представим, что компьютер Фреда пересыпает фрейм компьютеру Барни.

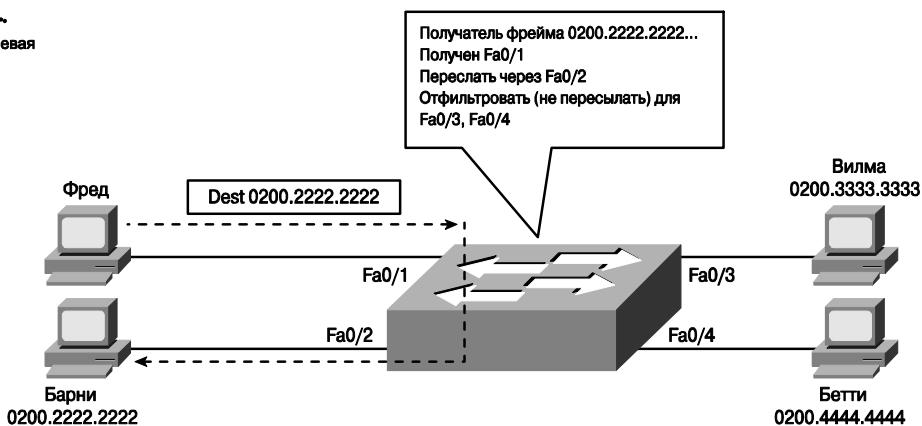


Таблица адресов	
0200.1111.1111	Fa0/1
0200.2222.2222	Fa0/2
0200.3333.3333	Fa0/3
0200.4444.4444	Fa0/4

Маршрут пересылки фрейма

Рис. 7.4. Пример коммутации и фильтрации фреймов

На рис. 7.4 приведен пример принятия решения о пересылке фрейма и о фильтрации. Компьютер Фреда пересыпает фрейм с MAC-адресом получателя 0200.2222.2222 (т.е. MAC-адресом компьютера Барни); коммутатор сравнивает такой адрес получателя со своей таблицей коммутации, чтобы найти совпадение. Таким образом, в рассматриваемой ситуации будет найден выходной интерфейс, через который можно доставить фрейм получателю с MAC-адресом 0200.2222.2222. Поскольку интерфейс, через который был получен фрейм (Fa0/1), отличается от того, через который он должен быть передан (Fa0/2), устройство принимает решение об отправке фрейма через интерфейс Fa0/2, как показано в таблице адресов на рис. 7.4.

ВНИМАНИЕ!

Таблицу MAC-адресов коммутатора также называют *таблицей коммутации* (switching table), *мостовой таблицей* (bridging table) и даже таблицей CAM (Content Addressable Memory — память, адресуемая по содержимому). Последний термин обычно используется для указания типа памяти, используемой для хранения коммутационной информации.

Чтобы понять, куда коммутатор должен отправить фрейм, нужно уметь просматривать и анализировать его таблицу адресов. В таблице содержится информация об адресах и используемых устройством интерфейсах для отправки пакетов к ним. Например, в таблице записано, что адрес 0200.3333.3333 связан с интерфейсом Fa0/3, следовательно, фрейм для такого получателя будет отправлен именно через этот интерфейс (для компьютера Вилмы).

На рис. 7.5 продемонстрирован другой вариант развития событий — коммутатор отфильтровывает фрейм. В данном случае компьютеры Фреда и Барни подключены к концентратору, который, в свою очередь, подключен к порту коммутатора. В таблице MAC-адресов коммутатора в этом примере будут записи для компьютеров Фреда и Барни, связанные с одним и тем же интерфейсом, Fa0/1, и устройство должно пересыпать фреймы с соответствующими идентификаторами получателей через него. Когда коммутатор получает фрейм, отправленный компьютером Фреда (т.е. с MAC-адресом отправителя 0200.1111.1111) и предназначенный компьютеру Барни (т.е. с MAC-адресом получателя 0200.2222.2222), он обнаруживает, что входной и выходной интерфейсы для такого фрейма совпадают, следовательно, пересыпать его повторно в тот интерфейс, из которого он был получен, бессмысленно, и фрейм будет отфильтрован (т.е. отброшен) устройством.

Следует помнить, что концентратор просто воспроизводит электрический сигнал на всех выходных интерфейсах, следовательно, биты передаваемого компьютером Фреда фрейма будут попадать как в интерфейс компьютера Барни, так и в порт коммутатора. Коммутатор принимает решение о фильтрации фрейма (т.е. об отбрасывании), потому что MAC-адрес получателя связан с входным интерфейсом для данного фрейма (т.е. с тем же самым портом — выходным интерфейсом для отправителя).

Как коммутатор находит MAC-адреса

Другой важной функцией коммутатора является механизм обнаружения MAC-адресов и построение таблицы коммутации для них. Если таблица коммутации устройства правильная и точная, коммутатор будет принимать правильные и точные решения об отправке или фильтрации фреймов.

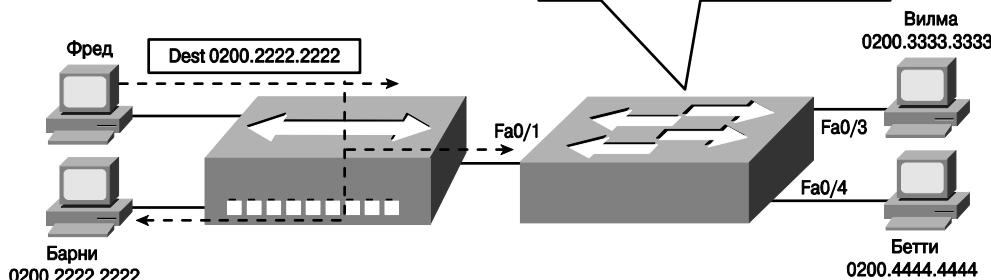


Таблица адресов

0200.1111.1111	Fa0/1
0200.2222.2222	Fa0/1
0200.3333.3333	Fa0/3
0200.4444.4444	Fa0/4

Маршрут пересылки фрейма

Рис. 7.5. Пример фильтрации фреймов

Коммутаторы строят таблицу адресов, просматривая входящие фреймы и выписывая из них *MAC-адреса получателей*. Если на вход какого-либо порта устройства получен фрейм и MAC-адрес в поле отправителя фрейма отсутствует в таблице коммутации, коммутатор создает соответствующую ему запись в таблице. В таблицу помещается адрес и идентификатор интерфейса, через который был получен фрейм.

На рис. 7.6 показана сеть, подобная представленной на рис. 7.4, но в этом примере коммутатор еще не построил себе таблицу коммутации, она пустая. В рассматриваемом на рис. 7.6 случае показаны два начальных фрейма коммуникации между двумя устройствами, первый фрейм от Фреда компьютеру Барни и ответ компьютера Барни компьютеру Фреда.

Как показано на рис. 7.6, после того как компьютер Фреда переслал первый фрейм (обозначен как “фрейм 1”) компьютеру Барни, коммутатор добавляет запись для MAC-адреса 0200.1111.1111 в таблицу коммутации и связывает ее с интерфейсом Fa0/1. Когда на втором этапе компьютер Барни пересыпает ответный фрейм, его адрес, 0200.2222.2222, вместе с идентификатором интерфейса Fa0/2, т.е. порта, через который получен фрейм, добавляется в таблицу коммутации устройства. Коммутатор всегда использует для построения таблицы адресов MAC-адрес отправителя фрейма.

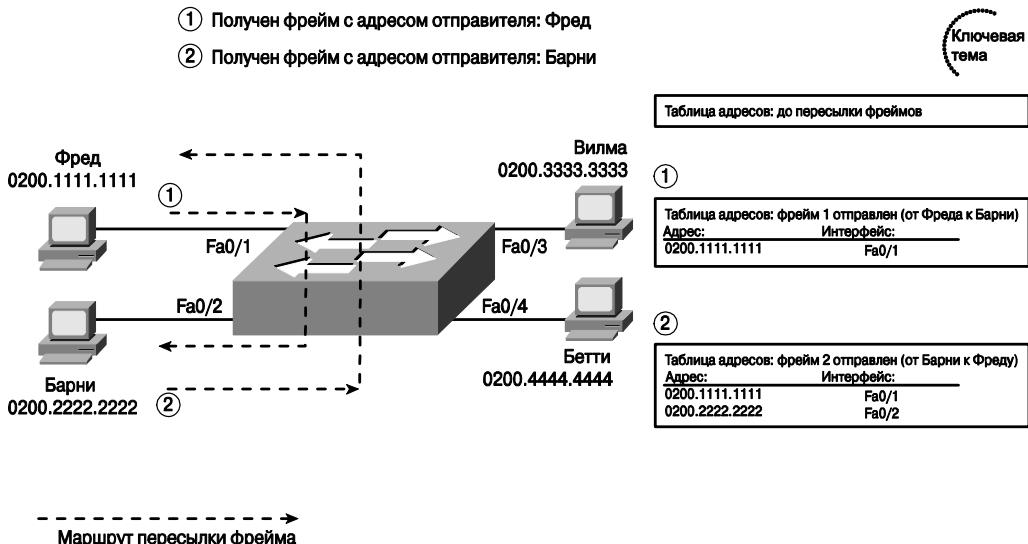


Рис. 7.6. Самообучение коммутатора: пустая таблица и два начальных фрейма

Лавинная рассылка фреймов

Обратимся снова к показанному на рис. 7.6 процессу рассылки фреймов. Как поступит коммутатор с первым фреймом от компьютера Фреда, т.е. на первом этапе обмена данными, если записи в таблице MAC-адресов еще нет? Когда получен фрейм с адресом получателя, отсутствующим в таблице, коммутатор пересыпает такой фрейм через все интерфейсы, кроме того, откуда он пришел. Итак, следует запомнить, что коммутатор всегда рассыпает *одноадресатный фрейм, адрес получателя которого отсутствует в таблице коммутации* (unknown unicast frame), через все интерфейсы в надежде, что искомое устройство окажется в каком-либо из подключенных к нему сегментов Ethernet и ответит на такой фрейм, а следовательно, можно будет внести правильную запись в таблицу MAC-адресов устройства.

Например, как показано на рис. 7.6, коммутатор пересыпает первый фрейм через интерфейсы Fa0/2, Fa0/3 и Fa0/4, несмотря на то, что MAC-адрес получателя 0200.2222.2222 (т.е. компьютер Барни) находится за интерфейсом Fa0/2. Коммутатор не отправляет фрейм обратно в интерфейс Fa0/1, поскольку он был получен через этот порт. Следует заметить, что на рис. 7.6 не показаны фреймы, пересыпаемые через Fa0/3 и Fa0/4, поскольку основное внимание здесь уделяется процессу самообучения коммутатора. Когда компьютер Барни отвечает компьютеру Фреда, коммутатор добавляет запись для MAC-адреса 0200.2222.2222 (и интерфейса Fa0/2) в таблицу адресов. Все последующие фреймы, передаваемые для адреса получателя 0200.2222.2222, не будут пересыпаться в интерфейсы Fa0/3 и Fa0/4, а только в порт Fa0/2.

Процесс пересылки фреймов через все активные интерфейсы коммутатора, кроме того, откуда он пришел, называют *лавинной рассылкой* (flooding). Коммутаторы с использованием лавинной рассылки передают как одноадресатные фреймы, адреса получателей которых отсутствуют в таблице, так и широковещательные. Аналогично устройства поступают с *многоадресатными* (multicast) фреймами, кроме тех случаев, когда в коммутаторах явно настроены некоторые средства оптимизации многоадре-

сатных потоков данных. Многоадресатные технологии выходят за рамки рассмотрения данной книги.

Коммутатор отсчитывает специальный таймер для каждой записи в таблице MAC-адресов, обычно называемый *таймером бездействия* (inactivity timer). Для каждой новой записи, т.е. нового адреса отправителя, такой таймер выставляется в нуль. Каждый раз при получении фрейма с тем же самым MAC-адресом отправителя таймер сбрасывается в нулевое значение. Значение таймера постоянно увеличивается, следовательно, устройство всегда может отследить, какие записи давно не обновлялись и от каких устройств давно не приходили фреймы. Если вдруг у коммутатора закончится место в оперативной памяти для адресных записей, самые старые MAC-адреса могут быть найдены по значению таймера бездействия и удалены из таблицы.

Защита от кольцевых маршрутов с помощью протокола STP

Третья главная функция коммутаторов локальных сетей заключается в предотвращении кольцевых маршрутов с помощью *протокола распределенного связующего дерева* (Spanning Tree Protocol — STP). Без протокола STP фреймы могут бесконечно долго курсировать по кольцевому маршруту, если в сети Ethernet есть резервные каналы. Чтобы избежать зацикливания фреймов, протокол STP блокирует некоторые порты и они не могут пересыпать данные, при этом в сети между сегментами (т.е. доменами коллизий) существует только один активный маршрут для передачи данных. Результат работы протокола распределенного связующего дерева очевиден и прост: в сети остается один маршрут, зацикливания фреймов не происходит, локальная сеть работает стабильно. Несмотря на то что в локальной сети есть резервные каналы, которые станут активными в случае отказа основного соединения, при использовании протокола STP нельзя получить балансировку нагрузки.

Чтобы избежать кольцевых маршрутов на втором уровне, на всех коммутаторах должен быть запущен протокол STP, который каждый из портов каждого устройства переводит или в *заблокированный режим* (blocking state), или в *режим передачи данных* (forwarding). Под *блокированием* (blocking) понимают такое состояние интерфейса, в котором он не может передавать или принимать фреймы пользовательских данных, но может обмениваться только служебными сообщениями протокола STP. В *режиме передачи данных* интерфейс может передавать и принимать пользовательские фреймы с данными. Если протокол заблокировал правильный набор интерфейсов, в сети остается только один активный логический маршрут между каждой парой сегментов.

ВНИМАНИЕ!

Протокол STP абсолютно одинаково работает в коммутаторах и прозрачных мостах, поэтому такие термины, как *мост* (bridge), *коммутатор* (switch) и *мостовое устройство* (bridging device), используются как синонимы в описаниях протокола STP.

Преимущества протокола STP становятся очевидными, если рассмотреть такой простой пример. Вспомним, что коммутаторы лавинно рассыпают фреймы с неизвестным им MAC-адресом получателя и широковещательные сообщения через все интерфейсы.

На рис. 7.7 проиллюстрирована ситуация, когда один фрейм, отправленный компьютером Ларри компьютеру Боба, будет зацикливаться, поскольку в сети есть резервный канал и нет протокола STP.

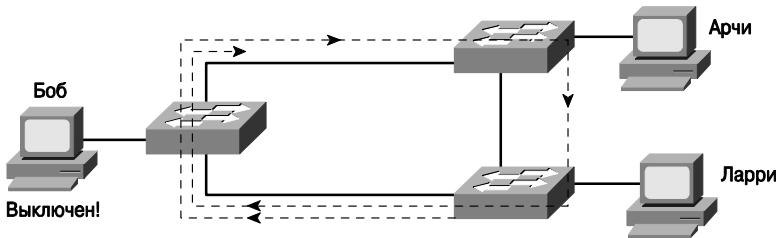


Рис. 7.7. Сеть с резервными каналами без протокола STP — фрейм зацикливается

Компьютер Ларри отправляет единственный фрейм компьютеру Боба, который выключен, следовательно, MAC-адреса хоста Боба нет в таблице коммутации у обоих коммутаторов. Поскольку это первый фрейм, то он представляет собой фрейм с неизвестным коммутаторам MAC-адресом получателя (unknown unicast) и должен быть переслан устройством через все порты, кроме того, откуда он был получен. Такой фрейм будет попадать в бесконечный кольцевой маршрут второго уровня, так как коммутаторы не могут никакими средствами обнаружить адрес компьютера Боба (поскольку он выключен и его адрес не известен устройствам). Коммутаторы будут рассыпать этот фрейм снова и снова до бесконечности.

Аналогично коммутаторы будут пересыпать широковещательные фреймы. Если какой-либо из компьютеров отправит такой фрейм, он также будет курсировать бесконечно по кольцевому маршруту.

Один из вариантов решения описанной выше проблемы — построить локальную сеть без использования резервных каналов, тем не менее, большинство инженеров преднамеренно разрабатывают сети с избыточными каналами для обеспечения отказоустойчивости. На практике, когда какой-либо из каналов отказывает, желательно, чтобы сеть все же работала, поэтому при ее разработке используют резервирование. Правильным решением в таком случае будет то, которое включает в себя коммутируемую локальную сеть с резервными каналами и протокол STP, в задачу которого входит блокирование некоторых интерфейсов, чтобы в сети между двумя конечными устройствами существовал только один активный маршрут второго уровня.

Методы коммутации в коммутаторах Cisco

Выше рассказывалось, как коммутатор принимает решение о том, переслать ли или отфильтровать фрейм. Когда коммутатор компании Cisco принимает решение об отправке фрейма, он может использовать один из механизмов пересылки, которые описаны ниже. Подавляющее большинство устройств на сегодняшний день использует метод коммутации с буферизацией фреймов (store-and-forward), тем не менее все описанные ниже методы внутренней обработки потоков данных реализованы как минимум в одном из выпускаемых компанией Cisco коммутаторов.

Большинство прозрачных мостов и коммутаторов на сегодняшний день использует метод коммутации с буферизацией фреймов. В этом механизме устройство должно получить фрейм полностью, прежде чем начать отправку его первого бита через выходной интерфейс. Существуют еще два метода внутренней обработки фреймов: коммутация без буферизации пакетов (cut-through) и без фрагментации (fragment-free). MAC-адрес получателя расположен в начале заголовка Ethernet, поэтому коммутатор может начать передачу задолго до того, как он примет весь фрейм. Коммутация без буферизации пакетов и коммутация без фрагментации работают именно таким образом, пере-

дача начинается задолго до того, как будет принят весь фрейм, следовательно, время обработки и отправки (т.е. задержка, delay) значительно уменьшается.

Метод коммутации без буферизации пакетов (cut-through) заключается в том, что устройство начинает передачу фрейма как можно раньше, т.е. как только принята часть заголовка, содержащая адрес получателя. Этот метод очень заметно уменьшает задержку в сети, но побочным его результатом будет распространение ошибок в сети. *Контрольная сумма фрейма* (Frame Check Sequence — FCS) находится в концевике Ethernet, следовательно, коммутатор не может определить, есть ли ошибки во фрейме, перед тем как начать передачу. Используя этот метод, следует помнить о двух основных моментах: задержка за счет обработки фреймов устройством значительно уменьшается, но за это приходится платить свою цену — фреймы с ошибками могут быть переданы дальше.

Метод коммутации без фрагментации (fragment-free processing) аналогичен методу коммутации без буферизации пакетов, но через устройство передается меньшее количество ошибок. Одна интересная особенность технологии *множественного доступа с контролем несущей и обнаружением коллизий* (Carrier Sense Multiple Access With Collision Detection — CSMA/CD) состоит в том, что большинство коллизий происходит на первых 64 байтах фрейма. Коммутация без фрагментации похожа на коммутацию без буферизации пакетов в том понимании, что в ней также принимается только часть фрейма, 64 байта, и начинается передача. Задержка за счет обработки фрейма коммутатором в таком случае будет заметно меньше, чем при буферизации, и чуть больше, чем при методе коммутации без буферизации пакетов. Количество предаваемых устройством ошибок также будет намного меньше, чем в методе коммутации с буферизацией.

На сегодняшний день большинство рабочих станций подключено к сети соединениями со скоростью 100 Мбит/с, вышестоящие каналы обычно работают на скорости 1 Гбит/с, в коммутаторах используются очень быстро работающие *специализированные микросхемы* (Application-Specific Integrated Circuits — ASIC) для аппаратной обработки потоков данных, поэтому в современных коммутаторах преимущественно используется метод коммутации с буферизацией фреймов, поскольку на таких скоростях передачи данных заметного уменьшения задержки не происходит.

Внутренние механизмы обработки фреймов в коммутаторах могут сильно отличаться у разных производителей, тем не менее все методы можно свести к трем основным или к некоторым их производным, которые перечислены в табл. 7.2.

Ключевая тема

Таблица 7.2. Методы коммутации фреймов

Метод коммутации	Описание
С буферизацией (store-and-forward processing)	Коммутатор получает фрейм полностью, до последнего бита, сохраняет, а затем начинает его передачу. Этот метод позволяет проверить целостность фрейма по контрольной сумме (FCS) до его отправки
Без буферизации (cut-through)	Коммутатор отправляет фрейм, как только получена нужная информация — MAC-адрес получателя. Этот метод значительно уменьшает задержку, но фреймы с неправильной контрольной суммой (FCS) не будут отброшены устройством
Без фрагментации (fragment-free processing)	Коммутатор начинает передачу, как только получит первые 64 байта фрейма. Этот метод позволяет исключить при коммутации большинство ошибочных фреймов и результатов коллизий

Преимущества и недостатки механизмов коммутации в сетях LAN

В коммутаторах есть множество дополнительных функций, отсутствующих в установленных устройствах для локальных сетей (LAN), таких как концентратор и мост. В частности, к основным достоинствам коммутаторов можно отнести перечисленные ниже.

Преимущества коммутации



- Если к порту коммутатора подключено всего одно сетевое устройство, то он выполняет микросегментацию сети и предоставляет выделенную полосу пропускания для устройства.
- Коммутаторы позволяют осуществлять передачу множественных одновременных потоков данных между устройствами, подключенными к разным интерфейсам.
- Если к порту коммутатора подключено всего одно сетевое устройство, работающее в дуплексном режиме, то эффективная полоса пропускания удваивается.
- Коммутаторы выполняют согласование скорости, означающее, что устройства, подключенные по технологии Ethernet устройствами с разными скоростями, могут взаимодействовать через коммутатор (через концентратор — не могут).

В коммутаторах используются специальные алгоритмы второго уровня, инспектирующие заголовки канального уровня для принятия решения о пересылке фрейма. В частности, коммутаторы принимают решение об отправке или фильтрации фрейма, строят таблицу MAC-адресов и используют протокол STP, чтобы разомкнуть кольцевые маршруты согласно приведенной ниже последовательности.

Резюме по алгоритмам коммутации, фильтрации фреймов и построению таблиц MAC-адресов



- Этап 1** Коммутаторы пересылают фреймы на основании адреса получателя в заголовке фрейма.
- а) Если адрес получателя является широковещательным, много- или одноадресатным, который отсутствует в таблице коммутации, то устройство лавинно рассыпает фрейм.
 - б) Когда адрес получателя известен (т.е. присутствует в таблице MAC-адресов устройства):
 - 1) если в таблице MAC-адресов выходной интерфейс не совпадает со входным для фрейма, коммутатор пересыпает фрейм через найденный в таблице интерфейс;
 - 2) если выходной интерфейс совпадает со входным интерфейсом, коммутатор отфильтровывает фрейм, т.е. просто игнорирует его и никуда дальше не передает.
- Этап 2** Коммутаторы используют следующий алгоритм для заполнения таблицы MAC-адресов.
- а) Для каждого принятого фрейма считывается MAC-адрес отправителя и запоминается интерфейс, откуда он был получен.
 - б) Если пары “адрес–интерфейс” нет в таблице устройства, они добавляются в таблицу коммутации, таймер бездействия (inactivity timer) устанавливается в нулевое значение.
 - в) Если для обнаруженного MAC-адреса уже есть запись в таблице коммутации устройства, таймер сбрасывается (устанавливается в нулевое значение).
- Этап 3** Коммутаторы используют протокол STP для предотвращения образования кольцевых маршрутов, блокируя некоторые из интерфейсов, т.е. переключения их в такой режим, в котором они не могут принимать и передавать пользовательские фреймы.

Принципы построения локальных сетей

До сих пор в этой книге в основном рассматривались отдельные разрозненные функции локальных компьютерных сетей. Например, выше рассказывалось о том, как коммутаторы пересыпают фреймы, были описаны различные варианты распайки кабеля UTP, рассмотрен алгоритм CSMA/CD и как он справляется с коллизиями передачи фреймов. Выше также были описаны различия между коммутаторами и концентраторами, отличия в их принципах работы, например, что концентраторы создают единый домен коллизий, а коммутаторы — несколько и т.д.

В этом разделе представлен более концептуальный подход к проблемам локальных сетей, дальше будут рассмотрены принципы построения средних и крупных локальных сетей. При построении сети малого размера можно купить буквально один коммутатор, подключить к нему правильными кабелями все необходимые устройства, и сеть готова. При разработке же сетей среднего и крупного размера выбор сетевых продуктов значительно больше и вариантов дизайна тоже больше, поскольку можно использовать концентраторы, коммутаторы и маршрутизаторы. Кроме всего прочего, нужно также хорошо обдумать свой выбор, например, моделей коммутаторов, которые отличаются по размеру и количеству портов, а также производительностью, набором функций и, в конце концов, ценой. Среда передачи данных в локальной сети также может быть различной. Инженеру придется взвесить все “за” и “против” как для кабеля UTP (низкая цена и простота установки), так и, например, для оптоволоконной среды (большая длина сегмента и лучшая защита на физическом уровне).

Ниже рассмотрено несколько наиболее важных тем, имеющих непосредственное отношение к дизайну локальных сетей. В частности, сначала рассмотрено поведение сети при использовании в ней концентраторов, коммутаторов и маршрутизаторов для объединения сегментов сети. Далее описана основная терминология компании Cisco в области сетевого дизайна. Завершает раздел краткое описание наиболее популярных разновидностей технологии Ethernet и типов кабелей, а также перечисление ограничения на максимальную длину для каждой технологии.

Широковещательный домен и домен коллизий

Создавая локальную сеть Ethernet, инженер устанавливает в ней некие сетевые устройства, как правило, коммутаторы, несколько маршрутизаторов и, возможно, несколько концентраторов. Разные участки сети могут быть построены и вести себя по-разному с точки зрения производительности и выполняемых функций, в зависимости от типа используемых устройств; при принятии решения о конструкции сети нужно учитывать разные функции оборудования.

Термины *домен коллизий* (collision domain) и *широковещательный домен* (broadcast domain) описывают два важных принципа сегментации локальных компьютерных сетей с помощью оборудования разного типа. В этом разделе описаны основные концепции, связанные с этими терминами в конструкции сетей, а основная цель заключается в том, чтобы объяснить, как концентраторы, коммутаторы и маршрутизаторы влияют на границы доменов коллизий и широковещательных доменов.

Домены коллизий

Как было замечено выше, *домен коллизий* (collision domain) представляет собой набор интерфейсов локальной сети, фреймы от которых могут вступать в коллизии друг с другом, но не с фреймами от остальных устройств в сети (рис. 7.8).

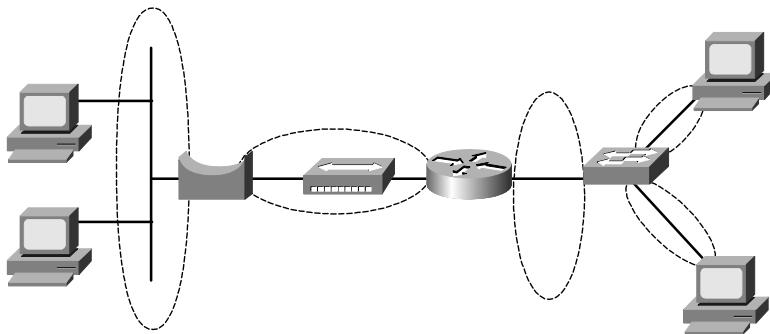


Рис. 7.8. Домены коллизий

Отдельные сегменты, или домены коллизий, показаны на рис. 7.8 пунктирной линией. Коммутатор, изображенный на схеме справа, разделяет локальную сеть на отдельные домены коллизий на каждом порту. Аналогично маршрутизатор и мост разделяют сеть на отдельные домены коллизий (роль маршрутизаторов в этой книге раньше подробно описана не была). Из всех показанных на схеме устройств только концентратор, показанный в центре схемы сети, не создает множество раздельных доменов коллизий для каждого интерфейса. Это устройство просто повторяет фреймы на всех своих портах без буферизации и задержки фрейма перед отправкой в загруженный сегмент сети.

ВНИМАНИЕ!

Структура сети, показанная на рис. 7.8, не является типичным дизайном реальной компьютерной инфраструктуры. Ее основное предназначение — проиллюстрировать домены коллизий и сравнить концентраторы, коммутаторы и маршрутизаторы.

Широковещательные домены

Термин *широковещательный домен* (broadcast domain) описывает участок сети, где могут распространяться широковещательные фреймы. Широковещательный домен включает в себя набор устройств, в котором одно устройство отправляет широковещательное сообщение, а все оставшиеся получают его и обрабатывают. Так, например, поскольку коммутаторы пересыпают все широковещательные и многоадресатные сообщения через все свои порты, кроме того, откуда они пришли, коммутатор создает единый широковещательный домен.

Только маршрутизаторы являются барьером между широковещательными фреймами, т.е. не пропускают их через себя. На рис. 7.9 показаны границы широковещательных доменов для схемы сети, приведенной на рис. 7.8.

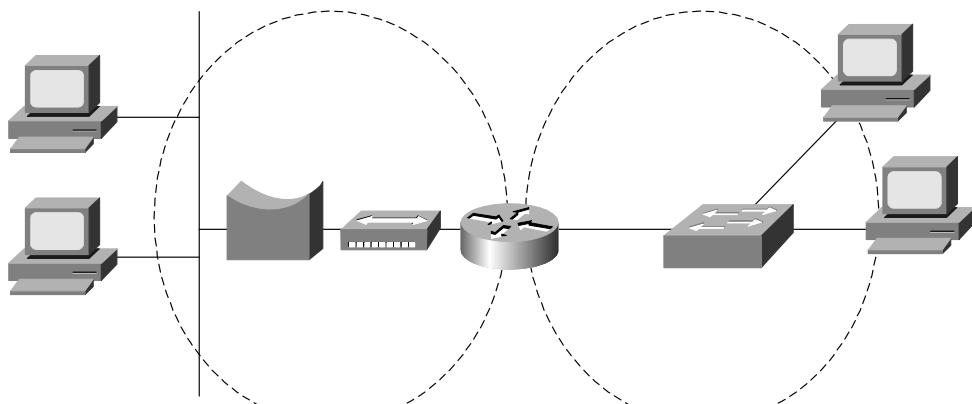


Рис. 7.9. Широковещательные домены

Широковещательное сообщение, отправленное одним устройством в широковещательном домене, не пересыпается устройствами в другом широковещательном домене. В приведенном на рис. 7.9 примере есть два широковещательных домена, т.е. маршрутизатор не будет пересыпать широковещательные фреймы, отправленные компьютером, показанным на схеме слева, в сетевой сегмент, расположенный на схеме справа. Раньше иногда маршрутизаторы, которые не пересыпали широковещательные сообщения, называли *широковещательным брандмауэром* (broadcast firewall).

Краткие определения широковещательного домена и домена коллизий приведены ниже.



Определения широковещательного домена и домена коллизий

- **Домен коллизий** представляет собой группу сетевых интерфейсов (интерфейсных плат, Network Interface Cards — NIC), для которых характерно, что фрейм, отправленный одним из них, может столкнуться в коллизии с фреймом, отправленным другим интерфейсом.
- **Широковещательный домен** представляет собой группу сетевых интерфейсов, для которых характерно, что широковещательный фрейм, отправленный одним из них, будет получен и обработан всеми интерфейсами в группе.

Влияние широковещательных доменов и доменов коллизий на дизайн сети

При разработке локальной сети нужно помнить основные особенности поведения сетевых интерфейсов разных устройств при подсчете их количества в каждом широковещательном домене и домене коллизий. Прежде всего следует рассмотреть поведение устройств в одном домене коллизий и помнить, что:

- устройства разделяют между собой одну доступную полосу пропускания;
- устройства могут неэффективно использовать такую полосу пропускания из-за коллизий, в частности, когда сеть сильно загружена.

Например, в сегменте сети планируется поставить десять персональных компьютеров с интерфейсами Ethernet 10/100. Если все десять компьютеров подключить

к портам концентратора с пропускной способностью 100 Мбит/с, то результатом будет единый домен коллизий и компьютеры будут разделять между собой общую полосу пропускания в 100 Мбит/с. При высокой загрузке производительность такой сети с использованием концентратора будет заметно падать. Если в той же топологии использовать коммутатор вместо концентратора, каждый порт последнего будет создавать собственный домен коллизий, в котором будет доступна полоса пропускания в 100 Мбит/с (т.е. будет создано 10 независимых доменов коллизий). Если к тому же включить дуплексный режим работы для каждого интерфейса, эффективная полоса пропускания для каждого порта (и для каждого домена коллизий!) будет приближаться к 200 Мбит/с, что в сумме для 10 компьютеров будет давать около 2 Гбит/с — очень заметное улучшение производительности сети!

В современных сетях преимущества использования коммутаторов вместо концентраторов вполне очевидны на фоне ошеломляющего увеличения производительности. Честно говоря, во всех новых внедряемых сетях на сегодняшний день используются исключительно коммутаторы. Тем не менее многие производители все еще выпускают концентраторы, поскольку они стоят немного дешевле, чем коммутаторы, и их вполне можно встретить также в некоторых современных сетях.

Далее мы рассмотрим проблемы, связанные с широковещательными сообщениями. Когда сетевой хост получает широковещательное сообщение, он обязан его обработать. Такое утверждение означает, что сетевая карта должна отправить центральному процессору (CPU) прерывание, а процессор должен выделить некоторые свои ресурсы на обработку такого фрейма. Все сетевые хости время от времени отправляют широковещательные фреймы — они необходимы для их нормальной работы. Например, сообщения протокола ARP используют широковещательный механизм работы, как было описано в главе 5. Таким образом, широковещание будет присутствовать в любой сети, это нормальный режим работы, но широковещательные фреймы требуют затрат ресурсов всех сетевых устройств на их обработку.

Рассмотрим теперь локальную сеть большего размера, состоящую из нескольких коммутаторов и 500 компьютеров. Все коммутаторы образуют единый широковещательный домен, поэтому если один из 500 компьютеров отправляет широковещательное сообщение, оставшиеся 499 его получают и обрабатывают. Если широковещательных фреймов в такой сети много, то они могут очень заметно снизить производительность персональных компьютеров в сети. Предположим, мы модифицируем сеть так, чтобы у нас было 5 сегментов по 100 компьютеров, которые разделены маршрутизатором, следовательно, в такой сети будет существовать 5 широковещательных доменов. В такой схеме сети широковещательное сообщение от одного компьютера будет вызывать прерывание у 99 других компьютеров, а 400 будут им “не затронуты”, что приведет к меньшему снижению производительности рабочих станций.

ВНИМАНИЕ!

Построение широковещательных доменов меньшего размера в сети может также значительно улучшить безопасность сети как за счет уменьшения количества широковещательных сообщений, так и за счет расширенных функций безопасности в маршрутизаторах.

Обычно выбор между концентраторами и коммутаторами прост и заканчивается в пользу последних, решить же, когда следует использовать маршрутизаторы для разделения широковещательных доменов, намного сложнее. Подробное описание

всех достоинств и недостатков разных устройств третьего уровня и возможных вариантов их реализации выходит за рамки данной книги. Тем не менее читатель должен понимать концепции широковещательных доменов, а именно, что маршрутизатор разделяет сеть на несколько широковещательных доменов, а концентратор или коммутатор — нет.

В сертификационном экзамене CCNA, скорее всего, будет много вопросов, связанных с терминологией сегментации локальных сетей и ее преимуществами, и мало простых вопросов, ориентированных просто на факты, имеющие отношение к широковещательным доменам и доменам коллизий. В табл. 7.3 перечислены основные преимущества сегментации, которые следует знать. Описанные в таблице функции можно выразить одним вопросом: “Какие из перечисленных ниже преимуществ могут быть получены при установке концентратора, коммутатора или маршрутизатора в сети Ethernet?”

 **Таблица 7.3. Преимущества сегментации сетей Ethernet с помощью концентраторов, коммутаторов и маршрутизаторов**

Преимущество	Концентратор	Коммутатор	Маршрутизатор
В сети общая длина кабеля может быть больше	Да	Да	Да
Сеть разделяется на множество доменов коллизий	Нет	Да	Да
Увеличивается доступная хостам полоса пропускания (bandwidth)	Нет	Да	Да
Сеть разделяется на множество широковещательных доменов	Нет	Нет	Да

Сети VLAN

Во многих корпоративных сетях (Enterprise) на сегодняшний день используются *виртуальные локальные сети* (Virtual LAN — VLAN). Прежде чем перейти к описанию терминологии и принципов работы сетей VLAN, необходимо вспомнить наиболее краткое и точное определение *локальной сети* (Local Area Network — LAN). Несмотря на то что понятие локальной сети может быть знакомо читателю из других книг и источников, мы приведем наиболее точное определение с нашей точки зрения: локальной сетью (LAN) называют совокупность сетевых устройств в одном и том же широковещательном домене.

Следовательно, первое, что следует запомнить: без сетей VLAN коммутатор все свои интерфейсы связывает с одним широковещательным доменом. Другими словами, все подключенные к нему устройства находятся в одной локальной сети (LAN). (В коммутаторах компании Cisco такое поведение реализовано за счет того, что все интерфейсы устройства стандартно связаны с одной сетью VLAN под номером 1.) Если виртуальные сети VLAN все же используются, то коммутатор, согласно конфигурации, помещает одни интерфейсы в один широковещательный домен, другие — в другой. На практике устройство просто связывает некоторые порты с одной сетью VLAN, некоторые — с другой, а точнее, просто с идентификатором соответствующей виртуальной локальной сети. Такие отдельные широковещательные домены в коммутаторе и носят название сетей VLAN.

На двух рисунках ниже приведены две локальные сети и показано, как на них по-влияют сети VLAN. В первом примере (рис. 7.10), чтобы создать два раздельных широковещательных домена, приходится использовать два независимых коммутатора: по одному на каждый широковещательный домен.

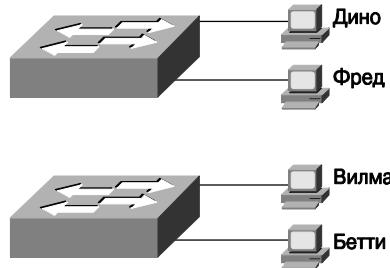


Рис. 7.10. Сеть с двумя широковещательными доменами без сетей VLAN

В качестве альтернативного решения можно предложить приведенную на рис. 7.11 схему сети с раздельными широковещательными доменами. В ней используется только один коммутатор, а раздельные широковещательные домены создаются с помощью виртуальных локальных сетей (VLAN).

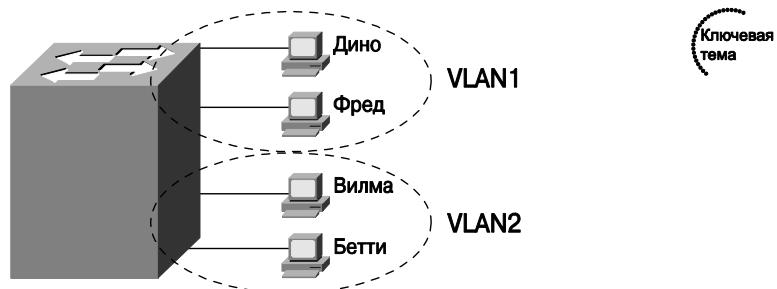


Рис. 7.11. Сеть с двумя широковещательными доменами и двумя сетями VLAN с использованием одного коммутатора

В сети, показанной на рис. 7.11, в действительности не очень нужны сети VLAN, так как она невелика. Тем не менее виртуальные локальные сети могут быть внедрены по многим причинам, в частности:

- чтобы создать более гибкую сетевую инфраструктуру и сгруппировать на логическом уровне пользователей по подразделениям, по выполняемым функциям и рабочим группам, а не на физическом;
- чтобы разделить сеть на более мелкие сегменты (т.е. широковещательные домены) для уменьшения нагрузки на хосты в каждой сети VLAN;
- чтобы уменьшить нагрузку для протокола STP, например, ограничив сеть VLAN одним коммутатором доступа к сети;
- чтобы повысить защиту сети за счет того, что хосты, работающие с критичными для компании потоками данных, вынесены в отдельную сеть VLAN;

- чтобы разделить трафик от IP-телефона и потоки данных от подключенного к нему персонального компьютера.

Конфигурирование, а также поиск и устранение неисправностей в сетях VLAN подробно описаны во втором томе книги.

Терминология дизайна территориальных сетей LAN

Территориальные (или кампусные) локальные сети представляют собой локальные сети, охватывающие крупные здания или несколько рядом расположенных зданий, т.е. некоторую территорию. Так, например, компания может арендовать несколько офисных помещений в разных зданиях одного большого офисного комплекса (office park). Сетевые инженеры такой компании могут построить сеть с использованием магистральных коммутаторов в каждом здании, которые соединены между собой каналами Ethernet, и создать территориальную локальную сеть.

В процессе планирования и разработки территориальной локальной сети инженеры должны рассмотреть различные варианты технологии Ethernet и учесть максимальную длину кабеля в каждой из них. Кроме того, следует учесть различные скорости передачи данных в разных технологиях и подумать о том, что к некоторым коммутаторам будут напрямую подключены устройства пользователей, а к другим будут подключены только коммутаторы доступа к сети пользователей. Кроме всего прочего, в большинстве проектов инженеру приходится учитывать уже имеющееся в сети оборудование и оценивать, нужно ли увеличение пропускной способности и скорости существующих сегментов и следует ли покупать новое оборудование.

Например, большинство уже установленных в сети компьютеров на сегодняшний день укомплектовано сетевыми картами со скоростями передачи данных 10/100, а новые компьютеры имеют встроенные сетевые карты со скоростями 10/100/1000. При использовании правильного типа кабелей такие новые современные рабочие станции могут за счет автосогласования использовать режим 10BASE-T (10 Мбит/с), 100BASE-TX (100 Мбит/с), или 1000BASE-T (1000 Мбит/с, или 1 Гбит/с) в сети Ethernet, причем по тому же самому кабелю UTP. Поэтому перед инженером будет стоять задача выбрать коммутатор с портами, поддерживающими режим 10/100, или устройство с интерфейсами 10/100/1000. Несмотря на разницу в цене, при использовании коммутаторов с режимом работы интерфейсов 10/100/1000 можно построить более масштабируемое решение и подключить практически любое пользовательское устройство. Кроме того, такая сеть будет готова к переходу со скорости передачи в 100 Мбит/с на рабочие станции с подключением в 1000 Мбит/с по мере покупки новых рабочих станций.

Чтобы упорядочить все требования к территориальным локальным сетям, а также облегчить процесс обсуждения принципов дизайна сети между специалистами, в сетях, построенных на оборудовании компании Cisco, используется некоторая общая терминология для описания основных принципов и компонентов. Типичная структура крупной территориальной сети вместе с основными терминами показана на рис. 7.12. Рассмотрим кратко представленную на рисунке терминологию.

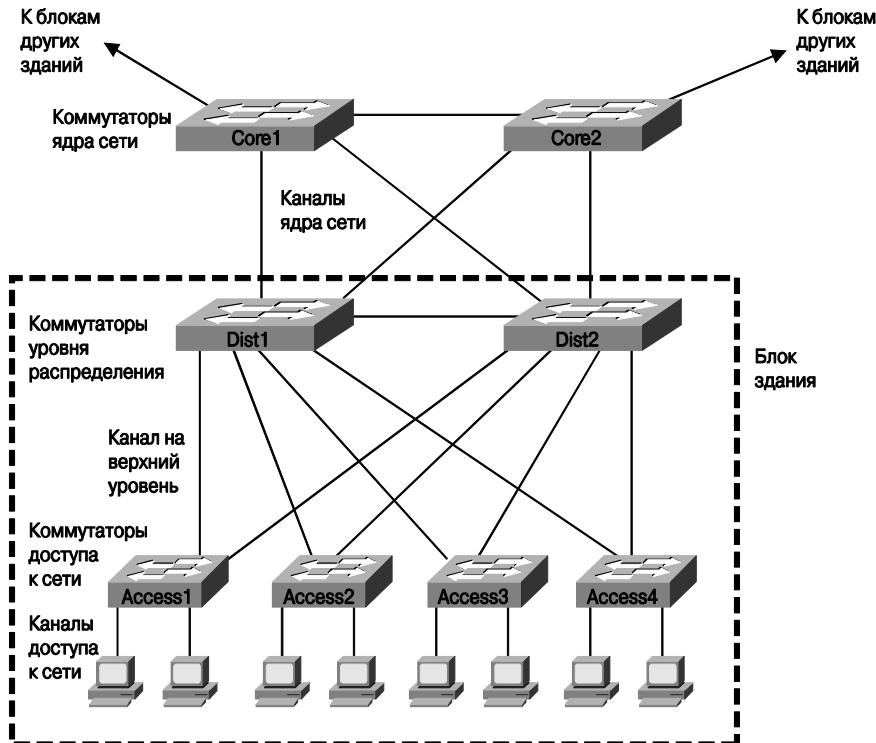


Рис. 7.12. Территориальные сети и их терминология

Согласно подходу компании Cisco используются три основных термина для описания роли каждого коммутатора (или сетевого устройства) в сети: *уровень доступа к сети* (access), *уровень распределения* (distribution) и *ядро сети* (core). Роль устройств определяется исходя из двух основных характеристик:

- подключены ли к коммутатору устройства конечных пользователей;
- должен ли коммутатор пересыпать фреймы между разными коммутаторами и подключен ли он к множеству различных коммутаторов.

К *коммутаторам уровня доступа к сети* (access switches) непосредственно подключены устройства конечных пользователей, которым предоставляется доступ к локальной сети. В нормальных условиях такие коммутаторы только пересыпают фреймы от пользовательских рабочих станций и не должны (по крайней мере, с точки зрения правильного дизайна сети) передавать трафик от одного коммутатора уровня доступа к другому. Например, в нормальных условиях работы сети, показанной на рис. 7.12, коммутатор Access1 не должен пересыпать трафик для компьютеров, подключенных к коммутатору Access3, через коммутатор Access4. Поскольку коммутаторы уровня доступа к сети должны передавать только пользовательский трафик, они менее высокопроизводительны и стоят дешевле; обычно от них требуется только достаточное количество портов для подключения оконечных устройств на этаже или в здании.

В крупных территориальных локальных сетях *коммутаторы уровня распределения* (distribution switches) обеспечивают маршруты для передачи потоков данных между коммутаторами уровня доступа к сети. Согласно стандартным требованиям дизайна сетей каждый коммутатор уровня доступа должен быть подключен как минимум к одному коммутатору уровня распределения. Тем не менее разработчики сетей зачастую используют каналы к двум разным коммутаторам вышестоящего уровня (см. рис. 7.12), чтобы получить сеть с резервированием.

Если в структуре сети использовать коммутаторы уровня распределения, то такой подход может привнести некоторые преимущества, как с точки зрения кабельной системы, так и в плане повышения производительности инфраструктуры в будущем. Представим себе сеть, в которой есть 30 коммутаторов уровня доступа к сети и для которой разработчик решил построить такую схему, где каждый из коммутаторов уровня доступа к сети должен быть подключен к остальным напрямую кабелем. В такой структуре понадобится 435 кабелей только для того, чтобы подключить друг к другу все коммутаторы! Как второй существенный недостаток такой схемы можно указать наличие только одного сегмента для соединения двух коммутаторов. Проблемы будут возникать в том случае, если канал между двумя устройствами обрывается и потоки данных идут через другой, например соседний, коммутатор. Следует учесть, что коммутаторы уровня доступа к сети не предназначены для обработки гигантских объемов данных, они имеют меньшую производительность и за счет этого — меньшую стоимость. Если же подключить рассматриваемые 30 коммутаторов уровня доступа к двум высокопроизводительным коммутаторам уровня распределения, то понадобится всего 60 кабелей (т.е. каналов). Кроме того, правильно подобранные коммутаторы уровня распределения могут обработать большие потоки данных от устройств смежных уровней и обычно позволяют достигнуть более высоких скоростей передачи данных. Такой дизайн сети с использованием двух вышестоящих коммутаторов уровня распределения и двумя каналами от коммутаторов уровня доступа к сети до них предоставляют высокую степень надежности и позволяют построить резервируемую инфраструктуру.

Коммутаторы ядра сети (core) дают еще больший выигрыш в плане агрегирования каналов, чем устройства уровня распределения. Эти коммутаторы работают на еще более высоких скоростях и коммутируют потоки данных еще быстрее; на сегодняшний день их типичная производительность составляет сотни миллионов фреймов в секунду. Тем не менее коммутаторы ядра сети выполняют практически те же функции, что и устройства уровня распределения, но с небольшими отличиями. Зачастую в средних, а обычно в малых территориальных сетях функции обоих уровней, распределения и ядра, объединяют в один.

Ниже кратко описаны функции коммутаторов в территориальных сетях.

- **Уровень доступа к сети** предоставляет точки доступа, или подключения, устройств конечного пользователя. На этом уровне фреймы между двумя коммутаторами доступа к сети в нормальных условиях напрямую не передаются, а должны быть отправлены на уровень распределения.
- **Уровень распределения** является точкой агрегирования каналов от коммутаторов уровня доступа к сети, пересыпает фреймы между коммутаторами, но не служит для подключения устройств конечного пользователя.

- Уровень ядра сети агрегирует каналы от коммутаторов уровня распределения в крупных территориальных локальных сетях и обеспечивает очень высокие скорости коммутации потоков данных.

Среда Ethernet и длина кабелей

Проектируя территориальную локальную сеть, инженер должен прежде всего оценить необходимую длину кабелей и выбрать на основе такой информации необходимую ему технологию Ethernet, поддерживающую сегменты нужной длины. Например, компания арендует помещения в пяти разных зданиях офисного комплекса, поэтому инженеру нужно вычислить длину кабельного маршрута между зданиями и подобрать подходящий канал Ethernet.

Наиболее распространенными на сегодняшний день являются три технологии Ethernet: 10BASE-T, 100BASE-TX, и 1000BASE-T. Для всех указанных технологий характерна максимальная длина кабеля в 100 м, но они слегка отличаются используемым кабелем. Ассоциации EIA/TIA стандартизовали и стандартизируют новые технологии Ethernet, а именно кабельные системы для них, в частности, например, качество кабеля. В каждом из стандартов технологии Ethernet указана категория кабеля, которую можно использовать, причем это минимально требуемая категория, в сети вполне может быть использован и более качественный кабель. Например, в стандарте 10BASE-T рекомендуется использовать кабель категории 3 (Category 3 — CAT3), в технологии 100BASE-TX используется кабель пятой категории (CAT5), а в стандарте 1000BASE-TX нужно использовать кабели категории 5е или 6 (CAT5e или CAT6). Если же инженер планирует использовать (чтобы не пропадала!) существующую кабельную систему, то он должен знать, какой тип кабеля UTP установлен, а также какие ограничения по скорости для соответствующей технологии Ethernet и кабеля существуют.

В нескольких технологиях Ethernet используются оптоволоконные кабели. В кабеле *неэкранированная витая пара* (Unshielded Twisted Pair — UTP) в качестве среды передачи используются медные проводники, по которым протекает ток; в оптоволоконных кабелях используется ультратонкое стеклянное волокно, через которое передаются световые импульсы. Чтобы передать биты, оптические интерфейсы могут менять уровень света, делать ярче или слабее соответственно, кодируя таким образом 1 и 0 в кабеле.

Для оптических кабелей характерна большая длина кабельного сегмента, которая заметно превышает 100 м для кабелей UTP в медных технологиях Ethernet. В оптических кабелях практически нет интерференции сигнала, вызываемой внешними источниками помех, и в зависимости от технологии в оптических коммутаторах в качестве источника сигнала могут быть использованы как лазеры, так и *светодиоды* (Light-Emitting Diode — LED). При использовании лазеров длина кабеля может быть очень большой, например, порядка 100 км на сегодняшний день. Для светодиодов, которые намного дешевле, характерны меньшие расстояния, вполне достаточные для подключения офисов и помещений в рамках территориальной сети.

И в заключение следует учесть, что используемая технология также определяет максимальную длину кабеля. Для оптоволоконных соединений следует помнить, что многомодовое оптическое волокно поддерживает меньшие расстояния, но зато стоит дешевле и позволяет использовать в качестве источника сигнала недорогие свето-

диоды. Второй тип оптоволоконных каналов — одномодовое волокно — поддерживает намного большие длины кабелей, но стоит дорого. Опять же коммутирующее оборудование на основе светодиодов (т.е. для многомодового оптоволокна) стоит значительно дешевле, чем оборудование с лазерными источниками (для одномодового оптоволокна).

В табл. 7.4 перечислены наиболее распространенные типы технологий Ethernet и приведены их ограничения и типы кабелей.

Таблица 7.4. Технологии Ethernet, их среда и максимальная длина сегмента (согласно стандартам IEEE)

Технология Ethernet	Среда	Максимальная длина сегмента, м (футы)
10BASE-T	Кабель UTP стандарта TIA/EIA категории CAT3 или лучше. Используются две пары	100 (328)
100BASE-TX	Кабель UTP стандарта TIA/EIA категории CAT5 или лучше. Используются две пары	100 (328)
100BASE-FX	Многомодовое оптическое волокно 62,5/125 микрон	400 (1312,3)
1000BASE-CX	Кабель STP ¹	25 (82)
1000BASE-T	Кабель UTP стандарта TIA/EIA категории CAT5e или лучше. Используются две пары	100 (328)
1000BASE-SX	Многомодовое оптоволокно	275 (853) для оптоволокна 62,5 микрона; 550 (1804,5) для оптоволокна 50 микрон
1000BASE-LX	Многомодовое оптоволокно	550 (1804,5) для оптоволокна 62,5 микрона и 50 микрон
1000BASE-LX	Одномодовое оптоволокно 9 микрон	5 км (3,1 мили)

Большинство инженеров обычно помнят только общие тенденции, а конкретные числа для максимальной длины кабеля подглядывают в каком-нибудь справочнике или таблице в книге (например, в табл. 7.4). Следует также принимать во внимание физический путь, по которому будет проложен кабель, — он может значительно повлиять на длину кабельного сегмента. Например, нужно проложить кабель из одного конца здания в другой. “Напрямую” это может быть не так уж и много, но нужно учесть, что кабель будет проложен по коробам, т.е. сначала будут выведены спуски, например, из-под фальшпотолка до оборудования кабельного узла. Потом кабель будет проложен по коробам этажа, которые могут быть очень даже извилистыми и похожими на лабиринт, — такой маршрут, вполне очевидно, может быть не самым коротким. И только после расчета реальной протяженности кабельного маршрута следует обратиться к таблице или справочнику и выбрать подходящую среду передачи данных.

¹ Экранированная витая пара (shielded twisted pair). — Примеч. ред.

Подготовка к экзамену

Повторите все ключевые темы

Повторите все ключевые темы данной главы, помеченные пиктограммой “Ключевая тема”. Ключевые темы и соответствующие им страницы перечислены в табл. 7.5.

Таблица 7.5. Ключевые темы главы 7

Элемент	Описание	Страница
Список	Действия, выполняемые коммутаторами	214
Рис. 7.4	Пример коммутации и фильтрации фреймов	214
Рис. 7.5	Пример фильтрации фреймов	216
Рис. 7.6	Самообучение коммутатора: пустая таблица и два начальных фрейма	217
Табл. 7.2	Методы коммутации фреймов	220
Список	Преимущества коммутации	221
Список	Резюме по алгоритмам коммутации, фильтрации фреймов и построению таблиц MAC-адресов	221
Список	Определения широковещательного домена и домена коллизий	224
Табл. 7.3	Преимущества сегментации сетей Ethernet с помощью концентраторов, коммутаторов и маршрутизаторов	226
Рис. 7.11	Сеть с двумя широковещательными доменами и двумя сетями VLAN с использованием одного коммутатора	227

Заполните таблицы и списки по памяти

Распечатайте приложение М (Appendix L) с компакт-диска или его раздел, относящийся к этой главе, и заполните таблицы и списки по памяти. В приложении Н (Appendix M) приведены заполненные таблицы и списки для самоконтроля.

Ключевые термины

Дайте определения перечисленных ниже терминов и проверьте правильность их написания в списке терминов:

широковещательный домен (broadcast domain), широковещательный фрейм (broadcast frame), домен коллизий (collision domain), коммутация без буферизации пакетов (cut-through switching), лавинная рассылка фреймов (flooding), коммутация без фрагментации (fragment-free switching), микросегментация (microsegmentation), сегментация (segmentation), протокол распределенного связующего дерева (Spanning Tree Protocol — STP), коммутация с буферизацией пакетов (store-and-forward switching), одноадресатный фрейм с неизвестным получателем (unknown unicast frame), виртуальная локальная сеть (Virtual LAN — VLAN).

В этой главе...

- **Доступ к интерфейсу командной строки коммутатора Cisco Catalyst 2960.** Описаны коммутаторы компании Cisco серии 2960 и рассказано, как получить доступ к интерфейсу командной строки, чтобы выполнить базовые настройки.
- **Конфигурирование программного обеспечения Cisco IOS.** Описано, как настроить различные параметры устройства с помощью интерфейса командной строки.

ГЛАВА 8

Работа с коммутаторами компании Cisco

Во многих корпоративных сетях и сетях небольших фирм сегодня можно найти коммутаторы Ethernet, поскольку большинство современных компьютеров комплектуется встроенной сетевой картой технологии Ethernet. Коммутаторы в сетях выполняют функцию точки концентрации соединений с устройствами Ethernet в локальной сети и обеспечивают возможность их взаимодействия, с остальной сетью и зачастую с Интернетом.

Командная строка маршрутизаторов компании Cisco выглядит точно так же, как и интерфейс коммутаторов Catalyst, который описан в этой главе. Несмотря на то что текущая глава называется “Работа с коммутаторами компании Cisco”, следует помнить, что пользовательский интерфейс для маршрутизаторов выглядит и работает абсолютно аналогично. В главе 19 продолжается описание основных функций и настроек, но уже в основном для маршрутизаторов.

Контрольные вопросы: знаете ли вы уже темы главы

Этот раздел предназначен для того, чтобы читатель мог предварительно оценить свои знания и решить, нужно ли ему читать главу целиком. Если ответы на девять из десяти вопросов даны правильно, можно сразу же перейти к последнему разделу “Подготовка к экзамену”. Основные темы этой главы и предварительных контрольных вопросов перечислены в табл. 8.1. Отвечая на контрольные вопросы и используя таблицу, читатель сможет достаточно точно определить свои знания в той или иной области. Ответы на вопросы приведены в приложении А “Ответы на контрольные вопросы”.

Таблица 8.1. Темы контрольных вопросов

Основная тема	Номера вопросов
Доступ к интерфейсу командной строки коммутатора Cisco Catalyst 2960	1–3
Конфигурирование программного обеспечения Cisco IOS	4–7

- Из какого режима можно выполнить команду `show mac-address-table?` (Выберите несколько ответов.)
 - Из режима обычного пользователя (User).
 - Из режима привилегированного пользователя (Enable).
 - Из режима глобальной конфигурации (Global configuration).
 - Из режима начальной настройки устройства (Setup).
 - Из режима конфигурирования интерфейса (Interface configuration).

2. В каком из указанных ниже режимов командной строки можно выполнить комманду перезагрузки устройства?
 - а) Из режима обычного пользователя (User).
 - б) Из режима привилегированного пользователя (Enable).
 - в) Из режима глобальной конфигурации (Global configuration).
 - г) Из режима конфигурирования интерфейса (Interface configuration).
3. Коммутаторы компании Cisco поддерживают доступ через сеансы Telnet и SSH. Чем отличаются эти протоколы?
 - а) В протоколе SSH шифруется пароль, используемый при аутентификации, остальной трафик — нет; в протоколе Telnet ничего не шифруется.
 - б) В протоколе SSH шифруется весь обмен данными, в том числе и пароли для аутентификации; в протоколе Telnet ничего не шифруется.
 - в) Протокол Telnet используется операционными системами от компании Microsoft; протокол SSH можно использовать только в операционных системах, подобных Unix, в частности в Linux.
 - г) В протоколе Telnet шифруется только пароль; в протоколе SSH шифруется весь обмен данными.
4. В какой памяти хранится используемая коммутатором конфигурация в процессе его работы?
 - а) RAM.
 - б) ROM.
 - в) Flash.
 - г) NVRAM.
 - д) Bubble.
5. С помощью какой команды можно скопировать конфигурацию из оперативной памяти RAM в энергонезависимую память NVRAM?
 - а) copy running-config tftp.
 - б) copy tftp running-config.
 - в) copy running-config start-up-config.
 - г) copy start-up-config running-config.
 - д) copy startup-config running-config.
 - е) copy running-config startup-config.
6. В каком режиме командной строки устройство запрашивает у пользователя базовую конфигурационную информацию?
 - а) В режиме обычного пользователя (User).
 - б) В режиме привилегированного пользователя (Enable).
 - в) В режиме глобальной конфигурации (Global configuration).
 - г) В режиме начальной настройки устройства (Setup).
 - д) В режиме конфигурирования интерфейса (Interface configuration).

7. Пользователь находится в режиме конфигурирования консольной линии в интерфейсе командной строки. Какая последовательность действий переведет его в режим привилегированного пользователя? (Выберите несколько ответов.)
- а) Необходимо однократно использовать команду `exit`.
 - б) Следует указать команду `exit` два раза подряд в одной командной строке.
 - в) Нужно нажать комбинацию клавиш `<Ctrl+z>`.
 - г) Следует использовать команду `quit`.

Основные темы

После покупки коммутатора Catalyst компании Cisco, когда вы вынули его из коробки, подключили питание от настенной розетки и подключили к нему рабочие станции правильным кабелем UTP, устройство сразу же заработает. Никаких дополнительных действий можно не предпринимать, настройек не вводить и, тем более, не указывать коммутатору, как передавать фреймы Ethernet. Стандартные настройки коммутатора предполагают, что все интерфейсы устройства включены, что использованы правильные кабели и правильные устройства подключены к коммутатору, поэтому он может передавать и принимать фреймы с данными.

Тем не менее в большинстве сетей администраторы хотят иметь возможность проверить состояние коммутатора, просмотреть информацию о том, чем занимается устройство в данный момент, и, возможно, настроить некоторые дополнительные функции. Зачастую также необходимо включить определенные функции безопасности, чтобы позволить сетевым инженерам безопасно подключаться к устройству и контролировать поведение пользователей в сети. Чтобы выполнять все вышеперечисленные действия, у сетевого инженера должна быть возможность подключиться к интерфейсу командной строки коммутатора.

В этой главе рассказывается, как получить доступ к интерфейсу командной строки коммутаторов компании Cisco, какие команды использовать, чтобы проверить текущую работу устройства и как осуществить некоторые базовые настройки устройства. В текущей главе основной упор сделан на процессы конфигурирования, а не на какие-либо определенные наборы команд. В главе 9 более подробно описаны различные команды для настройки устройства с помощью интерфейса командной строки.

У компании Cisco есть две основные фирменные линейки коммутирующих устройств для локальных сетей. Первый бренд, коммутаторы Cisco Catalyst, включает в себя обширный диапазон продуктов, разработанных для крупных и средних предприятий (компаний, государственных служб и т.п.). Линейка коммутаторов Catalyst включает в себя устройства существенно разного размера, производительности, различающихся по функциям и скоростям передачи данных. Второй бренд, коммутаторы серии Cisco Linksys, включает в себя разнообразные продукты для домашних сетей и малых офисов. На данный момент в сертификационном экзамене CCNA основное внимание уделяется внедрению коммутаторов Catalyst в локальных сетях, поэтому в текущей главе будет описано, как получить доступ к командной строке и настройкам только коммутаторов Cisco Catalyst, чтобы проверить работу устройства, настроить коммутатор, а также найти и устранить неисправности. Тем не менее следует отметить, что обе линейки продуктов, Catalyst и Linksys, содержат практически одинаковые функции и технологии, которые были описаны в главах 3 и 7.

Следует помнить, что в этой главе, как и в последующих, когда упоминаются коммутаторы компании Cisco, автор подразумевает именно устройства Cisco Catalyst, а не коммутаторы Cisco Linksys.

Доступ к интерфейсу командной строки коммутатора Cisco Catalyst 2960

В маршрутизаторах и большинстве моделей коммутаторов Catalyst компании Cisco используется одна и та же концепция *интерфейса командной строки* (Command-Line Interface — CLI). CLI представляет собой текстовый интерфейс, в котором пользователь, обычно сетевой инженер, вводит некоторые команды в виде текста. Нажатием клавиши <Enter> такая команда передается коммутатору и указывает устройству, что нужно сделать. Коммутатор выполняет действие, указанное в команде, и в определенных случаях выдает в ответ некоторое информационное сообщение, содержащее результат выполнения команды.

Прежде чем приступить к детальному изучению интерфейса командной строки, рассмотрим сначала наиболее распространенные модели коммутаторов локальных сетей, которые чаще всего встречаются в сертификационном экзамене CCNA. Ниже также будет описано, как сетевой инженер может получить доступ к интерфейсу CLI, чтобы вводить конфигурационные команды.

Коммутаторы Cisco Catalyst и модель 2960

Компания Cisco производит широкий ассортимент коммутирующих устройств Catalyst для локальных сетей, модели которых объединены в *серии* (series) или *семейства* (families) устройств. Каждая серия устройств включает в себя несколько специфических моделей коммутаторов с похожим набором функций, примерно одинаковым соотношением “цена-производительность” и близкими внутренними компонентами устройств.

Компания Cisco позиционирует коммутаторы серии (или семейства) 2960 как недорогое полнофункциональное устройство для *кабельных узлов* (wiring closet) корпоративного уровня. Такое утверждение означает, что эти коммутаторы рекомендуется использовать в качестве устройств доступа к сети, как показано на рис. 7.12 главы 7. Коммутаторы уровня доступа к сети являются точкой подключения устройств конечного пользователя. Такое подключение осуществляется с помощью кабеля, проложенного от рабочей станции пользователя до ближайшего коммутатора в кабельном узле. Коммутаторы серии 2960 подключаются к корпоративной сети с помощью двух каналов к устройствам уровня распределения, обычно к коммутаторам. В качестве коммутаторов уровня распределения обычно используются также устройства компании Cisco, но другой серии — более мощные и дорогие.

На рис. 8.1 представлены фотографии коммутаторов разных моделей серии 2960. Например, верхний коммутатор — это модель WS-2960-24TT-L с 24 портами для разъемов RJ-45 кабеля UTP со скоростями передачи данных 10/100, следовательно, такие порты могут автоматически согласовывать режим работы 10BASE-T или 100BASE-TX Ethernet. В коммутаторе этой модели также есть два дополнительных порта RJ-45 справа, которые могут работать со скоростями 10/100/1000 и обычно используются для подключения устройства к вышестоящим коммутаторам (уровня распределения или ядра) корпоративной локальной сети.

В документации и книгах по устройствам компании Cisco физические соединения коммутатора называют *интерфейсами* (interface), или *портами* (port). Каждый интерфейс обозначается номером в формате *x/y*, где *x* и *y* — разные числа. В коммутаторе модели 2960 число перед косой чертой (/) всегда равно 0, следовательно,

первый интерфейс со скоростью 10/100 обозначается как 0/1, второй — 0/2 и т.д. У каждого интерфейса также есть название, связанное с его технологией работы, например, полное название интерфейса с номером выглядит как “interface FastEthernet 0/1”, означающее первый интерфейс 10/100. Любой интерфейс, поддерживающий гигабитовую скорость работы, обозначается как “GigabitEthernet”, например, первый интерфейс со скоростями 10/100/1000 будет обозначаться в интерфейсе командной строки как “interface gigabitethernet 0/1”.



Рис. 8.1. Коммутаторы серии Cisco 2960 Catalyst

В коммутирующих устройствах компании Cisco встречаются две операционные системы: *межсетевая операционная система* (Internetwork Operating System — IOS) и *операционная система коммутаторов Catalyst* (Catalyst Operating System — Cat OS). В большинстве коммутаторов Catalyst компании Cisco на сегодняшний день используется система IOS, но по некоторым исторически сложившимся причинам высокоразвитые коммутаторы корпоративных локальных сетей поддерживают как систему IOS, так и Cat OS. Для сертификационного экзамена CCNA операционную систему Cat OS можно пока проигнорировать, поскольку вопросов о ней не встречается. Тем не менее о существовании двух операционных систем следует знать, так как в англоязычной литературе и документации можно встретить фразу “IOS-based switch”, которая означает, что в коммутаторе используется именно операционная система Cisco IOS, а не Cat OS.

ВНИМАНИЕ!

В самом популярном магистральном коммутаторе компании Cisco (т.е. в устройстве уровня высокоскоростного ядра локальной сети) серии 6500 может использоваться как операционная система Cisco IOS, так и Cat OS. Такие устройства обычно называют *гибридными* (hybrid), чтобы подчеркнуть, что коммутатор серии 6500 работает с операционной системой Cat OS, и говорят, что коммутатор работает в *собственном* (native) режиме IOS, когда используется операционная система Cisco IOS.

Световые индикаторы коммутатора

Представим себе ситуацию, когда сетевому инженеру нужно быстро проверить, как работает коммутатор, определить состояние портов, чтобы найти и устранить какую-либо проблему в сети. В таком случае очень много времени будет потрачено на консольное подключение к устройству, ввод и интерпретацию результатов команд в интерфейсе командной строки операционной системы Cisco IOS. Чтобы упростить такую задачу, в коммутаторах компании Cisco используются *светодиодные индикаторы* (LED), позволяющие получить некоторую информацию о состоянии устройства, причем как в процессе загрузки устройства, так и при его нормальной обычной работе. Прежде чем переходить к обсуждению интерфейса командной строки (CLI), кратко опишем, какие светодиодные индикаторы есть у коммутатора и что они значат.

У большинства коммутаторов Catalyst компании Cisco на передней панели есть светодиодные индикаторы, в том числе и индикаторы для каждого интерфейса Ethernet. На рис. 8.2 показан коммутатор серии 2960, у которого есть пять индикаторов слева на передней панели, светодиодный индикатор для каждого порта и кнопка переключения режима (mode button).

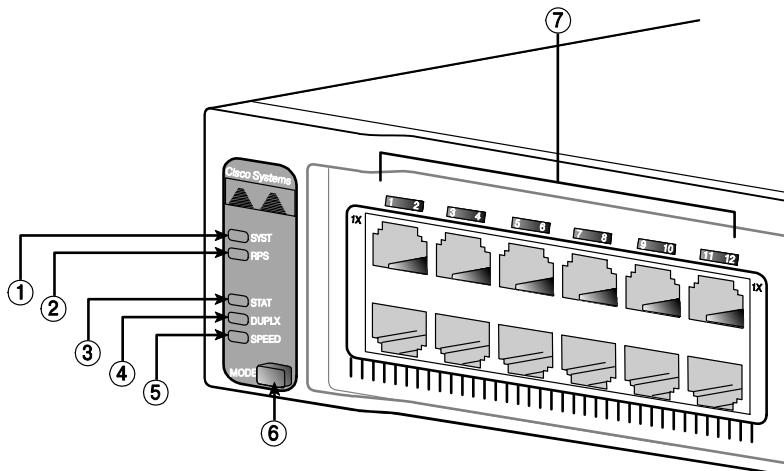


Рис. 8.2. Индикаторы коммутатора 2960 и кнопка переключения режима

На рис. 8.2 показан внешний вид передней панели устройства, а в табл. 8.2 приведено их описание.

Таблица 8.2. Светодиодные индикаторы и кнопка коммутатора на рис. 8.2

Номер на рис. 8.2	Название	Описание
1	SYST (system, системный)	Общее состояние системы
2	RPS (redundant Power Supply, резервный блок питания)	Показывает состояние дополнительного (резервного) блока питания
3	STAT (status, состояние)	Будучи включенным (светится зеленым), сигнализирует о нормальном состоянии порта

Окончание табл. 8.2

Номер на рис. 8.2	Название	Описание
4	DUPLX (duplex, дуплексный)	Будучи включенным (светится зеленым), свидетельствует о работе порта в дуплексном режиме, выключенными — в полудуплексном
5	SPEED	Будучи выключенными, свидетельствует о скорости работы 10 Мбит/с, включенными (светится зеленым) — 100 Мбит/с, мигающим зеленым — 1 Гбит/с
6	MODE	Кнопка переключения режимов индикаторов (STAT, DUPLX, SPEED)
7	Port	Индикаторы указывают разные состояния в зависимости от того, какой режим выбран кнопкой переключения режимов

Рассмотрим несколько примеров, чтобы понять, что означают различные индикаторы. Например, разберемся, о чем сигнализирует индикатор SYST в процессе работы устройства. Для коммутатора серии 2960 этот индикатор может работать в трех режимах:

- не горит — питание коммутатора не включено;
- горит зеленым — питание устройства включено и коммутатор нормально работает (операционная система Cisco IOS нормально загрузилась);
- горит оранжевым — *самотестирование при включении питания* (Power-On Self Test — POST) закончилась с ошибками и операционная система Cisco IOS не загружена.

Если бросить быстрый взгляд на индикатор SYST, то сразу же становится понятным, работает устройство или нет. Если не работает, то можно грубо определить причину: нет электропитания (индикатор не горит) или процедура самотестирования не была успешно завершена (индикатор горит оранжевым) и отказал какой-то аппаратный модуль. Таким образом, сначала нужно проверить и переключить питание; если симптомы не изменились, скорее всего, придется обращаться в службу технической поддержки компании Cisco (Cisco Technical Assistance Center — TAC) либо поставщика оборудования.

Кроме системного индикатора устройства, функции которого достаточно очевидны, у коммутаторов обычно есть индикаторы для каждого порта, размещенные сверху или снизу разъема интерфейса. Что они показывают, зависит от режима работы индикаторов, включенных с помощью кнопки переключения режимов (см. рис. 8.2). Нажимая такую кнопку, можно циклически переключать режим работы индикаторов между состояниями STAT, DUPLX и SPEED (см. табл. 8.2 и рис. 8.2). Чтобы перейти в нужный режим, следует нажать кнопку переключения режимов один или два раза.

В каждом из трех режимов светодиодных индикаторов портов значение индикатора изменяется. Например, в режиме STAT (status, состояние) для каждого порта отображается его состояние:

- выключен — соединение не работает;
- горит зеленым — соединение работает, но через интерфейс не передаются данные;

- мигает зеленым — соединение работает, через интерфейс передаются данные;
- мигает оранжевым — интерфейс административно выключен или был динамически отключен по какой-либо причине.

Для сравнения: если переключить индикаторы в режим SPEED (скорость порта), то они будут просто показывать рабочую скорость передачи данных для интерфейса: выключенный индикатор свидетельствует о скорости 10 Мбит/с, горящий зеленым — 100 Мбит/с, а мигающий зеленым — 1000 Мбит/с (т.е. 1 Гбит/с).

В действительности значение индикаторов и доступные режимы работы для разных серий устройств могут быть существенно разными и совпадать только для устройств внутри серии. Поэтому запоминать на память значения определенных комбинаций индикаторов и режимы работы, скорее всего, бесполезно. Мы не будем подробно останавливаться на всех возможных вариантах работы индикаторов для каждой модели коммутатора или даже для целых семейств устройств, но если читателю нужна дополнительная информация, то он может обратиться к документации компании Cisco. Тем не менее важно запомнить основную идею, т.е. для чего предназначены индикаторы, а также помнить о том, что кнопка переключения режимов используется для изменения класса отображаемой информации. Следует также помнить, для чего нужен индикатор SYST и что он показывает.

В подавляющем большинстве случаев коммутатор включается, успешно загружает операционную систему Cisco IOS, далее инженер получает доступ к интерфейсу командной строки устройства, чтобы управлять устройством и контролировать его. В разделе ниже основное внимание будет уделено тому, как получить доступ к интерфейсу командной строки.

Получение доступа к интерфейсу командной строки системы IOS

Программное обеспечение IOS компании Cisco для коммутаторов Catalyst реализует алгоритмы обработки потоков данных и управляет функциями коммутирующего устройства. Операционная система не только контролирует производительность, функции и поведение коммутатора, но и предоставляет дружественный пользователю *интерфейс командной строки*, обычно обозначаемый аббревиатурой CLI (Command Line Interface). Интерфейс CLI операционной системы Cisco IOS подразумевает использование какой-либо программы эмуляции терминала, которая позволяет передавать вводимый в ней текст устройству. Когда пользователь нажимает клавишу <Enter>, программа пересыпает текст, а коммутатор обрабатывает его так, как если бы это была команда, и возвращает некоторый ответ обратно программе-эмulationатору.

Получить доступ к интерфейсу командной строки можно с помощью трех популярных методов: через консольное подключение, через протокол Telnet и различные варианты программы протокола SSH (Secure Shell). Два последних метода предполагают, что коммутатор установлен в уже работающей, причем правильно, сети IP, через которую осуществляется дистанционное управление устройством. Консольное подключение — это специализированный физический порт в устройстве для доступа к интерфейсу командной строки и конфигурирования. На рис. 8.3 показаны различные варианты доступа к интерфейсу командной строки коммутатора.

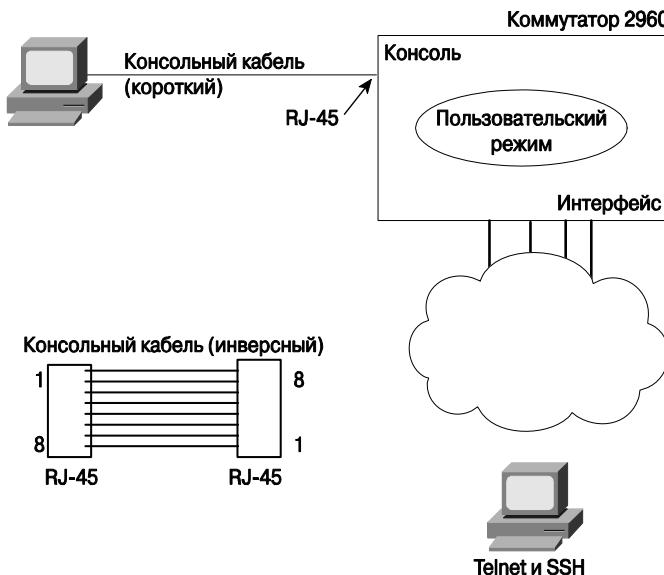


Рис. 8.3. Доступ к интерфейсу командной строки

ВНИМАНИЕ!

Для конфигурирования коммутатора можно также использовать веб-интерфейс, который не похож на интерфейс командной строки. Для такой настройки используется диспетчер управления устройствами Cisco (Cisco Device Manager — CDM) или диспетчер управления устройствами безопасности Cisco (Cisco Security Device Manager — SDM). Основы программного обеспечения описаны в главе 23, в частности, рассказывается о настройке маршрутизаторов с помощью этого продукта.

В последующих разделах три метода доступа к интерфейсу командной строки будут описаны подробнее.

Доступ к интерфейсу командной строки через консоль

Консольный порт используется для доступа к интерфейсу командной строки коммутатора прежде всего в том случае, если устройство еще не подключено к локальной сети. У всех коммутаторов компании Cisco есть консольный интерфейс, который на физическом уровне представляет собой стандартное гнездо RJ-45. *Последовательный порт* (serial port) обычного персонального компьютера подключается к такому консольному интерфейсу с помощью консольного (инверсного) кабеля UTP. В консольном кабеле UTP контакт №1 разъема RJ-45 на одном конце кабеля подключен к контакту №8 разъема RJ-45 на другом, соответственно контакт №2 подключен к контакту №7 на другом конце, контакт №3 — к контакту №6 и так далее, поэтому такой кабель иногда называют инверсным, или перекрещенным (rollover). В большинстве персональных компьютеров для последовательного порта не используется разъем RJ-45, поэтому нужно использовать специализированный адаптер, например, переходник с девятиконтактным стандартным разъемом последовательного порта в RJ-45 или адаптер порта USB в RJ-45. На рис. 8.4 показана

схема подключения порта DB-9 (девятиконтактного) персонального компьютера к гнезду RJ-45 консольного порта коммутатора.

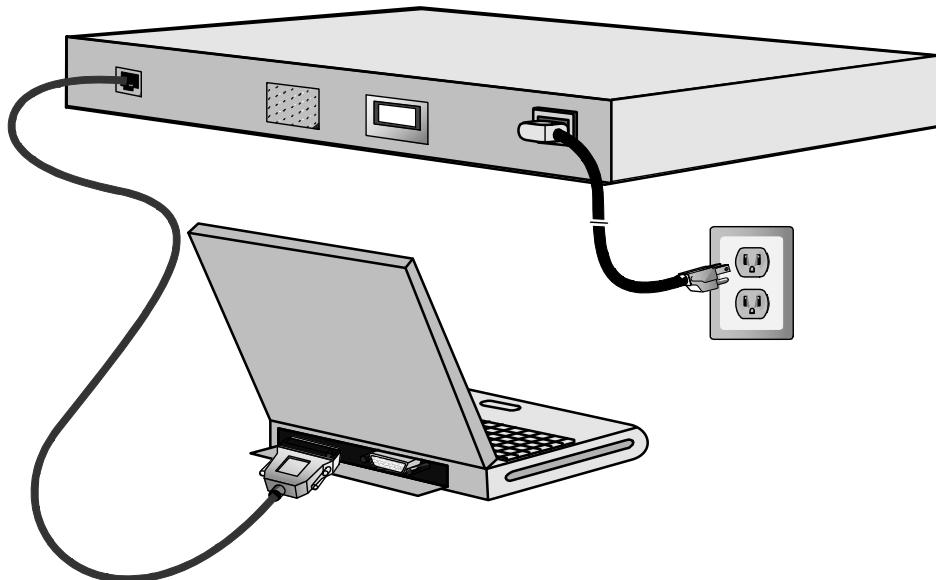


Рис. 8.4. Консольное подключение к коммутатору

После того как компьютер физически подключен к консольному порту устройства, на нем должно быть установлено и настроено программное обеспечение эмуляции терминала. Современное программное обеспечение эмуляции терминала зачастую также поддерживает протоколы Telnet и Secure Shell (SSH), которые могут быть использованы для доступа к интерфейсу командной строки через компьютерную сеть, а не через консольный порт.

На рис. 8.5 показано окно программного обеспечения терминала Tera Term Pro и его настройки (этот бесплатный программный продукт доступен на веб-сайте разработчика <http://www.ayera.com/teraterm>). Эмулятор терминала нужно настроить так, чтобы он использовал последовательный порт компьютера, а настройки его должны совпадать со стандартными настройками коммутатора. Стандартные настройки консольного порта коммутатора должны быть следующими:

Стандартные настройки консольного порта коммутатора компании Cisco



- скорость 9600 бод/с;
- без аппаратного контроля потока (hardware flow control);
- 8 бит данных;
- без контроля четности (no parity);
- 1 стоповый бит.

Последние три настройки по первым буквам параметров для простого запоминания записывают как “8N1”.

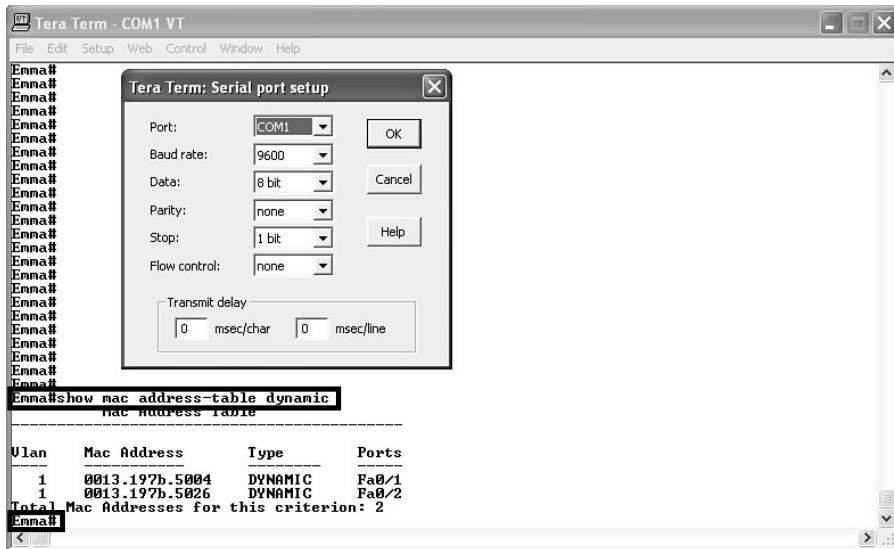


Рис. 8.5. Настройки программы эмуляции терминала для подключения к консоли

На рис. 8.5 показано окно программы-эмулятора терминала с результатом выполнения нескольких команд и окно настроек, которые были перечислены выше.

В выводимой на терминале информации выделен текст `Emma#show mac address-table dynamic`, в которой часть строки приглашения, `Emma#`, обычно показывает название устройства (в данном случае `Emma`), заданное системным администратором. Эта строка представляет собой команду, введенную системными инженером (`show mac address-table dynamic`), в ответ на нее коммутатор перешлет программному обеспечению эмулятора терминала некоторую информацию. На рисунке эта информация следует сразу же после выделенной команды. Второй блок выделенного текста внизу, т.е. строка приглашения `Emma#`, появляется после выполнения и выдачи результатов команды коммутатором. Окно терминала будет оставаться в таком состоянии и с таким приглашением интерфейса командной строки сколь угодно долго, пока пользователь не введет что-либо еще в командной строке.

Доступ к интерфейсу командной строки с помощью протоколов Telnet и SSH

Приложение Telnet стандартного стека протоколов TCP/IP позволяет эмулятору терминала взаимодействовать с устройством и выглядит очень похоже на консольное подключение. В отличие от последнего, в этом приложении используется сеть IP для отправки и получения данных, а не специализированный кабель и физический порт в устройстве. В протоколе уровня приложений Telnet программа эмуляции терминала рабочей станции называется клиентом Telnet, а устройство, принимающее команды и отвечающее на них, — сервером Telnet. Telnet — это основанный на механизме TCP протокол уровня приложений, использующий стандартный зарезервированный порт с номером 23.

Чтобы использовать службу Telnet, пользователь должен установить клиент Telnet на своей рабочей станции¹. (Как было сказано выше, большинство современных пакетов программного обеспечения эмуляции терминала включает в себя клиент Telnet и SSH.) Сервер Telnet в коммутаторе стандартно запущен и работает всегда, тем не менее, чтобы он мог отправлять и принимать пакеты IP, для устройства нужно задать IP-адрес. (Установка IP-адреса подробно описана в главе 9.) Кроме того, чтобы рабочая станция сетевого инженера или администратора и коммутатор могли обмениваться пакетами, сеть между двумя устройствами должна правильно работать.

Многие из сетевых инженеров постоянно используют клиент Telnet, чтобы контролировать и настраивать коммутаторы, — инженер может находиться на своем рабочем месте, ему не нужно идти в соседнее здание, а иногда и ехать в другую область или в другую страну, тем не менее у него есть возможность что-либо выполнять в интерфейсе командной строки устройства. Протокол Telnet пересыпает все данные (в том числе имя пользователя и пароль для доступа к устройству) в виде открытого текста, что представляет собой очень серьезную потенциальную брешь в системе безопасности.

Безопасный протокол SSH (Secure Shell) выполняет те же самые основные задачи, что и Telnet, но с более высоким уровнем защищенности. Точно так же как и в модели Telnet, в протоколе SSH есть клиентское программное обеспечение, выполняющее эмуляцию терминала. Аналогично используется протокол TCP для пересылки данных, но зарезервирован другой стандартный порт — 22 (а не 23, как в протоколе Telnet). В протоколе также есть сервер (в данном случае на коммутаторе), принимающий команды от клиента, обрабатывающий их текст и отправляющий ответ обратно. Основное отличие между протоколами Telnet и SSH состоит в том, что последний шифрует абсолютно весь обмен данными, поэтому он обеспечивает намного более высокий уровень конфиденциальности и защиты, чем Telnet.

Пароли на доступ к интерфейсу командной строки

Коммутатор компании Cisco будет устройством с высоким уровнем безопасности только в том случае, если он закрыт на замок в комнате или в шкафчике. Стандартно доступ к командной строке устройства осуществляется только через консольный порт, но не через протоколы Telnet или SSH. Подключившись с помощью консоли, можно получить доступ к командам любого уровня и, если есть на то вдохновение, выключить необходимые для нормальной работы функции устройства. Тем не менее консольный доступ требует физического доступа к коммутатору, поэтому такая стандартная настройка вполне разумна: устройство как минимум нужно базово настроить, когда его только вынули из коробки.

Независимо от стандартных настроек, имеет смысл защитить паролями как консольный доступ, так и доступ по протоколам SSH и Telnet. Инженеру потребуется настроить всего лишь несколько простых команд, чтобы добавить в коммутатор базовую аутентификацию по паролю. Процесс конфигурирования описан в этой главе ниже, а необходимые команды показаны в крайнем правом столбце табл. 8.3. В таблице показаны настройки для аутентификации по паролю консоли и виртуальных терминалов (vty); после того как указанные команды будут введены, коммутатор начинает при подключении выдавать запрос на простую аутентификацию (это результат команды `login`) и ожидает от пользователя ввода пароля, указанного в команде `password`.

¹ В действительности простейшее приложение Telnet входит практически в любую операционную систему, где есть поддержка стека TCP/IP. — Примеч. ред.

Таблица 8.3. Настройка паролей доступа к интерфейсу командной строки для консоли и подключений Telnet

Метод доступа	Тип пароля	Пример конфигурации
Консоль	Консольный пароль	line console 0 login password faith
Приложение Telnet	Пароль терминала vty	line vty 0 15 login password love

В коммутаторах компании Cisco консольный порт обозначается как специализированная линия, а именно как консольная линия 0. Устройство также поддерживает 16 одновременных сеансов протокола Telnet, называемых *виртуальными линиями* (vty) и нумеруемых с 0 по 15. Команда `line vty 0 15` указывает коммутатору, что следующие за ней настройки будут применены ко всем 16 возможным виртуальным терминальным соединениям с устройством, при этом такие настройки будут использоваться как для сеансов Telnet, так и SSH.

ВНИМАНИЕ!

В старых версиях операционной системы поддерживалось только пять одновременных удаленных сеансов, или линий vty: с 0 по 4.

После ввода конфигурационных команд, перечисленных в табл. 8.3, у каждого подключающегося с помощью консоли к устройству пользователя будет запрошен пароль, и он должен будет ввести слово `faith`, согласно настройкам. Для каждого нового сеанса Telnet также будет запрашиваться пароль, в данном случае слово `love`. В рассмотренной конфигурации не нужно вводить имя пользователя, только пароль.

Чтобы настроить доступ SSH к устройству, понадобится добавить еще несколько команд, кроме тех, которые указаны в табл. 8.3. Протокол требует наличия открытого ключа шифрования для обмена общим ключом между сервером и клиентами, который, собственно, и будет использоваться для шифрования трафика. Кроме того, протокол SSH требует более высокого уровня безопасности, поэтому в нем запрашивается как имя пользователя, так и пароль. Полезные примеры, этапы и конфигурирование нужных характеристик и параметров протокола SSH подробнее рассмотрены в главе 9.

Пользовательский и привилегированный режимы

Три рассмотренных выше метода доступа к устройству (консольное подключение, сеанс Telnet и SSH) подключают пользователя к режиму интерфейса командной строки, называемому *пользовательским режимом* (user mode), или режимом EXEC обычного пользователя (user EXEC mode). В этом режиме пользователь преимущественно может просматривать различную информацию, но не настроить или “сломать” что-то. Приставка “EXEC” используется для того, чтобы подчеркнуть, что когда пользователь вводит какую-либо команду, коммутатор ее выполняет и выводит некоторое сообщение о результатах работы.

В операционной системе Cisco IOS есть расширенный режим, называемый *привилегированным режимом* (privileged mode), привилегированным режимом EXEC, или

enable-режимом. Последний вариант названия режима возник из соответствующей режиму команды, используемой для перехода в него, — `enable` (рис. 8.6). Привилегированным режим называется потому, что позволяет использовать более “мощные”, или привилегированные, команды для работы с устройством. Например, в этом режиме можно использовать команду `reload`, позволяющую перезагрузить устройство, и эта команда доступна только из привилегированного режима.

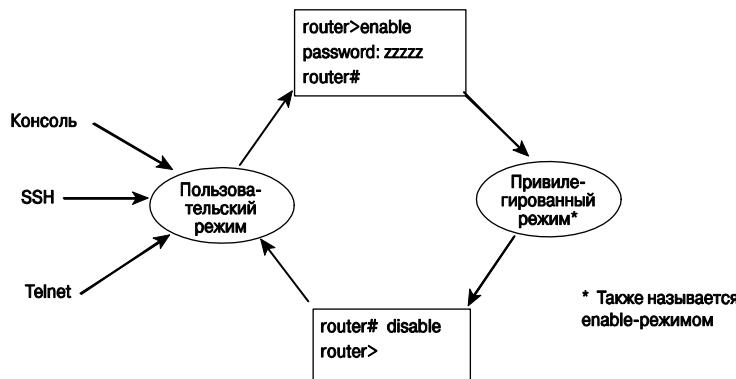


Рис. 8.6. Пользовательский и привилегированный режимы

ВНИМАНИЕ!

Следует запомнить, что если в приглашении командной строки в конце имени устройства стоит символ угловой скобки (`>`), то это обычный пользовательский режим; если в конце имени устройства стоит символ “решетки” (`#`), то это привилегированный режим.

Предпочтительным методом конфигурирования пароля для доступа к привилегированному режиму является команда вида `enable secret` пароль. Следует помнить, что если пароль для привилегированного режима не установлен (стандартное состояние), то из сеансов Telnet и SSH операционная система Cisco IOS не разрешит пользователю зайти в привилегированный режим, а в консольном подключении — разрешит. Такое поведение отражает описанный выше подход компании Cisco к безопасности устройств: стандартно пользователи за пределами защищенного сетевого или кабельного узла, аппаратной или серверной комнаты не могут получить доступ к устройству без вмешательства сетевого инженера.

ВНИМАНИЕ!

Зачастую команды, которые могут быть использованы как в обычном режиме EXEC, так и в привилегированном режиме EXEC, называют просто командами EXEC.

Выше были описаны основные особенности стандартной настройки коммутаторов компании Cisco, которые следует учитывать, если вы приобрели и устанавливаете новое устройство. Коммутатор будет работать без какой-либо конфигурации, достаточно просто включить питание и подключить кабели Ethernet, и сеть заработает. Тем не менее рекомендуется подключиться к консольному порту устройства и задать пароли для консольного доступа, протоколов Telnet и SSH, а также установить пароль для привилегированного (enable) режима.

В разделах ниже описаны некоторые функции интерфейса командной строки, не зависящие от метода доступа и режима работы.

Интерактивная подсказка

Если распечатать справочник по командам операционной системы Cisco IOS (Cisco IOS Command Reference), то получится стопка бумаги не меньше метра высотой. Никто не ждет, что сетевой инженер будет помнить все команды, да и никто их не сможет запомнить. Существует несколько простых и удобных методов и инструментов для запоминания команд операционной системы, также помогающих сэкономить время на печатании команд. По мере продвижения ко все более сложным экзаменам и сертификациям компании Cisco количество команд, которые нужно запомнить, будет расти, поэтому следует знать, как пользоваться встроенной в операционную систему подсказкой.

В табл. 8.4 перечислены пункты интерактивной подсказки операционной системы IOS, связанные с вызовом команд, вводившихся ранее инженером. Обратите внимание на то, что в первом столбце таблицы слово *команда* — это какая угодно произвольная команда, а не команда с именем *команда*; аналогично слово *параметр* — любой параметр команды. Например, в третьей строке таблицы показан пример интерактивной подсказки в виде *команда ?*, который может означать как команду *show ?*, так и команду *copy ?*, или любую другую команду со знаком вопроса в конце, в результате которой будет выведена подсказка по доступным параметрам.

Таблица 8.4. Интерактивная подсказка операционной системы Cisco IOS

Вводимая команда	Подсказка
? help	Список всех команд, доступных для текущего режима Текст, описывающий как пользоваться подсказкой. Подсказка для команд не выводится
команда ?	Текстовая подсказка, описывающая первый параметр команды
команды ?	Эта команда выдаст список команд, начинающихся с символов <i>команды</i>
команда начальные_буквы_параметра ?	Список параметров, начинающихся с указанной последовательности символов (обратите внимание: между параметром и знаком вопроса нет пробела!)
команда начальные_буквы_параметра<Tab>	Если нажать клавишу <Tab> в середине любого параметра какой-либо команды, интерфейс командной строки или закончит слово команды, или ничего не сделает. Если нажатие клавиши не приводит к какому-либо результату, значит, у команды есть несколько параметров, начинающихся с уже введенной последовательности символов, и интерфейс не знает, какой из них выбрать
команда параметр1 ?	Если между параметром команды и знаком вопроса стоит пробел, интерфейс командной строки выводит список следующего параметра команды и короткое текстовое описание каждого

Следует помнить, что интерфейс командной строки операционной системы Cisco IOS реагирует на ввод знака вопроса (?) мгновенно — нажимать клавишу <Enter> или какую-либо другую не нужно. Операционная система после вывода подсказки

повторно выводит все, что было введено в командной строке до символа ?, чтобы облегчить жизнь системному инженеру. Если нажать клавишу <Enter> сразу же после ввода знака вопроса, система Cisco IOS повторит команду без знака вопроса в конце и выполнит ее по нажатию клавиши, т.е. только с теми параметрами, которые были введены до знака вопроса.

Вид подсказки зависит от того, в каком режиме интерфейса командной строки находится пользователь. Например, если нажать <?> в режиме обычного (непrivилегированного) пользователя, будут показаны команды, которые разрешено выполнять из этого режима, а команды из привилегированного режима не будут отображаться. По-другому также будет выглядеть интерактивная подсказка при использовании ее в режиме конфигурирования — как минимум, она будет показывать со всем другие команды. Подробнее режим конфигурирования описан ниже. Итак, следует запомнить, что в любом из подрежимов можно воспользоваться интерактивной подсказкой, но ее результат будет разным.

Операционная система Cisco IOS сохраняет вводимые пользователем команды в так называемом буфере истории команд, стандартно в нем хранится десять записей. Интерфейс командной строки позволяет перемещаться вперед и назад по такому списку введенных команд и редактировать “прежние” команды перед их повторным введением. Необходимые для навигации по буферу истории команд клавиши и их комбинации помогут значительно быстрее перемещаться по командам на экзамене и в практической работе, поэтому их нужно запомнить. В табл. 8.5 перечислены клавиши и комбинации клавиш для работы с буфером.

Таблица 8.5. Комбинации клавиш для вызова и редактирования команд из буфера

Комбинация клавиш	Выполняемое действие
<↑> или <Ctrl+p>	Отображает последнюю введенную команду, если нажать ее еще раз, предпоследнюю и так далее до тех пор, пока не закончится буфер (символ “p” означает “previous”; в переводе с англ. предыдущий)
<↓> или <Ctrl+n>	Если пользователь перешел на какую-либо из ранее введенных команд, эти клавиши перемещают вперед по буферу истории команд (символ “n” означает “next”; в переводе с англ. следующий)
<←> или <Ctrl+b>	Перемещает курсор влево (часто говорят “назад”) по командной строке на один символ без удаления текста (символ “b” означает “back”; в переводе с англ. назад)
<→> или <Ctrl+f>	Перемещает курсор вправо (“вперед”) по командной строке на один символ без удаления текста (символ “f” означает “forward”; в переводе с англ. вперед)
<Backspace>	Однократное нажатие удаляет последний введенный символ и перемещает курсор влево
<Ctrl+a>	Эта комбинация клавиш перемещает курсор в начало строки на самый первый символ команды
<Ctrl+e>	Перемещает курсор в конец командной строки
<Ctrl+r>	Повторно отображает командную строку. Эта комбинация клавиш полезна, когда выводимые устройством сообщения мешают вводить команду
<Ctrl+d>	Эта комбинация клавиш удаляет один символ
<Esc+b>	Перемещает курсор на одно слово назад
<Esc+f>	Перемещает курсор на одно слово вперед

Команды `debug` и `show`

Команда `show`, несомненно, самая популярная в операционной системе Cisco IOS. У нее есть великое множество разнообразных параметров, позволяющих отследить состояние практически всех функций операционной системы, аппаратных модулей и т.п. Команда `show` отображает текущее состояние коммутатора, все, что устройство делает в ответ на любой вариант этой команды, — просто находит нужную информацию о состоянии чего-либо и отправляет ее в виде сообщений пользователю.

Менее популярной, но не менее полезной является команда отладки `debug`. Точно так же как и у команды `show`, у нее есть огромное количество параметров, но, в отличие от первой команды, принцип работы последней существенно отличается. Если команда `show` выдает некоторое текущее состояние какой-либо функции, другими словами, состояние устройства в какой-то определенный момент времени, то команда `debug` позволяет отслеживать функцию в процессе работы в течение промежутка времени. Так, например, коммутатор может отправлять сообщения пользователю о каких-либо событиях, когда они происходят.

Команды `show` и `debug` можно сравнить с фотографией и с фильмом соответственно. Как и на фотографии, в выводе команды `show` показано что-то актуальное в определенный момент времени, другими словами, некоторая “застывшая картина”; такая операция не требует много ресурсов. Команда `debug` показывает, как развивается процесс, что происходит и тому подобное; такой процесс требует намного больше ресурсов. Вполне очевидно, что команда `debug` требует значительно больше времени центрального процессора, в этом состоит ее основной недостаток, в то же время она показывает, что происходит в момент, когда происходит событие.

Операционная система Cisco IOS обрабатывает сообщения, созданные командой `debug`, иным образом, чем полученные от команды `show`. Когда любой из пользователей, подключенных к устройству, вводит команду `debug` с параметрами, операционная система, независимо от того, какой вариант команды был введен и кем из пользователей, трактует отладочные сообщения как сообщения системного журнала (`log message`). Любой из подключенных к устройству пользователей, в том числе и дистанционный (если ввести команду `terminal monitor`), может получать такие системные сообщения. Кроме того, системные сообщения стандартно автоматически выводятся в консольный порт. Команда `show` выводит набор сообщений для одного пользователя; команда `debug`, в отличие от нее, может выводить сообщения всем заинтересованным пользователям, для чего необходимо только ввести команду, позволяющую смотреть системные сообщения.

Если вывод какой-либо информации был включен командой `debug` с параметрами, то сообщения будут появляться до тех пор, пока пользователь не отключит их явно или не перезагрузит устройство. Перезагрузка (командой `reload`) устройства отключает все варианты отладки. Чтобы отключить вывод каких-либо определенных отладочных сообщений, следует использовать ту же самую команду `debug` с теми же самыми параметрами и ключевым словом `no` в начале командной строки. Например, пользователь ввел команду `debug spanning-tree`; чтобы ее отключить, нужно ввести команду `no debug spanning-tree`. Можно также использовать команды `no debug all` и `undebug all`, чтобы отключить абсолютно все отладочные сообщения, которые были заданы ранее.

Следует помнить, что некоторые параметры команды `debug` создают огромное количество отладочных сообщений и, как следствие, система Cisco IOS не может их обработать или происходит аварийный отказ операционной системы. Просмотреть загрузку процессора устройства можно с помощью команды `show process`, это рекомендуется выполнить до запуска команд отладки. Чтобы быть уверенным в том, что устройство не “повиснет” или вдруг не перезагрузится от большой нагрузки, рекомендуется сначала ввести команду `no debug all`, а потом команду `debug` с параметрами. Если в результате выполнения второй команды устройство начнет работать неустойчиво, можно с помощью клавиши `<↑>` или комбинации `<Ctrl+p>` вызвать команду `no debug all` из буфера и применить ее. Если производительность устройства из-за отладки значительно упала, коммутатор может быть “слишком занят”, чтобы отслеживать, что вводится в командной строке. Прием, описанный в последнем абзаце, сэкономит время системному администратору и, несомненно, поможет избежать аварийного отказа операционной системы и незатребованной перезагрузки устройства.

Конфигурирование программного обеспечения Cisco IOS

Чтобы сдать сертификационный экзамен и достичь успеха в профессиональной деятельности, нужно уметь настроить коммутатор компании Cisco. В этом разделе описаны основные последовательности конфигурирования различных функций, в том числе что такое конфигурационный файл и где он может быть сохранен. Несмотря на то что в текущем разделе основное внимание уделяется принципам конфигурирования устройств, а не каким-либо конкретным командам, все приведенные здесь команды нужно запомнить на память для сдачи экзамена и четко себе представлять процесс конфигурирования устройства.

Режим конфигурирования (configuration mode) устройства представляет собой специализированный режим интерфейса командной строки, в чем-то похожий на режим обычного или привилегированного пользователя. Режим привилегированного пользователя позволяет инженеру вводить “неопасные” для работы устройства команды и просматривать различные характеристики и информацию о состоянии устройства. В привилегированном режиме имеется намного больше команд по сравнению с пользовательским, в том числе и команды, которые могут привести к неработоспособности устройства. Тем не менее ни в пользовательском, ни в привилегированном режиме нельзя изменить настройки коммутатора. Только в режиме конфигурирования устройства можно ввести конфигурационные команды, т.е. команды, сообщающие устройству, что нужно предпринять и как нужно что-то сделать. На рис. 8.7 показана взаимосвязь режимов конфигурирования, пользовательского и привилегированного.

Вводимые в конфигурационном режиме команды изменяют активный (т.е. текущий) конфигурационный файл. Изменения попадают в конфигурацию сразу же после нажатия клавиши `<Enter>` в конце команды, поэтому следует быть осторожным и аккуратным при вводе команд!

Конфигурационные подрежимы и контексты

В конфигурационном режиме коммутатора или маршрутизатора есть много подрежимов. Контекстные команды настройки переводят пользовательский интерфейс из одного подрежима конфигурирования, или контекста, в другой. Такие команды

указывают маршрутизатору, с чем будут связаны вводимые после них команды. Что еще более важно, текущий подрежим указывает коммутатору, какие именно команды могут быть введены, поэтому, нажав знак вопроса (?) на клавиатуре, чтобы получить подсказку, вы увидите команды, относящиеся только к текущему контексту интерфейса командной строки.

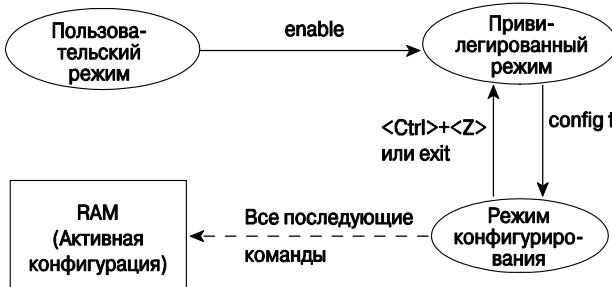


Рис. 8.7. Режимы конфигурирования, пользовательский и привилегированный

ВНИМАНИЕ!

Контекстные команды настройки (context-setting) — это не стандартный термин компании Cisco, а термин автора, здесь он используется только для удобства описания различных режимов конфигурирования.

В качестве примера контекстной команды настройки устройства рассмотрим комманду `interface`. Пользовательский интерфейс коммутатора переключается в режим конфигурирования интерфейса после ввода команды, например, `interface FastEthernet 0/1` в режиме глобальной конфигурации устройства. Если в таком подрежиме вызвать встроенную подсказку как обычно, в ней будут присутствовать только команды, характерные для интерфейсов Ethernet. Команды в таком режиме иногда называют *подкомандами* (subcommand), или, в данном случае, подкомандами конфигурирования интерфейса. Зачастую также специфические режимы конфигурирования называют *подрежимами* (submode). Стоит попрактиковаться в конфигурировании настоящих коммутаторов и маршрутизаторов, тогда переходы между режимами станут более понятными. Теперь рассмотрим небольшой пример (см. пример 8.1) конфигурирования устройства, в котором показаны такие моменты:

- переход из привилегированного режима в режим глобальной конфигурации устройства с помощью комманды `configure terminal`;
- использование комманды `hostname Fred` режима глобальной конфигурации для настройки названия устройства;
- переход из режима глобальной конфигурации в режим конфигурирования консольной линии с помощью комманды `line console 0`;
- установка простого метода аутентификации по паролю с помощью комманды `password hope`;
- переход из режима конфигурирования консольного порта в режим конфигурирования интерфейса с помощью комманды `interface`;

- установка скорости в 100 Мбит/с для интерфейса Fa0/1 с помощью команды `speed 100`;
- переход из режима конфигурирования интерфейса обратно в режим привилегированного пользователя с помощью команды `exit`.

Пример 8.1. Переходы между различными подрежимами конфигурирования

```
Switch#configure terminal
Switch(config)#hostname Fred
Fred(config)#line console 0
Fred(config-line)#password hope
Fred(config-line)#interface FastEthernet 0/1
Fred(config-if)#speed 100
Fred(config-if)#exit
Fred(config)#[/pre]

```

Текст в скобках в приглашении командной строки устройства идентифицирует текущий конфигурационный режим, например, после введения соответствующей команды в первой строке во второй строке примера 8.1 видно, что режим поменялся. Обозначение “`(config)`” сообщает пользователю, что он находится в режиме глобальной конфигурации. После выполнения команды `line console 0` текст в скобках меняется на “`config-line`”, что сигнализирует пользователю о том, что он перешел в режим конфигурирования линии. В табл. 8.6 перечислены наиболее часто встречающиеся в работе варианты приглашения командной строки, названия соответствующих режимов и контекстные команды для перехода в такие режимы.

Таблица 8.6. Конфигурационные режимы коммутатора



Приглашение командной строки	Название режима	Команды для перехода в режим
<code>hostname(config) #</code>	Глобальной конфигурации	<code>configure terminal</code>
<code>hostname(config-line) #</code>	Конфигурации линии	<code>line console 0</code> <code>line vty 0 15</code>
<code>hostname(config-if) #</code>	Конфигурации интерфейса	<code>interface тип номер</code>

Каких-либо особых правил для глобальных команд или подкоманд не существует, тем не менее можно запомнить такое простое эмпирическое правило: если какой-то параметр может быть установлен в коммутаторе несколько раз, то соответствующая команда, вероятнее всего, вводится в каком-либо подрежиме. Если какая-то настройка может быть выставлена только один раз для всего коммутатора в целом, скорее всего, это команда глобального режима конфигурирования. Например, команда `hostname` относится к глобальной настройке устройства, поскольку название (`hostname`), или имя хоста, у коммутатора может быть только одно. Для сравнения: команда `duplex` является настройкой подрежима конфигурирования интерфейса, следовательно, может быть введена несколько раз, и для различных интерфейсов могут быть указаны разные настройки.

Комбинация клавиш `<Ctrl+z>` и команда `end` используются для перехода из любого конфигурационного режима или подрежима в режим привилегированного пользователя. Еще одна команда, `exit`, переводит интерфейс на один режим назад,

например, из какого-либо подрежима в режим глобальной конфигурации или из одного подрежима в вышестоящий.

Где хранятся конфигурационные файлы?

Когда системный инженер настраивает коммутатор, он использует текущую конфигурацию. Текущую конфигурацию нужно где-либо сохранять, чтобы при отсутствии питания можно было ее заново загрузить и использовать. В коммутаторах компании Cisco есть *оперативное запоминающее устройство*, ОЗУ (Random Access Memory — RAM), используемое для хранения данных, которые нужны операционной системе Cisco IOS. Все данные в оперативной памяти (RAM) пропадают после перезагрузки или выключения питания устройства. Чтобы сохранить информацию, которая понадобится после выключения питания устройства, в коммутаторах компании Cisco используется несколько разновидностей постоянных запоминающих устройств, в которых нет никаких движущихся механических частей. За счет того, что механизмов в запоминающих устройствах нет (как в жестких дисках компьютеров, например), отказоустойчивость устройств заметно увеличивается и время наработки на отказ становится намного больше.

Ниже перечислены четыре основные типа памяти, которые есть в коммутаторах компании Cisco, а также описано применение соответствующего хранилища.

- *Оперативная память* (Random Access Memory — RAM), иногда еще называемая *динамическим оперативным запоминающим устройством* (Dynamic Random-Access Memory — DRAM), используется в коммутаторе точно так же, как и в любом компьютере: для хранения текущей рабочей информации. *Текущая* (running) или *активная* (active) конфигурация устройства хранится в этой памяти.
- *Постоянное запоминающее устройство* (Read-Only Memory — ROM) хранит *программу самозагрузки* (bootstrap или boothelper), которая срабатывает при включении питания устройства. Программа самозагрузки находит образ операционной системы Cisco IOS и управляет процессом его загрузки в оперативную память, после чего операционная система берет управление устройством на себя.
- *Флеш-память* (flash memory) представляет собой микросхему в коммутаторе, или съемный модуль памяти, в котором хранится полнофункциональный образ (или образы) операционной системы, и именно здесь процедура самозагрузки стандартно ищет систему. Во флеш-памяти могут также храниться другие файлы, например резервные копии конфигурационных файлов.
- *Энергонезависимая память* (Nonvolatile RAM — NVRAM) используется для хранения *начальной*, или *стартовой* (startup), конфигурации устройства, использующейся при включении питания коммутатора и перезагрузке устройства.

На рис. 8.8 проиллюстрирована представленная выше информация в краткой форме, чтобы упростить запоминание материала.

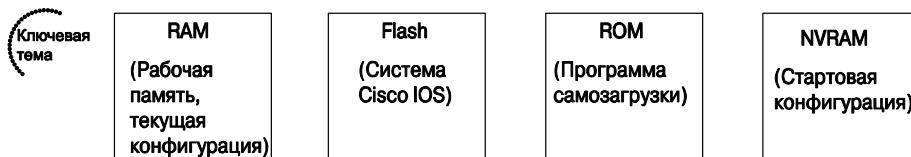


Рис. 8.8. Различные типы памяти коммутатора Cisco

Операционная система Cisco IOS сохраняет последовательность конфигурационных команд в виде конфигурационного файла. В действительности в коммутаторе есть два конфигурационных файла: файл стартовой конфигурации, используемой при загрузке устройства, и файл текущей конфигурации, хранимый в оперативной памяти. В табл. 8.7 указаны оба конфигурационных файла, их местоположение и предназначение.

Таблица 8.7. Названия и назначение двух основных конфигурационных файлов операционной системы Cisco IOS



Название конфигурационного файла	Назначение	Где хранится
Startup-config	Содержит стартовую конфигурацию, используемую каждый раз при загрузке и перезагрузке операционной системы Cisco IOS	NVRAM
Running-config	Содержит текущие настройки устройства. Этот файл изменяется, когда кто-то вводит команды в режиме конфигурирования устройства	RAM

По существу, когда системный инженер использует любой конфигурационный режим, он изменяет *файл текущей конфигурации* (running-config). Так, если вспомнить пример 8.1, то все вводимые в нем команды меняют только текущую конфигурацию устройств, и если после их ввода перезагрузить коммутатор (или если вдруг пропадет электропитание), вся новая конфигурация будет потеряна. Если же требуется, чтобы конфигурация сохранилась, то следует скопировать текущую конфигурацию в энергонезависимую память (NVRAM), т.е. перезаписать *файл стартовой конфигурации* (startup-config) устройства.

В примере 8.2 показано, как команды режима конфигурации устройства меняют только текущий конфигурационный файл в оперативной памяти коммутатора. В этом примере продемонстрированы следующие этапы и концепции.

- Этап 1** Проверить, что стартовая и текущая конфигурации совпадают, можно по параметру `hostname`.
- Этап 2** С помощью команды `hostname` инженер изменяет название устройства, но, согласно стандартному поведению коммутатора, только в файле текущей конфигурации (running-config).
- Этап 3** На последнем этапе показан результат выполнения команд `show running-config` и `show startup-config` (показана настройка только названия устройства). По выводимой на экран информации можно определить, что два конфигурационных файла отличаются.

Пример 8.2. Конфигурационные команды меняют только файл текущей конфигурации (running-config), но не стартовой (startup-config)

! Две команды, приведенные ниже, относятся к первому этапу
!

```
hannah#show running-config
! (строки конфигурации опущены)
hostname hannah
! (остальные строки также опущены)

hannah#show startup-config
! (строки конфигурации опущены)
```

```

hostname hannah
! (остальные строки также опущены)
! Ниже идут команды второго этапа.
! Обратите внимание, что приглашение командной строки меняется
! сразу же после ввода команды hostname.
!
hannah#configure terminal
hannah(config)#hostname jessie
jessie(config)#exit
! Две команды, приведенные ниже, относятся к третьему этапу
!
jessie#show running-config
! (строки конфигурации опущены)
hostname jessie
! (остальные строки также опущены)
! Обратите внимание, что в текущей конфигурации
! отображается измененное название устройства.
jessie# show startup-config
! (строки конфигурации опущены)
hostname hannah
! (остальные строки также опущены)
! Обратите внимание, что в стартовой конфигурации
! название устройства не поменялось.

```

ВНИМАНИЕ!

Для обозначения того, что в большинстве компьютерных операционных систем называется *перезапуском* (rebooting) или *перезагрузкой* (restarting), компания Cisco использует термин *перезагрузка* (reload). В любом случае это подразумевает повторную инициализацию программного обеспечения. Для перезагрузки коммутатора используется команда EXEC reload.

Копирование и удаление конфигурационных файлов

Если бы в самом конце примера 8.2 коммутатор был перезагружен, то именем хоста стало бы “hannah”, как в самом начале, поскольку файл текущей конфигурации (running-config) не был скопирован в файл стартовой конфигурации (startup-config). Тем не менее, если нужно, чтобы новым именем хоста стало “jessie”, следует выполнить команду copy running-config startup-config, которая перепишет файл стартовой конфигурации (startup-config) и занесет в него информацию из файла текущей конфигурации. Команда copy используется для копирования файлов в коммутаторе, обычно конфигураций, или образов, операционной системы Cisco IOS. Это наиболее простой способ передачи файлов в коммутатор и из него, причем перемещать файлы можно между оперативной и энергонезависимой памятью, сервером TFTP и т.п. Файлы могут быть скопированы между разными устройствами, как показано на рис. 8.9.

Общий формат копирования файлов в операционной системе Cisco IOS выглядит следующим образом.

```
copy {tftp | running-config | startup-config} {tftp | running-config | startup-config}
```

Первый параметр в фигурных скобках ({}) указывает, откуда копировать файл, второй — куда.

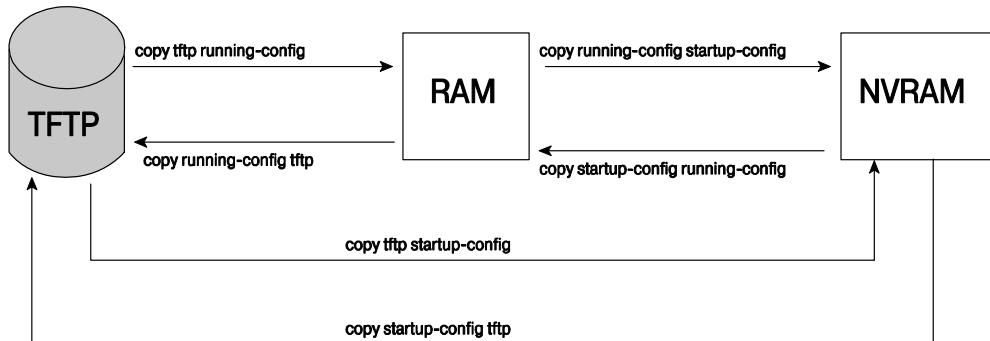


Рис. 8.9. Копирование файлов и результат этой операции

Команда `copy` всегда заменяет существующий файл на копируемый при перемещении файла в память NVRAM или на сервер TFTP. Другими словами, она удаляет файл, в который копируется источник, и заменяет его новым. При копировании файла из какого-либо источника в текущую конфигурацию (`running-config`) в оперативной памяти устройства файлы конфигурации не удаляются и не заменяются новыми, а объединяется, т.е. результирующая конфигурация будет комбинацией старого и нового конфигурационных файлов. В действительности команда `copy` при копировании файла в оперативную память работает так, как если бы инженер вводил по очереди команды из нового конфигурационного файла в интерфейсе командной строки.

“Ну, и какая разница, как работает команда?” — подумает читатель. Очень большая. Представим себе, что текущая конфигурация была изменена, но результат получился неудовлетворительным. Инженер решает вернуться к стартовой конфигурации и выполняет команду `copy startup-config running-config`, чтобы убрать неправильные настройки, но в результате два файла конфигурации, стартовой и текущей, все равно не будут совпадать. Единственным гарантированным методом возврата конфигурации в исходное состояние в этом случае будет команда `reload`, в результате выполнения которой коммутатор перезагрузится, все изменения в оперативной памяти будут потеряны, а при загрузке стартовая конфигурация будет скопирована в оперативную память, т.е. в файл текущей конфигурации.

Чтобы удалить содержимое энергонезависимой памяти (NVRAM), можно использовать три команды: `write erase` и `erase startup-config` (устаревшие варианты команды), `erase nvram`: (рекомендуемый современный вариант команды). Все указанные команды просто очищают память NVRAM и, следовательно, удаляют стартовый конфигурационный файл. Если же сразу после удаления содержимого энергонезависимой памяти перезагрузить коммутатор, стартовой конфигурации не будет. Следует также запомнить, что у операционной системы компании Cisco нет команды для удаления текущей конфигурации (`running-config`), поэтому для очистки текущей конфигурации необходимо удалить файл стартовой конфигурации (`startup-config`) и перезагрузить устройство (командой `reload`).

ВНИМАНИЕ!

Текущие конфигурации всех коммутаторов и маршрутизаторов в сети должны быть скопированы в безопасное место: на сетевой сервер, рабочую станцию сетевого инженера и т.п. Такой подход должен быть частью общей стратегии сетевой безопасности компании, поскольку позволит быстро заменить конфигурацию устройства в случае отказа или после хакерской атаки, в результате которой были изменены или повреждены настройки оборудования.

Несмотря на то что для конфигурационных файлов чаще всего используются два названия, *startup-config* и *running-config* (соответственно стартовая и текущая конфигурации), в операционной системе Cisco IOS определены два формализованных названия. В устройствах компании для работы с файлами используется специализированная файловая система, называемая *файловой системой IOS компании Cisco* (Cisco IOS File System — IFS). В ней, например, в команде *copy* рекомендуется использовать для обращения к файлу стартовой конфигурации не параметр “*startup-config*”, а формат “*nvrwam:startup-config*”. В табл. 8.8 перечислены альтернативные названия для двух конфигурационных файлов.

Таблица 8.8. Названия файлов стартовой и текущей конфигурации в файловой системе IFS

Общепринятое название конфигурационного файла	Альтернативное название
<i>startup-config</i>	<i>nvrwam:</i> <i>nvrwam:startup-config</i>
<i>running-config</i>	<i>system:running-config</i>

Диалог начального конфигурирования

В операционной системе Cisco IOS есть два основных метода создания начальной конфигурации устройства: через режим конфигурирования, который был подробно описан выше, и с использованием *диалога начальной настройки* (*setup mode*). Диалог начальной настройки в интерактивной форме запрашивает у системного администратора базовые параметры устройства. Поскольку для большинства настроек требуется именно режим конфигурации устройства, большинство сетевых инженеров диалогом начальной настройки не пользуются. Тем не менее начинающим системным администраторам зачастую нравится использовать такой простой диалог, по крайней мере, до тех пор, пока они не наберутся опыта работы с интерфейсом командной строки устройств компании Cisco.

На рис. 8.10 и в примере 8.3 проиллюстрирован диалог начального конфигурирования коммутатора. Этот диалог чаще всего используется после загрузки операционной системы устройства, когда в памяти NVRAM нет конфигурации. Перейти к диалогу начального конфигурирования можно, введя команду *setup* в режиме привилегированного пользователя.

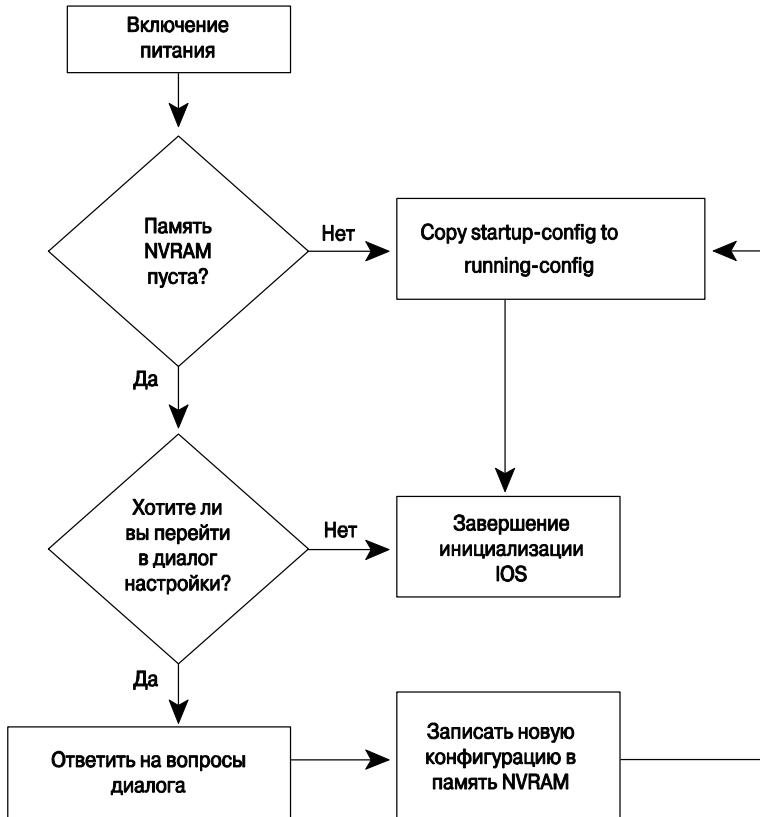


Рис. 8.10. Переход к диалогу начального конфигурирования устройства

Пример 8.3. Пример диалога начального конфигурирования устройства

--- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no] : yes

At any point you may enter a question mark '?' for help.
 Use ctrl-c to abort configuration dialog at any prompt.
 Default settings are in square brackets '[]'.

Basic management setup configures only enough connectivity
 for management of the system, extended setup will ask you
 to configure each interface on the system

Would you like to enter basic management setup? [yes/no] : yes
 Configuring global parameters:

Enter host name [Switch] : fred

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.

Enter enable secret: cisco

The enable password is used when you do not specify an enable secret password, with some older software versions, and some boot images.

Enter enable password: **notcisco**

The virtual terminal password is used to protect access to the switch over a network interface.

Enter virtual terminal password: **wilma**

Configure SNMP Network Management? [no] :

Current interface summary

Any interface listed with OK? value "NO" does not have a valid configuration

Interface	IP-Address	OK?	Method	Status	Protocol
Vlan1	unassigned	NO	unset	up	up
FastEthernet0/1	unassigned	YES	unset	up	up
FastEthernet0/2	unassigned	YES	unset	up	up
FastEthernet0/3	unassigned	YES	unset	up	up
!					
! Часть строк опущена					
!					
GigabitEthernet0/1	unassigned	YES	unset	down	down
GigabitEthernet0/2	unassigned	YES	unset	down	down

The following configuration command script was created:

```
hostname fred
enable secret 5 $1$wNE7$4JSktD3uN1Af5FpctmPz11
enable password notcisco
line vty 0 15
password wilma
no snmp-server
!
!
interface Vlan1
shutdown
no ip address
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
! Часть похожих строк опущена
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
end
```

```
[0] Go to the IOS command prompt without saving this config.  
[1] Return back to the setup without saving this config.  
[2] Save this configuration to nvram and exit.
```

Enter your selection [2]: 2

Building configuration...

[OK]

Use the enabled mode 'configure' command to modify this configuration.
Press RETURN to get started!

Диалог начального конфигурирования, показанный выше, выглядит одинаково, независимо от того, была ли использована команда `setup` привилегированного режима, или устройство загрузилось с пустой памятью NVRAM. Когда диалог запускается, сетевому инженеру или администратору прежде всего нужно ответить на вопрос, хочет ли он использовать диалог начального конфигурирования. Чтобы продолжить работу с диалогом, следует нажать клавишу `<y>` или ввести слово “`yes`”. После этого в диалоге будут задаваться вопросы, отвечая на которые можно создать простую базовую конфигурацию устройства. После того как все ответы даны, т.е. все нужные параметры настроены, пользователь может выбрать, как поступить с полученной конфигурацией. Чтобы выбрать действие, нужно нажать одну из перечисленных ниже цифр.

- 0 — не сохранять конфигурацию и перейти в интерфейс командной строки.
- 1 — не сохранять конфигурацию и перезапустить диалог начальной настройки коммутатора.
- 2 — сохранить конфигурацию как стартовую и текущую и перейти в интерфейс командной строки.

Можно прервать диалог начальной настройки в любой момент времени и перейти в интерфейс командной строки с помощью комбинации клавиш `<Ctrl+c>`. Обратите внимание: в третьем варианте действия (цифра 2) в конце диалога конфигурация записывается и в стартовый, и в текущий конфигурационный файл; в свою очередь, при сохранении результата работы в режиме конфигурирования устройства информация заносится только в текущую конфигурацию.

Повторите все ключевые темы

Повторите все ключевые темы данной главы, помеченные пиктограммой “Ключевая тема”. Ключевые темы и соответствующие им страницы перечислены в табл. 8.9.

Таблица 8.9. Ключевые темы главы 8

Элемент	Описание	Страница
Список	Стандартные настройки консольного порта коммутатора компании Cisco	229
Табл. 8.6	Конфигурационные режимы коммутатора	239
Рис. 8.8	Различные типы памяти коммутатора Cisco	241
Табл. 8.7	Названия и предназначение двух основных конфигурационных файлов операционной системы Cisco IOS	241

Заполните таблицы и списки по памяти

Распечатайте приложение М (Appendix L) с компакт-диска или его раздел, относящийся к этой главе, и заполните таблицы и списки по памяти. В приложении Н (Appendix M) приведены заполненные таблицы и списки для самоконтроля.

Ключевые термины

Дайте определения перечисленных ниже терминов и проверьте правильность их написания в списке терминов:

интерфейс командной строки (Command-Line Interface — CLI), протокол SSH (Secure Shell — SSH), привилегированный режим (enable mode), пользовательский режим (user mode), режим конфигурирования (configuration mode), файл стартовой конфигурационный (startup-config file), файл текущей конфигурации (running-config file), диалог начальной настройки (setup mode).

Список команд

В табл. 8.10 приведен список команд этой главы, а также даны их краткие описания.

Таблица 8.10. Список команд главы 8

Команда	Режим и назначение
line console 0	Переключает контекст командной строки в режим конфигурирования консольной линии
line vty 1-я_vty_линия последняя_vty_линия	Переключает контекст в режим конфигурирования линий vty для указанного в команде диапазона
login	Режим конфигурирования консольной или линии vty. Указывает операционной системе IOS, что нужно выдавать приглашение для ввода пароля
password пароль	Режим конфигурирования консольной линии или линии vty. Задает пароль, который будет запрашиваться при подключении к устройству
interface тип номер_порта	Переключает контекст командной строки в режим конфигурирования интерфейса. В параметре типа интерфейса обычно указывают значение FastEthernet или GigabitEthernet (для коммутаторов). Возможные номера портов зависят от модели коммутатора и выглядят, например, так: 0/1, 0/2 и т.п.
shutdown no shutdown	Режим конфигурирования интерфейса. Первая команда административно выключает интерфейс, вторая, соответственно, включает
hostname имя	Режим глобальной конфигурации. Задает имя узла для коммутатора, которое также используется в приглашении командной строки
enable secret пароль	Режим глобальной конфигурации. Задает пароль привилегированного режима, который хранится в конфигурации в зашифрованном виде
enable password пароль	Режим глобальной конфигурации. Задает пароль привилегированного режима, который хранится в конфигурации в виде открытого текста

Окончание табл. 8.10

Команда	Режим и назначение
Exit	Переводит интерфейс командной строки на один подрежим выше в режиме конфигурирования чего-либо
End	Переводит интерфейс командной строки из любого подрежима конфигурирования в режим привилегированного пользователя
<Ctrl+Z>	Эта комбинация клавиш делает то же самое, что и команда end
no debug all	Команды привилегированного уровня, отключающие все активные отладки в устройстве
undebug all	
show process	Команда непривилегированного уровня, которая показывает статистику загрузки процессора устройства
terminal monitor	Указывает операционной системе Cisco IOS, что нужно копии всех системных сообщений, в том числе и отладочных, пересыпать в сеанс Telnet или SSH пользователя
reload	Режим привилегированного пользователя. Команда вызывает перезагрузку коммутатора или маршрутизатора
copy откуда куда	Режим привилегированного пользователя. Команда копирует файл из одного местоположения в другое. В качестве источника и получателя файла могут использоваться текущая и стартовая конфигурация, сервер TFTP и RPC, флеш-накопитель
copy running-config startup-config	Режим привилегированного пользователя. Команда сохраняет активную текущую конфигурацию в стартовой, перезаписывая соответствующий файл. Стартовая конфигурация используется при загрузке устройства
copy startup-config running-config	Режим привилегированного пользователя. Команда объединяет файл стартовой конфигурации и текущей (в оперативной памяти)
show running-config	Показывает файл текущей конфигурации устройства
write erase	Все указанные команды в привилегированном режиме позволяют полностью удалить стартовую конфигурацию
erase startup-config	
erase nvram:	
setup	Режим привилегированного пользователя. Команда запускает интерактивный диалог начальной настройки коммутатора (или маршрутизатора)
quit	Команда непривилегированного режима. Разрывает сеанс с интерфейсом командной строки
show system:running-config	Аналог команды show running-config
show startup-config	Показывает файл стартовой конфигурации устройства
show nvram:startup-config	Аналоги команды show startup-config
show nvram:	
enable	Переводит из режима обычного пользователя в привилегированный и запрашивает пароль, если он задан
disable	Переводит из привилегированного режима пользователя в обычный
configure terminal	Команда режима привилегированного пользователя. Переводит в режим конфигурирования устройства

В этой главе...

- **Настройка функций, общих для коммутаторов и маршрутизаторов.** Описано, как настроить функции коммутаторов, которые совпадают с функциями маршрутизаторов.
- **Настройка коммутаторов локальных сетей и управление ими.** Описано конфигурирование уникальных функций коммутаторов, которые присущи только им. У маршрутизаторов могут быть некоторые аналогичные функции, но они настраиваются совсем по-другому.

ГЛАВА 9

Настройка коммутаторов Ethernet

В главах 3 и 7 были подробно описаны концепции локальных сетей Ethernet. Вы узнали, как работает технология Ethernet, как работают коммутаторы, как строится кабельная система сети и как коммутаторы пересылают фреймы Ethernet на основании MAC-адреса получателя.

Коммутаторы локальных сетей компании Cisco выполняют свои основные функции без какой-либо конфигурации. Можно просто купить такой коммутатор, подключить кабелями правильного типа различные сетевые устройства к его портам, включить питание, и коммутатор заработает. Тем не менее во многих сетях инженерам нужно будет настроить разнообразные дополнительные функции коммутатора или искать и устранять неисправности в уже работающей сети. В этой главе подробно описано, как конфигурируются различные функции коммутаторов, а в главе 10 описаны методики поиска и устранения неисправностей в коммутаторах компании Cisco.

Контрольные вопросы: знаете ли вы уже темы главы

Этот раздел предназначен для того, чтобы читатель мог предварительно оценить свои знания и решить, нужно ли ему читать главу целиком. Если ответы на девять из десяти вопросов даны правильно, можно сразу же перейти к последнему разделу “Подготовка к экзамену”. Основные темы этой главы и предварительных контрольных вопросов перечислены в табл. 9.1. Отвечая на контрольные вопросы и используя таблицу, читатель сможет достаточно точно определить свои знания в той или иной области. Ответы на вопросы приведены в приложении А “Ответы на контрольные вопросы”.

Таблица 9.1. Темы контрольных вопросов

Основная тема	Номера вопросов
Настройка функций, общих для коммутаторов и маршрутизаторов	1–3
Настройка коммутаторов локальных сетей и управление ими	4–8

- Предположим, коммутатору с консоли были отданы команды `enable secret` и `enable password`. Вам необходимо отключиться от коммутатора и опять подключиться к нему через консоль. Пароль какой из заданных команд нужно будет ввести?
 - `enable password`.
 - `enable secret`.
 - пароля не будет.
 - пароль команды `password`, если она была введена.

2. Сетевой инженер настроил коммутатор Cisco 2960 таким образом, что к нему разрешен доступ Telnet с паролем `mypassword`. Позже инженер изменил конфигурацию так, чтобы доступ был возможен по защищенному соединению SSH. Какие из указанных ниже команд вошли в новую конфигурацию?
- а) `username имя password` пароль в режиме конфигурирования виртуальных терминалов (vty).
 - б) `username имя password` пароль в режиме глобальной конфигурации устройства.
 - в) `transport input ssh` в режиме конфигурирования виртуальных терминалов (vty).
 - г) `transport input ssh` в режиме глобальной конфигурации устройства.
3. Следующая команда была скопирована из буфера в командную строку режима конфигурирования коммутатора компании Cisco в сеансе Telnet `banner login this is the login banner`. Что из перечисленного ниже правильно описывает, как будет выглядеть экран при последующем доступе к консоли устройства?
- а) Текст сообщения отображаться не будет.
 - б) Текст сообщения будет состоять из фразы “`his is`”.
 - в) Текст сообщения будет состоять из фразы “`this is the login banner`”.
 - г) Текст сообщения будет состоять из фразы “`Login banner configured. no text defined`” (сообщения настроены, но текст не задан).
4. Какое действие не является обязательным при настройке защиты порта (port security) без автоматического обнаружения MAC-адресов (sticky learning)?
- а) Указать максимально разрешенное количество MAC-адресов для интерфейса с помощью команды `switchport port-security maximum` в режиме конфигурирования интерфейса.
 - б) Включить режим безопасности порта с помощью команды конфигурирования интерфейса `switchport port-security`.
 - в) Указать разрешенные MAC-адреса с помощью команды `switchport port-security mac-address` в режиме конфигурирования интерфейса.
 - г) Все указанные выше команды являются обязательными.
5. Персональный компьютер сетевого инженера подключен к коммутатору в главном офисе. К маршрутизатору главного офиса все филиалы подключены через последовательные интерфейсы, в каждом филиале есть малый маршрутизатор и коммутатор. Какие команды и в каком режиме конфигурации должны быть введены в устройства, чтобы инженер мог установить сеансы Telnet с коммутаторами всех филиалов?
- а) Нужно ввести команду `ip address` в режиме конфигурирования сети VLAN1.
 - б) Нужно ввести команду `ip address` в режиме глобальной конфигурации устройства.

в) Нужно ввести команду `ip default-gateway` в режиме конфигурирования сети VLAN1.

г) Нужно ввести команду `ip default-gateway` в режиме глобальной конфигурации устройства.

д) Нужно ввести команду `password` в режиме конфигурирования консольной линии.

е) Нужно ввести команду `password` в режиме конфигурирования виртуальных терминалов (vty).

6. Какая из приведенных ниже команд отключает согласование скорости согласно стандарту IEEE для порта 10/100 коммутатора Cisco?

а) `negotiate disable` в режиме конфигурирования интерфейса.

б) `no negotiate` в режиме конфигурирования интерфейса.

в) `speed 100` в режиме конфигурирования интерфейса.

г) `duplex half` в режиме конфигурирования интерфейса.

д) `duplex full` в режиме конфигурирования интерфейса.

е) `speed 100` и `duplex full` в режиме конфигурирования интерфейса.

7. В каком режиме командной строки (CLI) можно задать настройки дуплексного режима для интерфейса `fastethernet 0/5`?

а) В пользовательском режиме.

б) В привилегированном режиме.

в) В режиме глобальной конфигурации.

г) В режиме начальной настройки устройства (`setup`).

д) В режиме конфигурирования интерфейса.

8. Команда `show vlan brief` дает следующий результат:

```
2 my-vlan          active   Fa0/13, Fa0/15
```

Какая из указанных ниже команд могла быть использована для конфигурирования коммутатора в таком случае?

а) Команда `vlan 2` в режиме глобальной конфигурации устройства.

б) Команда `name MY-VLAN` в режиме конфигурирования сети VLAN.

в) Команда `interface range Fa0/13 - 15` в режиме глобальной конфигурации.

г) Команда `switchport vlan 2` в режиме конфигурирования интерфейса.

Основные темы

В большинстве коммутаторов Catalyst компании Cisco используется единый *интерфейс командной строки* (Command-Line Interface — CLI), который аналогичен применяемому в маршрутизаторах. Такой интерфейс выглядит и работает в обоих типах устройств одинаково, а кроме того, он поддерживает практически те же конфигурационные команды и команды группы `show`. Как было описано в главе 8, часть команд и процессов, которые можно встретить в коммутаторах компании Cisco, работают абсолютно аналогично в маршрутизаторах этой же компании.

В этой главе объяснены многие из стандартно конфигурируемых функций коммутаторов компании Cisco. Некоторые из тем очень важны, как, например, задание имен пользователей и паролей, позволяющих обеспечить безопасный доступ к коммутатору. Другие функции не очень важны, но полезны, как, например, назначение текстовых описаний интерфейсам устройства, которые упростят и сделают документацию и конфигурационные файлы удобнее. Эта глава содержит практически все темы, связанные с конфигурированием коммутаторов, за исключением команд конфигурирования *протокола обнаружения устройств Cisco* (Cisco Discovery Protocol — CDP), который подробно описан в главе 10.

Настройка функций, общих для коммутаторов и маршрутизаторов

В первом из двух разделов этой главы подробно описано конфигурирование функций, которые одинаково работают и настраиваются как в коммутаторах, так и в маршрутизаторах. В частности, будут подробно рассмотрены настройки для обеспечения безопасного доступа к интерфейсу командной строки, а также настройка различных параметров консольного подключения к устройству.

Безопасный доступ к командной строке коммутатора

Чтобы воспользоваться режимом привилегированного пользователя (enable) коммутатора, администратор должен сначала получить доступ к командной строке с правами обычного пользователя через консольное соединение, сеанс Telnet или SSH, а после ввести команду `enable`. Со стандартными настройками устройства пользователь, подключенный к консоли, не должен вводить имя или пароль, чтобы работать с обычным или привилегированным режимом. Причина такого подхода к безопасности заключается в том, что любой специалист, имеющий физический доступ к консоли коммутатора или маршрутизатора, может сбросить все пароли менее чем за 5 минут с помощью процедур восстановления пароля, которые компания Cisco публикует в открытых источниках. Итак, маршрутизаторы и коммутаторы компании Cisco разрешают пользователям, подключенным к консоли, обычный и привилегированный доступ к интерфейсу командной строки.

ВНИМАНИЕ!

Чтобы найти процедуры восстановления или сброса паролей, обратитесь к веб-сайту Cisco.com и выполните поиск по фразе “password recovery” (восстановление пароля).

Первый же результат на странице поиска, вполне вероятно, будет относиться к странице, где есть процедуры восстановления паролей практически для всех устройств компании Cisco.

Чтобы попасть в режим привилегированного пользователя через виртуальный терминал vty (сеанс Telnet или SSH), в коммутаторе должны быть заданы как минимум следующие настройки:

- IP-адрес устройства;
- процедура аутентификации пользователя для линий vty;
- пароль привилегированного режима (enable).

Большинство сетевых инженеров обычно хотят иметь дистанционный доступ к коммутаторам с помощью сеансов Telnet или SSH, поэтому имеет смысл настроить устройства с использованием безопасного доступа. Несмотря на то что кто-либо, имеющий физический доступ к устройству, может достаточно легко использовать процедуры восстановления паролей и получить полный контроль над коммутатором, имеет смысл также настроить функции безопасности и для консоли¹.

В этом разделе рассмотрено конфигурирование доступа к привилегированному режиму (enable) коммутатора или маршрутизатора. Одна ключевая тема — настройка IP-адреса — подробно рассмотрена ниже в этой же главе, в разделе “Конфигурирование IP-адреса коммутатора”. В частности, ниже подробно рассмотрены следующие темы:

- настройка аутентификации по паролю для консольных сеансов и сеансов Telnet;
- настройка безопасного протокола SSH;
- настройка шифрования паролей;
- настройка паролей режима привилегированного пользователя.

Настройка аутентификации по паролю

Инженер может получить доступ к командной строке коммутатора или маршрутизатора компании Cisco через консольное подключение, а также сеанс Telnet или SSH. Обычно коммутаторы и маршрутизаторы сразу же пускают в режим пользователя без аутентификации, а пользователям Telnet запрещен доступ, поскольку в стандартной конфигурации пароль на линиях vty не установлен. Вне зависимости от стандартных настроек рекомендуется защитить паролями все варианты подключения обычного пользователя командной строки: для консоли, сеансов Telnet и SSH.

Пользователь в непrivилегированном режиме может получить дополнительные права, используя команду enable, но результат ее ввода будет зависеть от того, как именно он подключен, через консольное соединение или дистанционно. Стандартно, если пароль не задан, команда enable переводит пользователя в привилегированный режим без какого-либо пароля в консольном подключении, а пользователям, пытающимся подключиться через сеанс Telnet, в доступе будет отказано, причем мгновенно, и пароль запрашиваться не будет. Независимо от того, какие стандартные настройки характерны для устройства, для повышения уровня безопасности сетевого оборудования рекомендуется задавать пароль для привилегированного режима с помощью команды enable secret в режиме глобальной конфигурации.

¹ В действительности все устройства должны быть размещены в телекоммуникационных узлах или помещены в специальные шкафчики с замком, если они находятся в публичных местах, ограничение физического доступа к устройству значительно улучшит систему безопасности. — Примеч. ред.

ВНИМАНИЕ!

Ниже, в разделе “Два варианта паролей привилегированного режима”, подробно описаны два варианта конфигурирования паролей привилегированного режима с помощью команд enable, enable secret и enable password, а также объяснено, почему первый вариант является наиболее предпочтительным.

В примере 9.1 показан процесс конфигурирования пароля для консольного (console) подключения, пароля для линий vty (сеансов Telnet), шифрованного пароля привилегированного пользователя (enable) и настройки имени хоста (hostname) для коммутатора. В примере показан процесс целиком, в том числе и внешний вид приглашения командной строки, которое было подробно описано в главе 8.

Ключевая тема Пример 9.1. Конфигурирование основных паролей и названия устройства

```
Switch>enable
Switch#configure terminal
Switch(config)#enable secret cisco
Switch(config)#hostname Emma
Emma(config)#line console 0
Emma(config-line)#password faith
Emma(config-line)#login
Emma(config-line)#exit
Emma(config)#line vty 0 15
Emma(config-line)#password love
Emma(config-line)#login
Emma(config-line)#exit
Emma(config)#exit
Emma#
! Указанная ниже команда показывает текущую конфигурацию
! коммутатора (running-config)
Emma#show running-config
!
Building configuration...
Current configuration : 1333 bytes
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
!
hostname Emma
!
enable secret 5 $1$YXRN$11zOe1Lb0Lv/nHyTquobd.
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
! Некоторые строки конфигурации были опущены, в частности,
! настройки интерфейсов FastEthernet с 0/3 по 0/23.
```

```
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
no ip address
no ip route-cache
!
ip http server
ip http secure-server
!
control-plane
!
!
line con 0
password faith
login
line vty 0 4
password love
login
line vty 5 15
password love
login
```

В примере 9.1 пользователь сначала переходит в привилегированный режим, потом в режим глобальных настроек устройства с помощью команды `configure terminal`. В этом режиме он вводит две команды глобальной конфигурации (`enable secret` и `hostname`), которые так называют потому, что они задают параметры, относящиеся к устройству в целом, т.е. глобальные параметры.

Например, команда `hostname` просто задает единное название для устройства (обратите внимание, как меняется приглашение интерфейса командной строки после этой команды). Команда `enable secret` задает единственный пароль, позволяющий получить доступ к привилегированному режиму, опять же это команда глобального уровня. Для сравнения: команда `login` (которая инструктирует коммутатор о том, что нужно запрашивать текстовый пароль без имени) и команда `password` (в которой указан требуемый пароль) вводятся как в подрежиме конфигурирования параметров консольного подключения, так и в режиме конфигурирования линий виртуальных терминалов (vty). Таким образом, эти команды являются подкомандами двух режимов конфигурирования. С их помощью можно задать разные пароли, один — для консольного подключения, второй — для виртуальных терминалов (vty), в соответствующем подрежиме конфигурирования, как было показано в примере выше.

Нажав комбинацию клавиш `<Ctrl+z>` в любой момент (в режиме конфигурирования), пользователь мгновенно возвращается в режим привилегированного пользователя. Тем не менее в данном примере показано несколько последовательных команд `exit`, которые переводят пользователя из определенного подрежима в режим глобальной конфигурации устройства, а потом и в режим привилегированного пользователя. Команда `end`, вводимая в любом из режимов или подрежимов конфигурирования устройства, выполняет точно то же действие, что и комбинация клавиш

<Ctrl+z>, — она из любого режима переводит пользователя просто в привилегированный режим².

Во второй половине примера 9.1 показан результат выполнения команды `show running-config`. Эта команда показывает текущую конфигурацию коммутатора, в том числе и изменения, которые были внесены в первой половине примера. Выделенные строки являются результатом команд, которые показаны в первой половине примера.

ВНИМАНИЕ!

Конфигурация, полученная в результате выполнения команды `show running-config`, содержит пять линий vty (с 0 по 4) и отдельно еще несколько линий (с 5 по 15). В старых версиях операционной системы Cisco IOS поддерживалось только пять линий vty, они имели номера с 0 по 4, следовательно, только пять соединений Telnet можно было установить с таким устройством. Позже компания Cisco добавила поддержку дополнительных линий, с 5 по 15. В современных устройствах таким образом разрешено 16 параллельных сеансов Telnet к устройству. Диапазоны линий указаны раздельно для совместимости конфигурационных файлов со старыми версиями операционных систем.

Конфигурирование имен пользователей и протокола SSH

Программа и протокол Telnet пересыпает все данные, в том числе и пароль пользователя, в виде открытого текста. Протокол безопасного соединения SSH и соответствующие ему приложения выполняют те же функции, что и Telnet, — эмулируют окно терминального сеанса и позволяют пользователю подключиться к интерфейсу командной строки (CLI) дистанционного устройства. Кроме того, в протоколе SSH шифруются все данные, пересылаемые между клиентом и сервером, поэтому этот протокол является самым предпочтительным на сегодня инструментом дистанционной работы с маршрутизаторами и коммутаторами.

Чтобы обеспечить поддержку протокола SSH в маршрутизаторе или коммутаторе компании Cisco, нужно ввести несколько дополнительных команд. Так, например, протокол SSH требует, чтобы пользователь всегда вводил имя и пароль, а не только пароль, как служба Telnet, поэтому в устройстве должна быть настроена как минимум одна пара соответствующих значений. Пара значений, состоящая из имени и пароля пользователя, может быть получена двумя методами: имя и пароль могут быть настроены непосредственно на коммутаторе, оба значения могут быть получены от дистанционного сервера, называемого сервером *автентификации, авторизации и учета* (Authentication, Authorization and Accounting — AAA). В этой книге рассматривается только метод с использованием локальных значений имени и пароля пользователя. На рис. 9.1 приведена диаграмма, иллюстрирующая процесс конфигурирования сервера протокола SSH в устройстве компании Cisco.

² Команда `exit` выводит на один уровень выше из какого-либо режима, команда `end` и комбинация клавиш <Ctrl+z> выводят из всех режимов в привилегированный режим. — Примеч. ред.

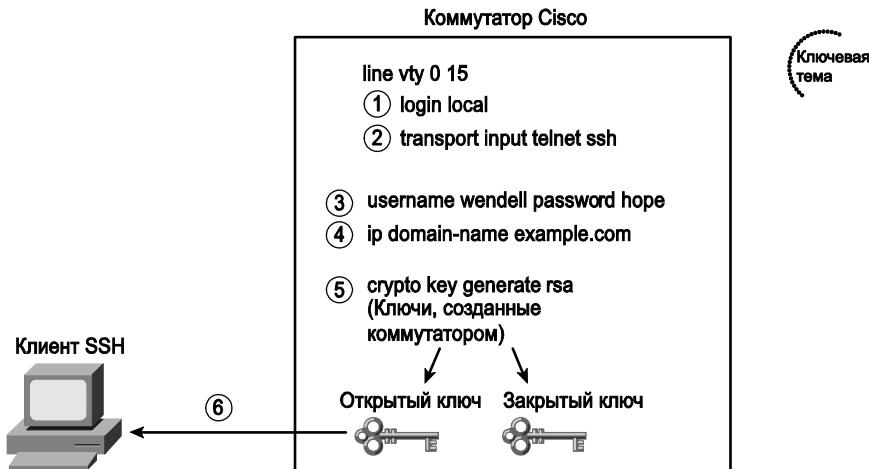


Рис. 9.1. Процесс конфигурирования протокола SSH

Этапы конфигурирования, представленные на рис. 9.1, подробно описаны ниже.

Процесс конфигурирования протокола SSH

- Этап 1** Следует изменить конфигурацию так, чтобы при подключении по линиям vty нужно было вводить имя пользователя, настроенное локально или полученное от сервера AAA. В данном случае (см. рис. 9.1) команда `login local` указывает на использование локально заданных имен. Эта команда заменяет подкоманду `login` для сеансов vty.
- Этап 2** Также необходимо указать коммутатору, что он должен принимать сеансы как Telnet, так и SSH с помощью команды `transport input telnet ssh` в подрежиме конфигурирования линий vty (стандартная настройка использует команду в виде `transport input telnet` без указания параметра `ssh`).
- Этап 3** Нужно настроить несколько пар имен и паролей в режиме глобальной конфигурации с помощью команды `username имя password пароль`.
- Этап 4** Далее требуется указать доменное имя устройства (имя DNS) с помощью команды `ip domain-name имя` в режиме глобальной конфигурации.
- Этап 5** На этом этапе нужно использовать команду, создающую пару открытого (public) и закрытого (private) ключей, а также общий ключ (shared) с помощью команды `crypto key generate rsa` в режиме глобальной конфигурации.
- Этап 6** Хотя никаких дополнительных настроек для коммутатора на этом этапе вводить не нужно, каждый клиент SSH должен скопировать открытый ключ коммутатора себе в кеш, прежде чем он сможет установить соединение с устройством.

ВНИМАНИЕ!

В описанной выше конфигурации указано несколько этапов, которые достаточно специфичны и относятся к технологии, выходящей за рамки рассмотрения данной книги, например настройки протокола SSH. И хотя запоминать такие этапы для соответствующего экзамена не нужно, они могут быть полезны при изучении методов конфигурирования устройств — в частности, они пригодятся на практике при конфигурировании какой-либо функции целиком.

В примере 9.2 показано использование команд, перечисленных на рис. 9.1.

Пример 9.2. Процесс конфигурирования протокола SSH

```

Emma#
Emma#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Emma(config)#line vty 0 15
! Ниже вводится команда этапа 1
Emma(config-line)#login local
! Команды этапа 2
Emma(config-line)#transport input telnet ssh
Emma(config-line)#exit
! Команда этапа 3
Emma(config)#username wendell password hope
! Команда этапа 4
Emma(config)#ip domain-name example.com
! Команда этапа 5
Emma(config)#crypto key generate rsa
The name for the keys will be: Emma.example.com
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys ...[OK]

00:03:58: %SSH-5-ENABLED: SSH 1.99 has been enabled
Emma(config)#^Z
! Ниже показано содержимое открытого ключа, именно он будет передан
! клиентам SSH
!
Emma#show crypto key mypubkey rsa
% Key pair was generated at: 00:03:58 UTC Mar 1 1993
Key name: Emma.example.com
Usage: General Purpose Key
Key is not exportable.
Key Data:
30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 00DB43DC
49C258FA 8E0B8EB2 0A6C8888 A00D29CE EAEE615B 456B68FD 491A9B63 B39A4334
86F64E02 1B320256 01941831 7B7304A2 720A57DA FBB3E75A 94517901 7764C332
A3A482B1 DB4F154E A84773B5 5337CE8C B1F5E832 8213EE6B 73B77006 BA8782DE
180966D9 9A6476D7 C9164ECE 1DC752BB 955F5BDE F82BFBCB2 A273C58C 8B020301
0001
% Key pair was generated at: 00:04:01 UTC Mar 1 1993
Key name: Emma.example.com.server
Usage: Encryption Key
Key is not exportable.

Key Data:
307C300D 06092A86 4886F70D 01010105 00036B00 30680261 00AC339C D4916728
6ACB627E A5EE26A5 00946AF9 E63FF322 A2DB4994 9E37BFDA AB1C503E AAF69FB3
2A22A5F3 0AA94454 B8242D72 A8582E7B 0642CF2B C06E0710 B0A06048 D90CBE9E
F0B88179 EC1C5EAC D551109D 69E39160 86C50122 9A37E954 85020301 0001

```

В приведенном выше примере выделенные строки отмечают комментарии к используемым командам. Обратите также внимание на то, что созданный коммутато-

ром открытый ключ для шифрованного сеанса также выделен в выводимой командой `show crypto key mypubkey rsa` информации. Каждому клиенту SSH потребуется копия такого ключа, чтобы установить соединение, поэтому клиент автоматически запрашивает ключ у устройства, загружает его в начале сеанса и в большинстве программ переспрашивает в диалоговом окне у пользователя, принимать ключ или нет.

Для наивысшего уровня безопасности может понадобиться полностью отключить доступ Telnet. Сделать это можно с помощью команды `transport input ssh` подрежима конфигурирования линий vty. Если в такой команде указать только параметр `ssh`, то коммутатор будет отбрасывать соединения Telnet.

Шифрование паролей

Несколько конфигурационных команд устройств компании Cisco используются для указания различных паролей; обычно такие пароли хранятся в конфигурации в виде открытого текста. В частности, если для линий vty использовать обычную аутентификацию по паролю, которая задается командой `password`, а также если задать имена пользователей командой `username`, то можно обнаружить, что такие пароли не шифруются. Исключением является команда `enable secret`, которая сохраняет пароль в шифрованном виде.

Чтобы повысить уровень безопасности и устраниТЬ уязвимости в сети, в частности, если используется печатная копия конфигураций или резервная копия хранится где-либо на сервере, можно зашифровать, или “закодировать”, пароли с помощью команды `service password-encryption` режима глобальной конфигурации устройства. В зависимости от того, есть такая команда в конфигурации или нет, пароли будут зашифрованы указанным ниже образом.

- Если команда `service password-encryption` введена в режиме глобальной конфигурации устройства, то все существующие пароли — для консоли, для линий vty, параметры команды `username` — будут тотчас же зашифрованы.
- Если команда `service password-encryption` была введена ранее, например, есть в резервной загрузочной конфигурации, то все новые пароли, которые добавляет пользователь, будут сразу же шифроваться.
- Если пароли были зашифрованы указанной выше командой, а после была введена команда `no service password-encryption`, то пароли будут храниться в зашифрованном виде до тех пор, пока они не будут сменены кем-либо.

В примере 9.3 проиллюстрировано описанное выше поведение конфигурации устройства.

ВНИМАНИЕ!

Показанная в примере 9.3 команда `show running-config | begin line vty` выдает текущую конфигурацию устройства, начиная с той строки, в которой встречается текст `line vty`. Это просто удобный метод отображения нужной части конфигурационного файла.

Пример 9.3. Шифрование паролей с помощью команды `service password-encryption`

```
Switch3#show running-config | begin line vty  
line vty 0 4
```

```

password cisco
login
Switch3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch3(config)#service password-encryption
Switch3(config)#^Z
Switch3#show running-config | begin line vty
line vty 0 4
password 7 070C285F4D06
login
end
Switch3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch3(config)#no service password-encryption
Switch3(config)#^Z
Switch3#show running-config | begin line vty
line vty 0 4
password 7 070C285F4D06
login
end
Switch3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch3(config)#line vty 0 4
Switch3(config-line)#password cisco
Switch3(config-line)#^Z
Switch3#show running-config | begin line vty
line vty 0 4
password cisco
login

```

ВНИМАНИЕ!

Команда `service password-encryption` включает алгоритм шифрования с номером 7, как видно из команды `password` в приведенном выше примере. Это один из нескольких возможных алгоритмов шифрования в операционной системе Cisco. Шифрование номер 7 используется исключительно командой `service password-encryption`, является слабым алгоритмом шифрования и его очень легко расшифровать.

Два варианта паролей привилегированного режима

Команда `enable` переводит пользователя из обычного режима (в котором строка приглашения выглядит так: `название_устройства>`) в привилегированный режим (строка приглашения имеет вид `название_устройства#`). Режим привилегированного пользователя в маршрутизаторах и коммутаторах может быть защищен паролем согласно одному из указанных ниже правил.



Ключевые отличия команд `enable secret` и `enable password`

- Команда режима глобальной конфигурации устройства `enable password` пароль применяется для конфигурирования пароля привилегированного режима `enable`. Стандартно такой пароль хранится в виде *открытого текста* в конфигурации.
- Команда режима глобальной конфигурации `enable secret` пароль также задает пароль привилегированного режима `enable`. Этот пароль хранится в виде *хеша MD5* в конфигурации, и узнать его действительное значение невозможно.

- Если при конфигурировании устройства были введены *обе команды*, то пароль, установленный командой `enable secret`, будет использоваться устройством, и именно его будет запрашивать маршрутизатор или коммутатор.

При использовании команды `enable secret` маршрутизатор или коммутатор автоматически шифрует (т.е. “прячет”) пароль. Несмотря на то что часто говорят, что пароль “зашифрован”, в действительности он не шифруется. Операционная система Cisco IOS применяет специализированную математическую функцию к символам пароля, называемую *сверткой сообщения №5*³ (Message Digest 5 — MD5), или просто хешем. Результат выполнения хеш-функции заносится в конфигурационный файл устройства. В операционной системе IOS этот метод обозначается цифрой 5 (пример 9.4). Следует отметить, что шифрование с помощью алгоритма MD5 является более безопасным методом хранения паролей, чем использование команды `service password-encryption`. В примере 9.4 показаны процесс установки пароля с помощью команды `enable secret`, формат команды и пароля, а также удаление пароля.

Пример 9.4. Установка шифрованного пароля `enable secret`

```
Switch3(config)#enable secret ?
 0      Specifies an UNENCRYPTED password will follow
 5      Specifies an ENCRYPTED secret will follow
 LINE   The UNENCRYPTED (cleartext) 'enable' secret
 level  Set exec level password

Switch3(config)#enable secret fred
Switch3(config)#^Z
Switch3#show running-config
! Вся конфигурация, кроме нужной строки, опущена !
enable secret 5 $1$ZGMA$e8cmvkz4UjiJhVp7.maLE1

Switch3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch3(config)#no enable secret
Switch3(config)#^Z
```

Когда задан пароль `enable secret` (что рекомендуется), а не `enable password`, он автоматически шифруется. В примере 9.4 вводится команда `enable secret fred`, которая устанавливает пароль `fred`. Тем не менее можно также ввести команду в виде `enable secret 0 fred`, — в данной конфигурации 0 свидетельствует о том, что далее идет нешифрованная строка. Операционная система IOS принимает команду, применяет алгоритм шифрования, который указан в команде `enable secret` (тип 5 в данном случае, т.е. хеш MD5), и сохраняет шифрованное или закодированное значение в текущей конфигурации устройства. После таких действий команда `show running-configuration` покажет результат с использованием шифрования номер 5 для пароля — длинную строку, которая выглядит как полная абракадабра.

К счастью, удалить пароль привилегированного доступа можно просто с помощью команды `no enable secret`, полное значение пароля вводить не требуется.

³ Сжатая текстовая строка, полученная из текста сообщения в результате применения односторонней хеш-функции (one-way hash function). — Примеч. ред.

В примере 9.4 как раз и продемонстрирована эта ситуация: в конце примера пароль удаляется. Возможно, пароль нужно будет удалить, но чаще его приходится заменять новым. Смена пароля осуществляется с помощью той же команды, но с новым паролем: `enable secret новый_пароль`.

Настройки консольного соединения и линий vty

В этом разделе описаны некоторые незначительные настройки, влияющие на поведение интерфейса командной строки (CLI), и соединения через консоль и/или сеансы vty (Telnet и SSH).

Сообщения, отображаемые при подключении

Маршрутизаторы и коммутаторы компании Cisco могут отображать несколько различных сообщений при подключении к ним, в зависимости от того, что задали системные администраторы. Отображаемое при подключении *сообщение* (banner) — это просто текст, который выводится на экран пользователя. Можно настроить маршрутизатор или коммутатор таким образом, что он будет показывать несколько сообщений, например, какой-то текст до аутентификации в системе, а какой-то после. В табл. 9.2 перечислены самые популярные сообщения и приведены примеры их типичного использования.

Таблица 9.2. Сообщения, отображаемые при подключении

Сообщение	Пример использования
Сообщение дня (Message of the Day — MOTD)	Отображается до того, как появится приглашение для аутентификации. Используется для некоторых временных сообщений, например, “Маршрутизатор будет выключен в полночь для технического осмотра” ⁴
Сообщение перед аутентификацией (login)	Это сообщение отображается до выполнения аутентификации, но после сообщения дня. Обычно используется для какого-либо постоянного сообщения, например: “Неавторизованный доступ к устройству запрещен”
Сообщение после аутентификации (exec)	Это сообщение отображается после успешной аутентификации пользователя. Обычно используется для вывода информации, которая должна быть скрыта от неавторизованных пользователей

Команда `banner` режима глобальной конфигурации применяется для настройки всех трех перечисленных выше типов сообщений. Формат команды универсален — в качестве первого параметра указывается тип сообщения; если же параметр не указан, операционная система стандартно использует его как сообщение MOTD. Текст сообщения может состоять из нескольких строк, для этого достаточно нажать клавишу `<Enter>` и продолжить ввод текста. Интерфейс строки обнаруживает, что ввод сообщения закончен, когда пользователь вводит тот же самый разделительный символ, который он вводил в начале текста.

В примере 9.5 показаны процесс конфигурирования трех сообщений, перечисленных в табл. 9.2, а также процесс подключения пользователя. Первое сообщение, сообщение дня (MOTD), в конфигурации приведено без ключевого слова `motd`, поскольку обычно, если не указаны параметры, операционная система привязывает

⁴ Как и все конфигурационные команды, описания интерфейсов, комментарии, такие сообщения можно писать только латиницей. — Примеч. ред.

текст к нему. В первых двух вариантах команды используется разделительный символ #. В третьем варианте команды используется символ Z, чтобы проиллюстрировать, что можно использовать разные символы, главное, чтобы начальный и конечный символы были одинаковыми. Кроме того, в последнем варианте команды banner вводится несколько строк текста.

Пример 9.5. Конфигурирование сообщений

! Ниже показан пример конфигурирования отображаемых при аутентификации сообщений.

! Обратите внимание, что любой символ можно использовать в качестве разделителя, главное, чтобы он не был частью вводимого текста.

SW1(config)#banner #

Enter TEXT message. End with the character '#'.
Switch down for maintenance at 11PM Today #

SW1(config)#banner login #

Enter TEXT message. End with the character '#'.
Unauthorized Access Prohibited!!!!

#

SW1(config)#banner exec Z

Enter TEXT message. End with the character 'Z'.
Company picnic at the park on Saturday

Don't tell outsiders!

Z

SW1(config)#^Z

! Ниже показано, что пользователь сначала отключается от устройства,
! потом подключается заново.

! Он видит сообщение дня, потом сообщение аутентификации, приглашение
! операционной системы и еще одно сообщение.
!
SW1#quit

SW1 con0 is now available

Press RETURN to get started.

Switch down for maintenance at 11PM Today
Unauthorized Access Prohibited!!!!

User Access Verification

Username: fred

Password:

Company picnic at the park on Saturday
don't tell outsiders!

SW1>

Буфер истории команд

Когда пользователь вводит несколько команд подряд в интерфейсе командной строки (CLI), несколько последних команд сохраняются в буфере истории команд. Как было сказано в главе 8, можно использовать клавишу <↑> или комбинацию клавиш <Ctrl+p>, чтобы переместиться вверх по истории команд и вызвать одну из предыдущих настроек. Эта функция значительно облегчает процесс ввода повторяющихся или подобных команд. В табл. 9.3 перечислены некоторые из наиболее полезных команд для работы с буфером истории команд.



Таблица 9.3. Команды буфера истории команд

Команда	Описание
show history	Отображает команды, находящиеся в буфере истории команд
history size x	Вводится в режиме конфигурирования консольного подключения или сеанса vty и задает количество команд (x), которое будет сохраняться в буфере истории команд, соответственно для консольного или сеанса vty
terminal history size x	Позволяет задавать размер буфера истории команд (x) только для текущего сеанса пользователя

Команды `logging synchronous` и `exec-timeout`

В консольную линию маршрутизатора или коммутатора стандартно выводятся все сообщения *системного журнала* (syslog), эту функцию в устройстве нельзя отключить. Предпосылкой такого подхода является то, что маршрутизатор или коммутатор должен сообщать о каких-то важных событиях и доставлять некоторую срочную информацию сетевому администратору, администратор же может случайно присутствовать у консоли устройства и заметить срочное сообщение. Обычно устройства компании Cisco выводят такие системные сообщения на консоль в любой момент времени, в том числе и в тот момент, когда сетевой администратор вводит какую-то команду или прямо посреди результата какой-либо команды `show`.

Чтобы упростить работу с консолью, пользователь может настроить коммутатор таким образом, чтобы он выводил системные сообщения в подходящие моменты времени, например, после того, как команда `show` отработала, или так, чтобы не разрывать вводимый текст команд в произвольном месте. Нужная настройка осуществляется с помощью команды `logging synchronous` в подрежиме конфигурирования линий.

Можно также сделать использование линий vty более удобным за счет установки различных тайм-аутов для консоли или vty. Обычно маршрутизатор или коммутатор автоматически отсоединяет пользователей от устройства, после чего они 5 минут не выполняют никаких действий (`idle`). Этот интервал одинаков для консольного подключения и для линий vty (т.е. сеансов Telnet и SSH). С помощью команды `exec-timeout` минуты секунды режима конфигурирования линий можно задать различные временные интервалы для разных линий. Если установить в такой команде тайм-аут, равный 0 минутам и 0 секундам, маршрутизатор или коммутатор не будет отключать пользователей от соответствующей линии никогда. В примере 9.6 показан синтаксис обеих команд.

Пример 9.6. Настройка тайм-аутов и поведения системных сообщений

```
line console 0
login
password cisco
exec-timeout 0 0
logging synchronous
```

Настройка коммутаторов локальных сетей и управление ими

Одна из наиболее удобных особенностей коммутаторов локальных сетей компании Cisco состоит в том, что они не требуют никакого начального конфигурирова-

ния. Коммутаторы на заводе настраиваются таким образом, что все интерфейсы включены (т.е. для них введена команда `no shutdown`), на них настроено автосогласование характеристик, т.е. интерфейсы могут работать на разных скоростях и с разными режимами дуплексности (в стандартной конфигурации для каждого порта указаны команды `duplex auto` и `speed auto`). Все, что требуется от сетевого инженера, — это подключить кабели Ethernet и включить шнур питания в настенную розетку. Устройство готово к работе — коммутатор начинает обнаруживать MAC-адреса, принимать решения об отправке или фильтрации фреймов и даже использовать протокол STP, который стандартно включен.

Во второй части данной главы продолжено описание конфигурации коммутаторов, в основном здесь рассматриваются функции, характерные именно для коммутаторов, но не для маршрутизаторов. Ниже подробно рассматриваются следующие вопросы:

- конфигурирование IP-адреса коммутатора;
- конфигурирование интерфейсов (в том числе установка дуплексности и скорости);
- конфигурирование технологии безопасности портов (port security);
- конфигурирование сетей VLAN;
- как сделать неиспользуемые интерфейсы безопасными.

Конфигурирование IP-адреса коммутатора

Для того чтобы обеспечить доступ к устройству с помощью протоколов (и программ) Telnet и SSH, а также разрешить другим протоколам IP взаимодействовать с устройством, например *простому протоколу управления сетью* (Simple Network Management Protocol — SNMP), или обеспечить работу инструментов с графическим интерфейсом для пользователя, например *диспетчер управления устройствами Cisco* (Cisco Device Manager — CDM), у коммутатора должен быть собственный IP-адрес. Такой адрес не нужен коммутатору для того, чтобы перенаправлять фреймы Ethernet между портами, он нужен только для того, чтобы иметь возможность с помощью различных средств управлять самим устройством, например, чтобы был возможен дистанционный доступ к нему.

Конфигурирование IP-адреса коммутатора очень похоже на настройку хоста с единственной сетевой картой Ethernet. В коммутаторе нужно настроить один IP-адрес и соответствующую ему маску. Устройству также нужно указать стандартный шлюз, или, другими словами, адрес некоторого ближайшего маршрутизатора. Точно так же как и в обычном компьютере, адрес устройства может быть статически задан в конфигурации (адрес, маска и шлюз) или получен от *протокола динамического конфигурирования хоста* (Dynamic Host Configuration Protocol — DHCP).

В коммутаторе под управлением операционной системы Cisco IOS IP-адрес и маска сети задаются на специальном виртуальном интерфейсе, называемом *интерфейсом сети VLAN 1*. Он играет ту же роль, что и интерфейс Ethernet персонального компьютера. В действительности виртуальный интерфейс сети VLAN 1 соединяет все порты устройства и само устройство со стандартной виртуальной локальной сетью, называемой, что вполне очевидно, сетью VLAN 1. Эта сеть всегда присутствует в устройстве, и ее нельзя удалить. Ниже перечислены этапы конфигурирования IP-адреса устройства.



Настройка IP-адреса и стандартного шлюза коммутатора

- Этап 1** Перейти в режим конфигурирования сети VLAN 1 с помощью команды `interface vlan 1` из режима глобального конфигурирования устройства.
- Этап 2** Присвоить IP-адрес и маску с помощью команды `ip address ip-адрес маска` в под режиме конфигурирования интерфейса.
- Этап 3** Включить виртуальный интерфейс сети VLAN 1 с помощью команды `no shutdown` в под режиме конфигурирования интерфейса.
- Этап 4** Указать стандартный шлюз устройства в режиме глобального конфигурирования с помощью команды `ip default-gateway ip-адрес`.

В примере 9.7 приведен описанный выше процесс конфигурирования адреса.

Пример 9.7. Конфигурирование статического IP-адреса коммутатора

```
Emma#configure terminal
Emma(config)#interface vlan 1
Emma(config-if)#ip address 192.168.1.200 255.255.255.0
Emma(config-if)#no shutdown
00:25:07: %LINK-3-UPDOWN: Interface Vlan1, changed state to up
00:25:08: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1,
changed
state to up
Emma(config-if)#exit
Emma(config)#ip default-gateway 192.168.1.1
```

Приведенный выше пример, следует заметить, справедлив для любого интерфейса, в данном случае конфигурируется виртуальный интерфейс сети VLAN 1. Чтобы административно включить интерфейс маршрутизатора или коммутатора, необходимо ввести команду `no shutdown`. Чтобы административно отключить — команду `shutdown` в под режиме конфигурирования интерфейса. Сообщения, которые появляются (см. пример 9.7) сразу же после команды `no shutdown`, представляют собой *системные сообщения* (*syslog*) и свидетельствуют о том, что интерфейс успешно включился.

Чтобы проверить конфигурацию, можно воспользоваться командой `show running-config`⁵ и просмотреть, правильно ли введены конфигурационные команды, в частности, правильно ли указан IP-адрес, маска и адрес стандартного шлюза.

Если требуется настроить коммутатор в режиме клиента DHCP, чтобы его адрес, маска подсети и адрес стандартного шлюза устанавливались автоматически, то нужно изменить конфигурацию устройства. При конфигурировании необходимо выполнить те же пять этапов, которые указаны выше, только этапы 2 и 4 будут отличаться.

- Этап 2** Вместо команды `ip address адрес` для интерфейса VLAN 1 следует использовать команду `ip address dhcp`.
- Этап 4** В режиме глобальной конфигурации устройства команду `ip default-gateway ip-адрес` вводить не нужно.

⁵ Лучше использовать команду `show running-config interface vlan 1`, и хотя она длиннее, но выводит не всю конфигурацию устройства, а только нужного интерфейса. — Примеч. ред.

Пример 9.8 иллюстрирует конфигурирование устройства с использованием протокола DHCP.

Пример 9.8. Динамическая установка IP-адреса с помощью протокола DHCP

```
Emma#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Emma(config)#interface vlan 1
Emma(config-if)#ip address dhcp
Emma(config-if)#no shutdown
Emma(config-if)#+Z
Emma#
00:38:20: %LINK-3-UPDOWN: Interface Vlan1, changed state to up
00:38:21: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed
state to up
Emma#
Interface Vlan1 assigned DHCP address 192.168.1.101, mask 255.255.255.0
Emma#show dhcp lease
Temp IP addr: 192.168.1.101 for peer on Interface: Vlan1
Temp sub net mask: 255.255.255.0
    DHCP Lease server: 192.168.1.1, state: 3 Bound
    DHCP transaction id: 1966
    Lease: 86400 secs, Renewal: 43200 secs, Rebind: 75600 secs
Temp default-gateway addr: 192.168.1.1
    Next timer fires after: 11:59:45
    Retry count: 0 Client-ID: cisco-0019.e86a.6fc0-Vl1
    Hostname: Emma
Emma#show interface vlan 1
Vlan1 is up, line protocol is up
    Hardware is EtherSVI, address is 0019.e86a.6fc0 (bia 0019.e86a.6fc0)
    Internet address is 192.168.1.101/24
    MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
        reliability 255/255, txload 1/255, rxload 1/255
! Остальная информация опущена
```

После того как устройство настроено со статическим IP-адресом, адрес можно посмотреть с помощью команды `show running-config`. Если же коммутатор получает адрес по протоколу DHCP, то в текущей конфигурации он не отображается, чтобы увидеть такой арендованный (временный) адрес и дополнительные параметры, нужно ввести команду `show dhcp lease`.

ВНИМАНИЕ!

Некоторые старые модели коммутаторов с устаревшей операционной системой Cisco IOS могут не поддерживать функцию клиента DHCP на интерфейсе VLAN 1. В примере 9.8 был использован коммутатор модели 2960 с операционной системой IOS версии 12.2.

В последней части примера 9.8 показан результат выполнения команды `show interface vlan 1`, в котором выделены две наиболее важные строки, связанные с адресацией коммутатора. В первой выделенной строке отображается состояние интерфейса VLAN 1, в данном случае это “*up and up*” (активен и активен). Если интерфейс виртуальной локальной сети неактивен, коммутатор не может отправлять и принимать трафик для своего IP-адреса. Такая ситуация может быть в том случае, если системный администратор забыл ввести команду `no shutdown`, а виртуаль-

ный интерфейс стандартно находится в выключенном состоянии и в результате вышеуказанной команды будет отображаться надпись “administratively down” (административно выключен). Обратите также внимание на следующую выделенную строку (третья строка выводимой командой информации). Если IP-адрес по какой-то причине не был получен через протокол DHCP, в этой строке вместо адреса будет отображаться надпись о том, что “адрес будет назначен протоколом DHCP”. Как только адрес будет успешно получен, результат выполнения команды будет похож на показанный в примере 9.8. Тем не менее из отображаемой с помощью команды `show interface vlan 1` информации нельзя определить, был ли установлен адрес статически или получен динамически от сервера DHCP.

Конфигурирование интерфейсов коммутатора

В операционной системе Cisco IOS используется название *интерфейс* (*interface*) для обозначения любого физического *порта*, пересылающего данные от одних устройств к другим. Обычно оба термина используются как синонимы и в дальнейшем так и будут использоваться во всей книге. Для интерфейсов могут быть заданы разные несовпадающие настройки.

В операционной системе Cisco IOS для конфигурирования интерфейсов используется специализированный режим конфигурирования интерфейса, называемый обычно подрежимом интерфейса. Например, в таком подрежиме могут быть использованы команды `duplex` и `speed` для статического указания настроек порта или может использоваться автоматическое определение скорости и дуплексного режима (это стандартная настройка). В примере 9.9 показаны процесс настройки дуплексного режима и скорости, а также использование команды `description` (описание), которая задает некоторое текстовое описание интерфейсу, чтобы было понятно его назначение.

Пример 9.9. Базовые настройки интерфейса

```
Emma#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Emma(config)#interface FastEthernet 0/1
Emma(config-if)#duplex full
Emma(config-if)#speed 100
Emma(config-if)#description Server1 connects here
Emma(config-if)#exit
Emma(config)#interface range FastEthernet 0/11 - 20
Emma(config-if-range)#description end-users connect_here
Emma(config-if-range)#{^Z
Emma#
Emma#show interfaces status
Port      Name          Status       Vlan Duplex    Speed     Type
Fa0/1    Server1 connects h  notconnect  1   full      100      10/100BaseTX
Fa0/2          notconnect  1   auto      auto      10/100BaseTX
Fa0/3          notconnect  1   auto      auto      10/100BaseTX
Fa0/4          connected   1   a-full    a-100    10/100BaseTX
Fa0/5          notconnect  1   auto      auto      10/100BaseTX
Fa0/6          connected   1   a-full    a-100    10/100BaseTX
Fa0/7          notconnect  1   auto      auto      10/100BaseTX
Fa0/8          notconnect  1   auto      auto      10/100BaseTX
Fa0/9          notconnect  1   auto      auto      10/100BaseTX
Fa0/10         notconnect  1   auto      auto      10/100BaseTX
Fa0/11  end-users connect notconnect  1   auto      auto      10/100BaseTX
```

Fa0/12	end-users	connect	notconnect	1	auto	auto	10/100BaseTX
Fa0/13	end-users	connect	notconnect	1	auto	auto	10/100BaseTX
Fa0/14	end-users	connect	notconnect	1	auto	auto	10/100BaseTX
Fa0/15	end-users	connect	notconnect	1	auto	auto	10/100BaseTX
Fa0/16	end-users	connect	notconnect	1	auto	auto	10/100BaseTX
Fa0/17	end-users	connect	notconnect	1	auto	auto	10/100BaseTX
Fa0/18	end-users	connect	notconnect	1	auto	auto	10/100BaseTX
Fa0/19	end-users	connect	notconnect	1	auto	auto	10/100BaseTX
Fa0/20	end-users	connect	notconnect	1	auto	auto	10/100BaseTX
Fa0/21		notconnect	1	auto	auto	auto	10/100BaseTX
Fa0/22		notconnect	1	auto	auto	auto	10/100BaseTX
Fa0/23		notconnect	1	auto	auto	auto	10/100BaseTX
Fa0/24		notconnect	1	auto	auto	auto	10/100BaseTX
Gi0/1		notconnect	1	auto	auto	auto	10/100/1000BaseTX
Gi0/2		notconnect	1	auto	auto	auto	10/100/1000BaseTX

Как именно настроены интерфейсы, можно узнать с помощью команды `show running-config` (она в примере не показана), а краткую информацию можно просмотреть с помощью команды `show interfaces status`. Результат выполнения последней — короткая строка информации о каждом интерфейсе, в первой части которой есть часть описания интерфейса (если оно введено), а во второй отображаются настройки дуплексного режима и скорости. Обратите внимание: в примере 9.9 для интерфейса FastEthernet 0/1 (в выводе команды он пишется сокращенно — Fa0/1) отображается установка скорости 100 и дуплексного режима full, что соответствует введенным конфигурационным командам. Можно сравнить его настройки с параметрами интерфейса Fa0/2, который пока никуда не подключен, и мы увидим, что в обоих полях отображается значение “auto”, которое обозначает автосогласование параметров линии. Аналогично можно сравнить первый и второй интерфейсы с портом Fa0/4, к которому подключено некое устройство, когда процесс автосогласования уже завершился. По строке состояния интерфейса можно определить, что в результате автоматического согласования параметров были установлены скорость в 100 Мбит/с и дуплексный режим работы; об этом свидетельствует приставка a– в соответствующих полях: a-100 и a-full.

Следует также обратить внимание на то, что в операционной системе для удобной и более эффективной работы есть возможность конфигурировать сразу диапазон интерфейсов с помощью команды `interface range`. В приведенном выше примере команда `interface range FastEthernet 0/11 – 20` инструктирует операционную систему IOS о том, что все последующие команды будут применяться к интерфейсам с Fa0/11 по Fa0/20.

Технология безопасности портов

Если сетевой инженер точно знает, какие конкретно устройства будут подключены кабелями к каким интерфейсам коммутатора, он может использовать *режим безопасности* (port security) для соответствующих портов, только указанные устройства смогут передавать данные через такие порты коммутатора. Эта технология заметно снижает уязвимость сети к определенным типам хакерских атак, когда злоумышленник подключает свой ноутбук к настенной компьютерной розетке и получает доступ к сети компании. Когда такое “нелегальное” устройство попадает в сеть и пытается отправить фреймы через интерфейс коммутатора, он создает информационные сообщения, отбрасывает фреймы злоумышленника или даже абсолютно все фреймы от всех устройств, т.е. просто выключает соответствующий порт коммутатора.

Конфигурирование безопасного режима работы порта состоит из нескольких этапов. Прежде всего нужно перевести порт в режим доступа (access, т.е. порт служит для подключения пользователей), следовательно, порт не будет работать в режиме магистрального канала (trunk) для соединения сетей VLAN. Затем нужно включить безопасный режим работы порта без каких-либо настроек, а потом указать MAC-адреса устройств, которые могут использовать этот порт для передачи данных. В приведенном ниже списке описаны основные этапы конфигурирования безопасного режима работы и показаны команды конфигурирования коммутатора.



Настройка режима безопасности порта

- Этап 1** Прежде всего следует перевести интерфейс в режим доступа к сети (access) с помощью команды `switchport mode access` под режимом конфигурирования интерфейса.
- Этап 2** Включить режим безопасности порта с помощью команды `switchport port-security` в под режиме конфигурирования интерфейса.
- Этап 3** Указать максимальное количество разрешенных MAC-адресов для интерфейса с помощью команды `switchport port-security maximum число` в под режиме конфигурирования интерфейса. Стандартно разрешен один MAC-адрес. (Необязательный этап.)
- Этап 4** Указать, какое действие будет выполнять коммутатор при нарушении режима безопасности (например, фрейм получен от MAC-адреса, который отсутствует в таблице) с помощью команды `switchport port-security violation {protect | restrict | shutdown}` в под режиме конфигурирования интерфейса. Стандартная настройка предполагает выключение интерфейса — `shutdown`. (Необязательный этап.)
- Этап 5**
 - а) Указать MAC-адрес (адреса), с которого разрешено отправлять фреймы через данный интерфейс с помощью команды `switchport port-security mac-address mac-адрес`. Эту команду можно вводить несколько раз с разными адресами, если нужно указать более чем один адрес.
 - б) В качестве альтернативы этапу 5 а можно использовать автоматическое обнаружение MAC-адресов (sticky learning) для подключенных к коммутатору узлов с помощью команды `switchport port-security mac-address sticky` под режимом конфигурирования интерфейса.

На рис. 9.2 показана ситуация, когда только Сервер 1 и Сервер 2 могут подключаться к интерфейсам FastEthernet 0/1 и 0/2 соответственно. Если настроен режим безопасности для таких интерфейсов, коммутатор проверяет MAC-адрес отправителя для всех фреймов, которые он получает на этих портах, и пропускает только фреймы для адресов, заданных в интерфейсе командной строки. В примере 9.10 показана конфигурация для рис. 9.2; для интерфейса Fa0/1 MAC-адрес указан явно в конфигурации, а для Fa0/2 используется автоматическое обнаружение.

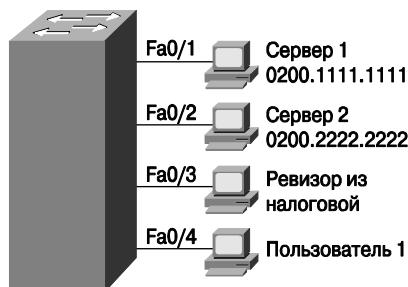


Рис. 9.2. Пример использования режима безопасности

Пример 9.10. Использование режима безопасности для указания разрешенных MAC-адресов для интерфейсов

```
fred#show running-config
! (Часть конфигурации опущена для краткости)

interface FastEthernet0/1
switchport mode access
switchport port-security
switchport port-security mac-address 0200.1111.1111

!
interface FastEthernet0/2
switchport mode access
switchport port-security
switchport port-security mac-address sticky

fred#show port-security interface fastEthernet 0/1
Port Security          : Enabled
Port Status             : Secure-shutdown
Violation Mode         : Shutdown
Aging Time              : 0 mins
Aging Type              : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses   : 1
Total MAC Addresses     : 1
Configured MAC Addresses : 1
Sticky MAC Addresses    : 0
Last Source Address:Vlan : 0013.197b.5004:1
Security Violation Count : 1

fred#show port-security interface fastEthernet 0/2
Port Security          : Enabled
Port Status             : Secure-up
Violation Mode         : Shutdown
Aging Time              : 0 mins
Aging Type              : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses   : 1
Total MAC Addresses     : 1
Configured MAC Addresses : 1
Sticky MAC Addresses    : 1
Last Source Address:Vlan : 0200.2222.2222:1
Security Violation Count : 0

fred#show running-config
! Часть конфигурации опущена для краткости
interface FastEthernet0/2
switchport mode access
switchport port-security
switchport port-security mac-address sticky
switchport port-security mac-address sticky 0200.2222.2222
```

В примере для интерфейса FastEthernet 0/1 MAC-адрес Сервера 1 задан с помощью команды switchport port-security mac-address 0200.1111.1111. Чтобы режим безопасности заработал, коммутатор модели 2960 должен использовать соответствующий интерфейс в режиме доступа к сети, т.е. должна быть указана команда switchport mode access. Далее нужно включить режим безопасности на интерфейсе с помощью команды switchport port-security. Указанные три

команды подрежима настройки интерфейса включают режим безопасности для конкретного порта и разрешают передавать фреймы только с MAC-адресом отправителя 0200.1111.1111. Все остальные настройки остаются стандартными, следовательно, только один внешний MAC-адрес должен быть в таблице интерфейса, и порт будет выключен, если будет получен фрейм с другим адресом отправителя (т.е. в нем будет стоять любой адрес, кроме 0200.1111.1111).

Для интерфейса FastEthernet 0/2 используется функция, называемая *безопасным автоматическим обнаружением MAC-адресов*. В конфигурации опять присутствуют команды `switchport mode access` и `switchport port-security`, поскольку они нужны для работы технологии безопасности порта. Команда `switchport port-security mac-address sticky` инструктирует коммутатор о том, что MAC-адреса устройств должны быть автоматически определены из первого пришедшего в порт фрейма. Такие адреса в дальнейшем добавляются в таблицу безопасных для устройства и в текущую конфигурацию. Другими словами, MAC-адрес как бы “прилипает” (sticks) к интерфейсу и конфигурации, следовательно, сетевому инженеру не нужно его искать и вводить вручную.

Вывод команды `show running-config` в первой части примера 9.10 содержит конфигурацию для интерфейса Fa0/2 до автоматического обнаружения адреса. В конце примера показана та же самая команда, но уже после обнаружения, содержащая команду `switchport port-security mac-address sticky 0200.2222.2222` подрежима конфигурирования интерфейса, которая была добавлена коммутатором автоматически. Если нужно, чтобы в дальнейшем использовался только MAC-адрес 0200.2222.2222 для данного интерфейса, следует сохранить текущую конфигурацию как резервную с помощью команды `copy running-config startup-config`.

В примере 9.10 также показано, что для интерфейса FastEthernet 0/1 произошло *нарушение режима безопасности* (security violation), а с интерфейсом FastEthernet 0/2 все в порядке. Команда `show port-security interface fastethernet 0/1` показывает состояние интерфейса `secure-shutdown`. Он выключен режимом безопасности, что сигнализирует о том, что в интерфейсе была проблема с безопасностью и он был отключен соответствующей службой. Например, в интерфейс Fa0/1 коммутатора пришел фрейм, MAC-адрес отправителя которого был не равен 0200.1111.1111, и произошло нарушение режима безопасности.

Коммутатор может выполнять одно из трех действий в ситуации, когда нарушается режим безопасности для порта. Все три действия приведут к тому, что коммутатор будет отбрасывать подозрительные фреймы, но с помощью конфигурационных команд можно указать дополнительные возможности. Дополнительные функции включают в себя возможность отправки сообщения в системный журнал (syslog) и консольный порт, а также отправку сообщения прерывания SNMP (trap) станции управления сетью, когда коммутатор отключает интерфейс-нарушитель (так называемое событие `err-disable` — отключение по ошибке). В действительности параметр `shutdown` режима безопасности порта переводит его в режим `err-disable`, т.е. в неиспользуемое состояние. Порт в состоянии `err-disable` требует ввода команды `shutdown`, а затем `no shutdown` для переключения его в режим нормальной работы. В табл. 9.4 перечислены параметры команды `switchport port-security violation`, а также указаны соответствующие им действия коммутатора.



Таблица 9.4. Действия коммутатора при нарушении режима безопасности

Параметр/Действие устройства при нарушении режима безопасности	Защита (Protect)	Ограничение (Restrict)	Выключение (Shutdown, стандартное действие)
Отбрасывание подозрительного трафика	Да	Да	Да
Отправка сообщения в системный журнал и через протокол SNMP	Нет	Да	Да
Выключение интерфейса и блокирование всего трафика	Нет	Нет	Да

Конфигурирование сетей VLAN

Интерфейсы коммутаторов компании Cisco могут работать в двух режимах: в режиме *доступа к сети* (access) и в режиме *магистрального канала* (trunk). По определению интерфейсы в режиме доступа к сети могут принимать и отправлять фреймы только для одной сети VLAN, которую называют *виртуальной локальной сетью доступа* (access VLAN). Магистральные порты могут принимать и отправлять фреймы для многих сетей VLAN. Концепции и конфигурирование магистральных соединений для сетей VLAN выходят за рамки рассмотрения данной книги и подробнее описаны в главах 1 и 3 второго тома. В этой книге основной упор делается на конфигурирование сетей VLAN в интерфейсах доступа к сети. Стандартно все интерфейсы привязаны к одной виртуальной локальной сети.

Чтобы коммутатор мог отправлять фреймы в какую-либо сеть VLAN, такая сеть должна существовать. Кроме того, как минимум один интерфейс доступа к сети должен быть связан с такой сетью VLAN. Стандартно во всех коммутаторах компании Cisco сеть VLAN 1 уже настроена и все интерфейсы связаны с ней. Тем не менее, если необходимо, можно создать еще одну виртуальную локальную сеть (VLAN) с другим номером и добавить в нее интерфейсы. Необходимые для этого действия перечислены ниже.

Настройка сетей VLAN



Этап 1 Чтобы настроить новую сеть VLAN, выполните следующие действия.

- В режиме глобальной конфигурации введите команду `vlan номер`, чтобы создать виртуальную сеть и перейти в соответствующий подрежим конфигурирования.
- С помощью команды `name имя` задайте удобное имя виртуальной локальной сети. Если имя не задано, операционная система создаст имя вида VLANxxxx, где xxxx — четырехзначный десятичный номер-идентификатор сети VLAN (VLAN ID). Это необязательная конфигурация.

Этап 2 Чтобы привязать сеть VLAN к интерфейсам, выполните следующие действия для каждого интерфейса доступа к сети.

- С помощью команды `interface` перейдите в режим конфигурирования нужного интерфейса.
- В подрежиме конфигурирования интерфейса введите команду `switchport access vlan номер-сети`, чтобы указать, какая сеть VLAN связана с этим интерфейсом.
- Чтобы отключить возможность автоматической установки *магистрального соединения* (trunking), введите команду `switchport mode access` в режиме конфигурирования интерфейса.

В примере 9.11 показан процесс добавления новой сети VLAN и привязки интерфейсов к ней. Сеть, используемая в этом примере, показана на рис. 9.3; она состоит из одного коммутатора (SW1) и двух хостов в обеих сетях VLAN (1 и 2). В примере 9.11 показан двухэтапный процесс добавления интерфейсов в сеть VLAN 2.

Пример 9.11. Конфигурирование сетей VLAN и привязка их к интерфейсам

! В коммутаторе стандартно есть 5 сетей VLAN, и все интерфейсы привязаны
! к сети 1

SW1#show vlan brief

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gi0/1, Gi0/2
1002	fdci-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fdinnet-default	act/unsup	
1005	trnet-default	act/unsup	

! Сеть VLAN 2 еще не существует. Ниже она добавлена администратором и
! названа Freds-vlan, а также два интерфейса привязаны к сети VLAN 2.

SW1#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

SW1(config)#vian 2

SW1(config-vlan)#name Freds-vlan

SW1(config-vlan)#exit

SW1(config)#interface range fastethernet 0/13 - 14

SW1(config-if)#switchport access vlan 2

SW1(config-if)#exit

! Ниже показан результат выполнения команды **show running-config**,

! содержащий нужные команды для интерфейсов Fa0/13 и Fa0/14.

! Команды **vlan 2** и **name Freds-vlan** не показываются в текущей

! конфигурации устройства, т.е. в running-config.

SW1#show running-config

! Часть строк опущена

interface FastEthernet0/13
switchport access vlan 2
switchport mode access

!

interface FastEthernet0/14
switchport access vlan 2
switchport mode access

!

SW1#show vlan brief

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/15, Fa0/16, Fa0/17, Fa0/18 Fa0/19, Fa0/20, Fa0/21, Fa0/22 Fa0/23, Fa0/24, Gi0/1, Gi0/2
2	Freds-vlan	active	Fa0/13, Fa0/14

```

1002 fddi-default      act/unsup
1003 token-ring-default act/unsup
1004 fddinet-default   act/unsup
1005 trnet-default    act/unsup

```

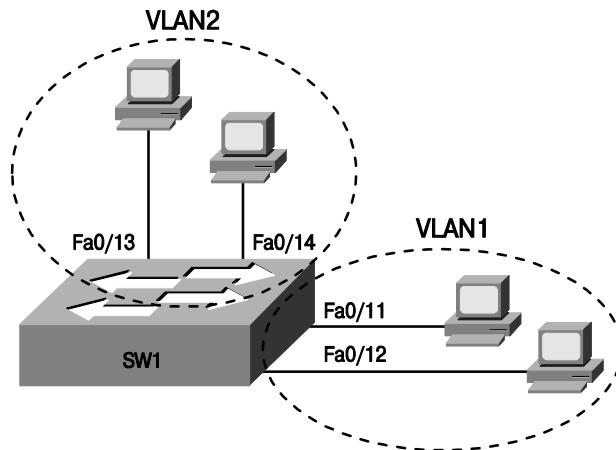


Рис. 9.3. Сеть, состоящая из одного коммутатора и двух сетей VLAN

В начале примера приведен результат выполнения команды `show vlan brief`, в котором видны стандартные настройки коммутатора: стандартные пять сетей VLAN, которые нельзя удалить (VLAN 1 и с 1002 по 1005); все интерфейсы привязаны к сети VLAN 1. Обратите внимание: у коммутатора модели 2960 есть 24 интерфейса FastEthernet (Fa0/1-Fa0/24) и два гигабитовых порта Ethernet (Gi0/1 и Gi0/2), все они имеются в конфигурации и привязаны к сети VLAN 1.

После первой команды `show vlan brief` в примере показан весь процесс конфигурации полностью. Сначала создается виртуальная локальная сеть VLAN 2, потом ейдается имя “*Freds-vlan*”, далее к ней привязываются интерфейсы Fa0/13 и Fa0/14. Обратите внимание на то, что в данном примере используется команда `interface range`, позволяющая ввести команду `switchport access vlan 2` сразу для двух интерфейсов (т.е. в указанном диапазоне интерфейсов). Результат этого действия впоследствии виден в выводе команды `show running-config` в конце примера.

После того как конфигурация была изменена, чтобы проверить новую сеть VLAN, еще раз используется команда `show vlan brief`, но теперь в ней появилась сеть VLAN 2 с именем “*Freds-vlan*”, и к ней привязаны два интерфейса: Fa0/13 и Fa0/14.

Повышение уровня безопасности неиспользуемых интерфейсов

Компания Cisco разработала стандартные настройки интерфейсов коммутаторов таким образом, чтобы они работали сразу после включения устройства без какой-либо дополнительной конфигурации. Интерфейсы автоматически согласовывают скорость и режим дуплексности, кроме того, каждый интерфейс находится во включенном состоянии (`no shutdown`), и все они привязаны к сети VLAN 1. Все интерфейсы также согласовывают дополнительные параметры сетей VLAN, используется ли *магистральное соединение (trunking)* и работает ли *протокол магистральных соединений (trunk protocols)*.

нений сетей VTP (VLAN Trunking Protocol — VTP), который подробно рассмотрен в главе 2 второго тома книги.

Благие намерения компании Cisco по созданию системы “подключи и работай” (plug-and-play) дали неожиданный побочный эффект в виде проблем с безопасностью устройства. Поэтому для всех неиспользуемых интерфейсов коммутатора компания Cisco рекомендует сменить стандартные настройки, чтобы сделать устройство более защищенным. Рекомендуется выполнить следующие действия для всех неиспользуемых интерфейсов:



Рекомендованные настройки неиспользуемых портов коммутатора

- административно отключить интерфейсы с помощью команды `shutdown` под режима конфигурирования интерфейса;
- отключить автоматическое согласование магистрального соединения (trunking) и протокола VTP, переведя порт в режим работы доступа к сети (access) с помощью команды `switchport mode access` под режима конфигурирования интерфейса;
- привязать все неиспользуемые порты к неиспользуемой сети VLAN с помощью команды `switchport access vlan номер` под режима конфигурирования интерфейса.

Откровенно говоря, административное отключение интерфейса является самым надежным методом и закрывает все бреши в защите устройства. Тем не менее два последних действия помогут избежать множества проблем в том случае, если кто-либо перенастроит устройство и включит интерфейс с помощью команды `no shutdown`.

Подготовка к экзамену

Повторите все ключевые темы

Повторите все ключевые темы данной главы, помеченные пиктограммой “Ключевая тема”. Ключевые темы и соответствующие им страницы перечислены в табл. 9.5.

ВНИМАНИЕ!

Рекомендуется запоминать этапы конфигурирования устройств, которые помечены как ключевые темы главы. Эти списки также нужны для изучения технологии и приобретения навыков работы с устройствами.

Таблица 9.5. Ключевые темы главы 9

Элемент	Описание	Страница
Пример 9.1	Конфигурирование основных паролей и названия устройства	272
Рис. 9.1	Процесс конфигурирования протокола SSH	275
Список	Процесс конфигурирования протокола SSH	275
Список	Ключевые отличия команд enable secret и enable password	278
Табл. 9.3	Команды буфера истории команд	282
Список	Настройка IP-адреса и стандартного шлюза коммутатора	284
Список	Настройка режима безопасности порта	288
Табл. 9.4	Действия коммутатора при нарушении режима безопасности	291
Список	Настройка сетей VLAN	291
Список	Рекомендованные настройки неиспользуемых портов коммутатора	294
Табл. 9.7	Список команд для поиска и устранения неисправностей В этой таблице показано несколько простых, но очень важных команд!	297

Заполните таблицы и списки по памяти

Распечатайте приложение М (Appendix L) с компакт-диска или его раздел, относящийся к этой главе, и заполните таблицы и списки по памяти. В приложении Н (Appendix M) приведены заполненные таблицы и списки для самоконтроля.

Ключевые термины

Дайте определения перечисленных ниже терминов и проверьте правильность их написания в списке терминов:

интерфейс доступа к сети (access), магистральный канал (trunk).

Список команд

В табл. 9.6 приведен список команд этой главы, а также даны их короткие описания.

Таблица 9.6. Список команд главы 9

Команда	Режим/назначение/описание
	Базовое конфигурирование паролей
line console 0	Переключает контекст командной строки в режим конфигурирования консольной линии
line vty 1-я_vty_линия последняя_vty_линия	Переключает контекст в режим конфигурирования линий vty для указанного в команде диапазона
login	Режим конфигурирования консольной линии или линии vty. Указывает операционной системе IOS, что нужно выдавать приглашение для ввода пароля
password пароль	Режим конфигурирования консольной или линии vty. Задает пароль, который будет запрашиваться при подключении к устройству
	Конфигурирование имен, паролей и протокола SSH
login local	Режим конфигурирования консольной линии или линии vty. Указывает операционной системе IOS, что нужно выдавать приглашение для ввода имени пользователя и пароля, которые проверяются в локальной базе данных (т.е. заданных с помощью команды username в режиме глобальной конфигурации маршрутизатора или коммутатора)
username имя password пароль	Режим глобальной конфигурации. С помощью этой команды можно задавать множество пар “имя пользователя–пароль” для аутентификации. Имена и пароли используются командой login local в режиме конфигурирования линий
crypto key generate rsa	Режим глобальной конфигурации. Создает и сохраняет (в закрытой области флеш-памяти) ключи протокола SSH
transport input {telnet ssh}	Режим конфигурирования линии vty. Указывает, разрешен ли к устройству доступ по протоколам Telnet, SSH и др. Если в команде указаны оба протокола, значит, доступ возможен как с помощью сеанса Telnet, так и SSH (стандартно)
	Конфигурирование IP-адреса
interface vlan номер	Переключает контекст командной строки в режим конфигурирования интерфейса сети VLAN. Для сети VLAN 1 устанавливается IP-адрес
ip address адрес маска_подсети	Режим конфигурирования интерфейса. Используется для статического указания IP-адреса и маски подсети
ip address dhcp	Режим конфигурирования интерфейса. Конфигурирует коммутатор как клиент DHCP, чтобы он мог автоматически получить IP-адрес, маску подсети и стандартный шлюз
ip default-gateway адрес	Режим глобальной конфигурации. Задает адрес стандартного шлюза для коммутатора. Эта команда не нужна, если коммутатор использует протокол DHCP
	Конфигурирование интерфейсов
interface тип номер_порта	Переключает контекст командной строки в режим конфигурирования интерфейса. В параметре типа интерфейса обычно указывают значение FastEthernet или GigabitEthernet (для коммутаторов). Возможные номера портов зависят от модели коммутатора и выглядят, например, так: 0/1, 0/2 и т.п.
interface range тип диапазон_портов	Переключает контекст командной строки в режим конфигурирования диапазона интерфейсов. Вводимые после этой команды настройки применяются ко всем интерфейсам диапазона
shutdown no shutdown	Режим конфигурирования интерфейса. Первая команда административно выключает интерфейс, вторая, соответственно, включает интерфейс

Окончание табл. 9.6

Команда	Режим/назначение/описание
speed { 10 100 1000 auto}	Режим конфигурирования интерфейса. Задает скорость интерфейса, если указан параметр <code>auto</code> , выполняется автосогласование скорости линии
duplex {auto full half}	Режим конфигурирования интерфейса. Задает дуплексный режим работы интерфейса, если указан параметр <code>auto</code> , выполняется автосогласование дуплексности
description текст	Режим конфигурирования интерфейса. Устанавливает текстовый комментарий-описание для интерфейса. Используется для упрощения поиска, устранения неисправностей и удобства в работе
Дополнительные настройки	
hostname имя	Режим глобальной конфигурации. Задает имя хоста для коммутатора, которое также используется в приглашении командной строки
enable secret пароль	Режим глобальной конфигурации. Задает пароль привилегированного режима
history size число	Режим конфигурирования линии. Задает количество команд, которое будет сохраняться в буфере истории команд
switchport port-security mac-address mac-адрес	Режим конфигурирования интерфейса. Добавляет статическую запись для указанного MAC-адреса в таблицу разрешенных для данного интерфейса
switchport port-security mac-address sticky	Режим конфигурирования интерфейса. Разрешает коммутатору самостоятельно обнаружить MAC-адреса и добавить их в таблицу безопасных для текущего интерфейса
switchport port-security maximum значение	Режим конфигурирования интерфейса. Указывает максимальное разрешенное количество безопасных MAC-адресов для данного интерфейса
switchport port-security violation {protect restrict shutdown}	Режим конфигурирования интерфейса. Указывает, какое действие должен предпринять коммутатор в том случае, если нарушен режим безопасности и устройство с небезопасным MAC-адресом пытается получить доступ к сети через безопасный порт

В табл. 9.7 приведен список команд для поиска и устранения неисправностей.

Таблица 9.7. Список команд для поиска и устранения неисправностей



Команда	Назначение
show mac address-table dynamic	Показывает динамические записи в таблице коммутации коммутатора
show dhcp lease	Показывает информацию, связанную с режимом клиента DHCP коммутатора. Информация содержит IP-адрес, сетевую маску и адрес стандартного шлюза
show crypto key mypubkey rsa	Показывает публичный и общий ключи, которые были созданы для протокола SSH с помощью команды <code>crypto key generate rsa</code> режима глобальной конфигурации устройства
show interfaces status	Показывает краткий список и состояние интерфейсов (одна строка на интерфейс). Выводимая командой информация содержит описание, состояние, а также настройки дуплексности и скорости для интерфейса
show interfaces vlan 1	Показывает состояние интерфейса, IP-адрес коммутатора, его сетевую маску и еще много полезной информации
show port-security interface тип номер	Показывает параметры конфигурации режима безопасности порта и его состояние

В этой главе...

- **Принципы проверки сетей, а также поиск и устранение неисправностей.** Поскольку это первая глава, посвященная поиску и устраниению неисправностей в книге, в этом разделе описаны основные концепции проверки сетей.
- **Построение топологии сети с помощью протокола обнаружения устройств Cisco.** Подробно описан протокол CDP, в частности, рассказывается, как его можно использовать для проверки сетевой документации.
- **Анализ состояния интерфейса на 1- и 2-м уровнях.** Объясняется, как получить и интерпретировать информацию о состоянии интерфейса, а также как обнаружить проблемы, если они с первого взгляда незаметны.
- **Анализ маршрута коммутации фреймов на основе таблиц MAC-адресов.** Здесь вы узнаете, как связать концепции коммутации фреймов с выводом команд `show` и проверить работу устройства.

ГЛАВА 10

Поиск и устранение неисправностей в коммутаторах Ethernet

В текущей главе рассмотрены две основные темы. Первая посвящена описанию технологий Ethernet, которые были раньше опущены, например, основные концепции и команды, связанные с проверкой работоспособности коммутируемых сетей LAN, а также необходимые для этого команды. В этой главе описан необходимый набор средств диагностики локальной сети в том случае, если она не работает. Вторая тема — основные методы поиска и устранения неисправностей, а также практические рекомендации, которые помогут получить некоторый начальный опыт проверки сетей. Несмотря на то что опыт по поиску и устранению неисправностей напрямую на экзамене не проверяется, эта глава поможет подготовиться к более сложным тестам и последующим экзаменам.

Контрольные вопросы: знаете ли вы уже темы главы

Этот раздел предназначен для того, чтобы читатель мог предварительно оценить свои знания и решить, нужно ли ему читать главу целиком. Если ответы на девять из десяти вопросов даны правильно, можно сразу же перейти к последнему разделу “Подготовка к экзамену”. Основные темы этой главы и предварительных контрольных вопросов перечислены в табл. 10.1. Отвечая на контрольные вопросы и используя таблицу, читатель сможет достаточно точно определить свои знания в той или иной области. Ответы на вопросы приведены в приложении А.

Таблица 10.1. Темы контрольных вопросов

Основная тема	Номера вопросов
Принципы проверки сетей, а также поиск и устранение неисправностей	—
Построение топологии сети с помощью протокола обнаружения устройств Cisco	1, 2
Анализ состояния интерфейса на 1- и 2-м уровнях	3–6
Анализ маршрута коммутации фреймов на основе таблиц MAC-адресов	7, 8

- Представьте себе коммутатор, который подключен кабелем Ethernet к маршрутизатору; маршрутизатору в конфигурации присвоено имя *Hannah*. С помощью какой команды можно узнать версию операционной системы устройства *Hannah*, не устанавливая с ним сеанс Telnet? (Выберите несколько ответов.)
 - show neighbor Hannah
 - show cdp
 - show cdp neighbor

- г) show cdp neighbor Hannah
- д) show cdp entry Hannah
- е) show cdp neighbor detail

2. С помощью какой команды для того же устройства (Hannah) можно установить модель аппаратной платформы? (Выберите несколько ответов.)

- а) show neighbors
- б) show neighbors Hannah
- в) show cdp
- г) show cdp interface
- д) show cdp neighbors
- е) show cdp entry Hannah

3. Вывод команды show interfaces status для коммутатора модели 2960 показывает в строке состояния слово “disabled” (отключен) для интерфейса Fa0/1. Какое из указанных ниже утверждений справедливо для такого интерфейса? (Выберите несколько ответов.)

- а) В конфигурации интерфейса указана команда shutdown.
- б) В выводе команды show interfaces fa0/1 будут отображаться два кода состояний: административно выключен (administratively down) и выключен (down).
- в) В выводе команды show interfaces fa0/1 будут отображаться два кода состояний: включен (up) и выключен (down).
- г) Интерфейс в данном случае не будет пересыпать фреймы.
- д) Интерфейс в данном случае будет пересыпать фреймы.

4. Гигабитовый интерфейс 0/1 (Gi0/1) коммутатора SW1 подключен к гигабитовому интерфейсу 0/2 (Gi0/2) коммутатора SW2. Для интерфейса Gi0/2 коммутатора SW2 указаны команды — speed 1000 и duplex full. В коммутаторе SW1 используются стандартные настройки для порта Gi0/1. Какое из указанных ниже утверждений справедливо для такого соединения между интерфейсами? (Выберите несколько ответов.)

- а) Соединение между устройствами будет работать на скорости 1000 Мбит/с (т.е. 1 Гбит/с).
- б) Коммутатор SW1 будет пытаться установить скорость 10 Мбит/с, поскольку у коммутатора SW2 отключено автоматическое согласование стандарта IEEE.
- в) Соединение будет работать на скорости 1 Гбит/с, но коммутатор SW1 будет работать в полудуплексном режиме, а SW2 — в дуплексном.
- г) Оба коммутатора будут работать в дуплексном режиме.

5. С помощью команды show interfaces fa0/1 был получен следующий результат:

Full-duplex, 100Mbps, media type is 10/100BaseTX

Что из перечисленного ниже справедливо для соответствующего интерфейса? (Выберите несколько ответов.)

а) Скорость была явно задана с помощью команды `speed 100` в подрежиме конфигурирования интерфейса.

б) Скорость, возможно, была задана с помощью команды `speed 100` в подрежиме конфигурирования интерфейса.

в) Дуплексный режим был явно задан с помощью команды `duplex full` в подрежиме конфигурирования интерфейса.

г) Дуплексный режим, возможно, был задан с помощью команды `duplex full` в подрежиме конфигурирования интерфейса.

6. Коммутатор SW1 модели Cisco 2960 имеет для интерфейса Fa0/1 стандартные настройки, для интерфейса Fa0/2 введена команда `speed 100`, а для интерфейса Fa0/3 введены обе команды: `duplex half` и `speed 100`. Эти интерфейсы подключены правильным кабелем к портам 10/1000 другого коммутатора модели 2960, порты которого используют стандартные настройки. Какое из перечисленных ниже утверждений справедливо для интерфейсов коммутатора со стандартными настройками? (Выберите несколько ответов.)

а) Интерфейс, подключенный к порту Fa0/1 коммутатора SW1, будет работать на скорости 100 Мбит/с в дуплексном режиме.

б) Интерфейс, подключенный к порту Fa0/2 коммутатора SW1, будет работать на скорости 100 Мбит/с в дуплексном режиме.

в) Интерфейс, подключенный к порту Fa0/3 коммутатора SW1, будет работать на скорости 100 Мбит/с в дуплексном режиме.

г) Интерфейс, подключенный к порту Fa0/3 коммутатора SW1, будет работать на скорости 100 Мбит/с в полудуплексном режиме.

д) Интерфейс, подключенный к порту Fa0/2 коммутатора SW1, будет работать на скорости 100 Мбит/с в полудуплексном режиме.

7. Фрейм поступил на интерфейс Fa0/3 коммутатора SW2 с MAC-адресом отправителя 0200.1111.1111 и MAC-адресом получателя 0200.2222.2222. Интерфейс Fa0/3 назначен сети VLAN 2. Рассмотрите приведенный ниже вывод коммутатора SW2. Какое из нижеперечисленных утверждений правильно описывает то, что коммутатор делает с этим фреймом?

```
SW2#show mac address-table dynamic
      Mac Address Table
```

Vlan	Mac Address	Type	Ports
1	0200.1111.1111	DYNAMIC	Gi0/2
1	0200.2222.2222	DYNAMIC	Fa0/13

Total Mac Addresses for this criterion: 2

а) Коммутатор отбрасывает фрейм.

б) Коммутатор пересыпает фрейм через порт Fa0/13.

в) Коммутатор изменит существующую запись для MAC-адреса 0200.1111.1111 как указано в выводе, но только изменит интерфейс на Fa0/3.

г) Коммутатор пересыпает фрейм через порт Gi0/2 и Fa0/13.

д) Коммутатор добавит новую запись в таблицу МАС-адресов для 0200.1111.1111.

8. Какая из указанных ниже команд отображает записи таблицы МАС-адресов, используемые в технологии безопасности порта коммутатора? (Выберите несколько ответов.)

- а) show mac address-table dynamic
- б) show mac address-table
- в) show mac address-table static
- г) show mac address-table port-security.

Основные темы

В этой главе представлены основные сведения о методах и командах проверки сети, а также о процедурах поиска и устранения неисправностей. Под проверкой подразумевается процесс исследования сети, результатом которого будет подтверждение того факта, что сеть работает именно так, как предполагалось при ее разработке и внедрении. Под поиском и устранением неисправностей понимают процесс изучения сети с целью обнаружения причины (или причин) какой-либо ошибки и действия по ее устранению.

Как говорилось во введении к этой книге, с течением времени в экзамене CCNA появляется все больше и больше вопросов, связанных с поиском и устранением неисправностей, а также с методами проверки работоспособности сети. В каждом таком вопросе обычно используется собственная топология сети. В задании обычно требуется применить свои сетевые знания к некоторой уникальной проблеме, а не просто выбрать правильный ответ из нескольких вариантов, т.е. вопрос не связан с запоминанием каких-либо чисел, фактов или технологий.

Чтобы помочь читателю подготовиться к уверенной сдаче экзамена, в обоих томах этой книги есть главы, целиком посвященные поиску и устранению неисправностей в сетях. Данная глава является первой главой на тему проверки работоспособности сети, поэтому в первом ее разделе описаны некоторые концепции и общие вопросы поиска и устранения проблем в компьютерных сетях. В трех оставшихся разделах подробно рассмотрены основные темы, связанные с поиском и устранением неисправностей в локальных сетях (LAN), которые построены на основе коммутаторов.

Принципы проверки сетей, а также поиск и устранение неисправностей

ВНИМАНИЕ!

Информация, представленная в этом разделе, поможет читателю приобрести полезные навыки поиска и устранения неисправностей в сетях. Специфические советы и методики, представленные в разделе, не связаны с какой-либо конкретной темой экзамена CCNA.

Для успешной сдачи экзамена CCNA недостаточно только теоретических знаний, нужны также некоторые практические навыки, чтобы ответить на сложные прикладные вопросы. Следует также отметить, что уровень сложности вопросов в сертификационном экзамене разный. В текущем разделе сначала рассмотрены различные типы вопросов, которые могут быть на экзамене CCNA, а потом даны общие комментарии по методам поиска и устранения неисправностей.

Вопросы с эмуляцией сети

В вопросах с *эмulationю сети* (sim questions), которые также называют зачастую лабораторными заданиями, есть текстовое описание сети и ее настроек, схема подключения устройств и, собственно, само программное обеспечение, эмулирующее сеть. Независимо от того, какое именно задание содержится в вопросе, его можно

свести к укороченной постановке задачи, которая звучит следующим образом: “Сеть работает не полностью, следовательно, нужно либо доделать незавершенную конфигурацию, либо найти проблему в сети и устраниить ее”. Другими словами, основная задача — внести нужные конфигурационные изменения, чтобы сеть заработала так, как надо.

Первый метод решения проблемы в сети — использовать формализованный процесс поиска и устранения неисправностей, который подразумевает инспектирование каждого этапа передачи данных на каждом транзитном узле от хоста отправителя к получателю. Тем не менее, как показывает практическая работа и опыт обучения слушателей, обычно сетевые инженеры изначально предполагают, что проблемы вызваны неправильной конфигурацией устройства, и сразу же начинают просматривать различные конфигурационные файлы. Наиболее быстрым методом выполнения задания с эмуляцией сети будет сравнение имеющихся конфигураций маршрутизаторов и/или коммутаторов с правильными. Обычно сравнения вполне достаточно, чтобы быстро выполнить задание.

В лабораторных заданиях экзаменуемый может быть точно уверен в правильности решения по крайней мере на уровне технологий, рассматриваемых в экзамене CCNA. Правильное решение должно полностью решать поставленную в вопросе задачу или проблему. Например, в постановке задачи написано, что маршрутизатор R1 не может переслать пакеты эхо-запросов (ping) маршрутизатору R2, и эту проблему нужно устранить. Если после выполнения задания в эмуляторе команда ping показывает, что пакеты успешно доходят до дистанционного хоста, значит, изменения в конфигурации полностью устранили проблему.

Если же вы не можете найти проблему, просто просматривая конфигурацию, то придется пойти по более сложному пути: инспектировать процесс передачи данных подробнее с помощью команд `show`. В последующих разделах, посвященных методам поиска и устранения неисправностей, первого и второго тома книги будут подробнее рассмотрены более сложные методики проверки сетей.

Симлэты

В этой разновидности экзаменационных заданий необходимо интерпретировать результаты выполнения различных команд `show` и `debug`. В *симлете* (*simlet*) обычно неизвестен пароль привилегированного пользователя (или недоступна соответствующая команда), поэтому нельзя увидеть конфигурацию устройства, чтобы быстро найти причину неполадки. В таких заданиях обычно в сопроводительном тексте описан некоторый сценарий, а необходимые команды `show` экзаменуемый должен помнить на память, ввести их и “расшифровать” результат выполнения команд. Кроме того, в симлэтах нельзя вносить изменения в конфигурацию, поэтому проверить, правильный ли выбран ответ или получен нужный результат, невозможно.

Например, в задании симлэта показана схема коммутируемой локальной сети (LAN) и сказано, что компьютер №1 успешно отправляет пакеты эхо-запросов компьютеру №2, а до компьютера №3 пакеты не доходят. Задача экзаменуемого — вспомнить нужные команды группы `show` (или потратить много времени на их поиск с помощью команды `?`), чтобы определить, в чем проблема.

Для успешного решения таких экзаменационных задач можно использовать несколько подходов; нельзя сказать, что какой-то из них лучше остальных: все они

примерно одинаковы. Сначала следует подумать над тем, что бы происходило в сети, если бы она работала нормально. Исходные данные для таких размышлений нужно взять из схемы сети и доступной в задании информации о ее работе. Затем большинство сдающих экзамен начинают использовать команды `show` (те, что они помнят), которые могут быть связаны с заданием. Скорее всего, в тексте задания будет некоторая подсказка, относящаяся к проблемной области. Например, задание симлита связано с технологией *безопасности портов* (*port security*). В таком случае следует сразу попробовать выполнить команды, связанные с проверкой этой технологии, например `show port-security`, чтобы посмотреть, нет ли там нужной информации и, возможно, ответа на заданный вопрос. Это вполне оправданный подход к выполнению экзаменационного задания. В нем используется обычный здравый смысл, небольшая толика интуиции, и такой метод может работать достаточно хорошо и быстро.

Если вы не нашли ответ или ответы для симлита после того, как были использованы вполне стандартные и очевидные команды, следует использовать более сложный подход. В этой главе и в последующих главах первого и второго тома, посвященных поиску и устранению неисправностей, представлены различные методы проверки сетей и приведены обзоры многих технологий. Их и следует использовать, если ответ на задание симлита оказался не настолько простым, как хотелось бы.

Вопросы с многовариантным ответом

Как и симлты, *вопросы с многовариантным ответом* (*multiple-choice questions*) могут требовать интерпретации результатов выполнения команд `show` и `debug`. Такие вопросы могут просто сопровождаться результатом вывода какой-либо команды, а также еще и рисунком или схемой сети и проверять, понимает ли экзаменуемый, что происходит. Например, во многовариантном вопросе может быть показан результат выполнения команды `show mac address-table dynamic`, в котором видна таблица динамически обнаруженных коммутатором МАС-адресов. По такой таблице, согласно заданию, нужно будет определить, как именно коммутатор будет пересыпать фрейм от одного устройства другому. Для такого вопроса потребуется применить свои знания о принципах коммутации в локальных сетях к выводу указанной команды.

Вопросы с многовариантным ответом, в которых есть результат выполнения команд `show` и `debug`, требуют такого же подхода, как и симлты. Точно так же как и в симлтах, первым делом следует подумать о том, что должно происходить в сети в нормальных условиях с учетом схемы сети на рисунке и постановки задачи в вопросе. Далее следует сравнить информацию в задании, в том числе и результаты команд, с той, что должна быть правильной с точки зрения теории, чтобы определить, работает сеть нормально или есть какая-либо проблема. Сеть может работать вполне корректно, и в таком случае вопрос направлен на то, чтобы подтвердить, что специалист знает, как именно должна работать сеть, и знает, с помощью какой именно команды можно проверить этот факт. Принципиальное отличие вопросов многовариантного типа состоит в том, что не нужно помнить, какие именно команды нужно использовать. Результат команды уже есть в задании, нужно только умело им воспользоваться.

ВНИМАНИЕ!

Какие типы вопросов могут быть в экзамене на сертификат CCNA, можно посмотреть на веб-сайте компании по адресу

http://www.cisco.com/web/learning/wwtraining/certprog/training/cert_exam_tutorial.html.

Как ответить на сложные вопросы экзамена

Если решение лабораторного задания, симлита или ответ на многовариантный вопрос не очевидны после использования стандартных простых средств, которые обсуждались выше, следует использовать метод упорядоченной проверки сети. Он хорошо работает не только на экзаменах, но и в задачах, которые инженеру обычно приходится решать в реальной жизни.

К сожалению, время экзамена ограничено, а тщательное обдумывание проблемы потребует его много.

Процесс упорядоченного поиска и устранения неисправностей хорош при подготовке к экзамену, когда времени много, — он поможет лучше разобраться в сетевых технологиях и подготовиться к вопросам экзамена. В этой книге рассмотрены многие методы поиска и устранения неисправностей, тем не менее, такие методы не являются самоцелью, поэтому не нужно запоминать их на память. Методы поиска и устранения неисправностей представляют собой в основном инструмент для обучения, а также имеют дополнительный плюс — помогают подготовиться к самым сложным вопросам сертификационного экзамена.

В этом разделе представлено описание некоторого обобщенного процесса поиска и устранения неисправностей в сетях. По мере изучения материала данной книги этот процесс будет периодически повторяться, но уже для определенных сетевых технологий, например, для IP-маршрутизации. Три основных этапа процесса поиска и устранения неисправностей подробно описаны ниже.

Этап 1 Предсказание и анализ нормального поведения. Нужно представить себе, что должно происходить, когда сеть работает правильно, на основании документации, конфигурационных команд и результатов выполнения команд `show` и `debug`.

Этап 2 Изоляция проблемы. Необходимо определить, как далеко по пути следования пакета или фрейма распространяется проблема и где начинается нормальная работа сети, опять же на основании документации, конфигурационных команд и результатов выполнения команд `show` и `debug`.

Этап 3 Анализ источника проблемы. Необходимо идентифицировать глубинные причины проблемы, которая была выявлена на предыдущем этапе. В частности, следует продумать, какие именно действия помогут решить проблему.

Следование описанному выше процессу требует достаточно обширных знаний и навыков. Чтобы успешно искать отказы в сети, следует хорошо помнить теоретические основы работы компьютерных сетей, а также уметь интерпретировать результаты различных команд `show` в разных ситуациях и режимах работы сети. В процессе поиска неисправностей понадобятся дополнительные инструменты, такие как команды `ping` и `traceroute`, которые помогут локализовать и изолировать проблемный участок. Кроме того, нужно уметь мыслить широко и обладать разнообразными знаниями, чтобы учесть все факторы, которые могут влиять на какой-либо компонент сети.

Например, представим себе простую локальную сеть, в которой два коммутатора соединены друг с другом и к каждому из них подключено по одному компьютеру (ПК). Изначально компьютеры могли отправлять друг другу пакеты эхо-запросов (например, компьютер ПК1 мог переслать пакеты компьютеру ПК2), а сейчас такие запросы не достигают цели. Следует изучить документацию и вывод команд группы `show`, чтобы убедиться, что топология сети не поменялась, и предсказать, как должна работать сеть, на основе знаний о коммутации в локальных сетях. В результате на схеме сети можно нарисовать маршрут следования фреймов от компьютера ПК1 к компьютеру ПК2. Чтобы изолировать проблему, следует просмотреть таблицы MAC-адресов коммутаторов. По таблицам можно сказать, что интерфейсы, через которые должен пересыпаться фрейм, функционируют правильно, или, вполне возможно, убедиться в том, что какой-то из интерфейсов коммутаторов (например, подключенный к ПК2) не работает. Сведения о том, что интерфейс не работает, не дают нам никакой информации о том, почему это произошло и в чем причина проблемы. На этом этапе следует включить свое воображение и представить себе причины, почему возникла данная ситуация. Причины могут быть очень разнообразными: отключенный сетевой кабель, интерференция и помехи в линии и другие, вплоть до того, что просто сработала технология *безопасности порта* (*port security*) и отключила интерфейс. Команды группы `show` в таком случае могут либо подтвердить предположения, либо исключить какие-то технологии из рассмотрения и натолкнуть на новую мысль.

Изоляция проблем 3-го уровня, а также уровней 1 и 2

Прежде чем перейти к рассмотрению методов поиска и устранения неисправностей в локальных сетях Ethernet, следует окунуть беглым взглядом более широкий круг технологий. Большая часть проблем в сетях IP на сегодняшний день начинается с того, что именно наблюдает и с чем сталкивается конечный пользователь. Поэтому анализ ситуации обычно начинается с исследования того, насколько хорошо работает именно третий уровень сети (Layer 3). Например, пользователь ПК1 (рис. 10.1) обычно без проблем может подключиться к веб-серверу, просто введя адрес `www.example.com` в строке браузера. Представим себе, что в данный момент соединение с сервером не было успешным. Пользователь звонит в службу технической поддержки, и решение этой проблемы передается дежурному сетевому инженеру.

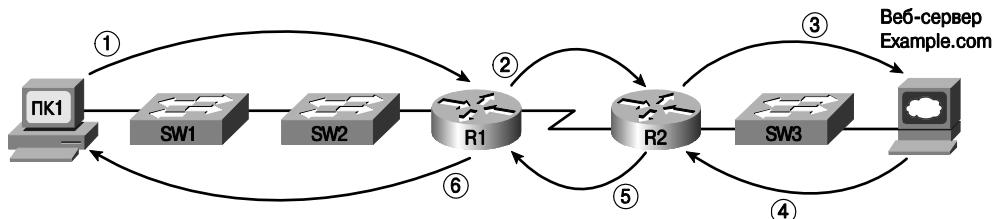


Рис. 10.1. Изоляция проблемы третьего уровня

После того как проблема описана, инженер сначала проверяет, может ли компьютер ПК1 правильно преобразовать имя хоста (`www.example.com`) в его IP-адрес. Далее процесс изоляции проблемы на третьем уровне для технологии IP может сле-

довать шести указанным ниже этапам. Описание этапов, показанных на рис. 10.1, приведено ниже.

- Этап 1** Компьютер ПК1 пересыпает пакет своему стандартному шлюзу (маршрутизатору R1), поскольку IP-адрес получателя находится в другой подсети.
- Этап 2** Маршрутизатор R1 пересыпает пакет маршрутизатору R2 согласно записям в своей таблице маршрутизации.
- Этап 3** Маршрутизатор R2 пересыпает пакет веб-серверу согласно записям в своей таблице маршрутизации.
- Этап 4** Веб-сервер отправляет ответный пакет компьютеру ПК1 через свой стандартный шлюз (маршрутизатор R2).
- Этап 5** Маршрутизатор R2 пересыпает ответный пакет для компьютера ПК1 маршрутизатору R1 согласно записям в своей таблице маршрутизации.
- Этап 6** Маршрутизатор R1 пересыпает пакет компьютеру ПК1 согласно записям в своей таблице маршрутизации.

В главе 21 процесс пересылки пакетов рассмотрен подробнее. Для начала представим себе, что на этапе 1, 3, 4 или 6 возникла проблема. Что произойдет в таком случае на третьем уровне и что нам даст информация о такой ситуации с точки зрения изоляции проблемы? Дальнейшая изоляция проблемы потребует дополнительного анализа третьего уровня. Тем не менее предположим, что мы не нашли проблем на уровне 3 (адреса правильны, маршрутизация работает). В таком случае придется “спуститься” на уровни 2 и 1, чтобы увидеть, почему не работает сеть.

Представим себе ситуацию, когда анализ третьего уровня выявил, что компьютер ПК1 не может отправить пакет своему *стандартному шлюзу* (default gateway), т.е. проблемы появились на первом этапе (см. рис. 10.1). Чтобы еще более четко изолировать проблему и ее причины, инженеру потребуется собрать следующую информацию:

- определить MAC-адрес компьютера ПК1 и интерфейса локальной сети маршрутизатора R1;
- идентифицировать используемые интерфейсы коммутаторов SW1 и SW2;
- определить состояние всех интерфейсов;
- проверить пересылку фрейма от компьютера ПК1 к маршрутизатору R1, не-посредственно для MAC-адреса последнего.

Собрав и проанализировав все вышеперечисленные факты, инженер, скорее всего, найдет, в чем корень проблемы, и исправит ее.

Советы по поиску и устранению неисправностей

В этой книге есть три главы, посвященные преимущественно поиску и устранению неисправностей в сетях:

- глава 10, “Поиск и устранение неисправностей в коммутаторах Ethernet”;
- глава 21, “Поиск и устранение неисправностей маршрутизации”;
- глава 23, “Конфигурирование соединений WAN”.

В главе 21 описаны методы анализа и решения проблем третьего уровня сети, обобщенный и упрощенный вариант которых показан на рис. 10.1. В текущей главе

в основном рассказывается о том, как устранять проблемы, если вы подозреваете, что они в основном связаны с технологиями локальных сетей. В главе 23 представлены методы поиска и устранения неисправностей в соединениях WAN и подробно описаны их этапы.

В указанных выше трех главах основное внимание уделяется формализованному процессу поиска и устранения неисправностей, но только как к средству достижения трех самых главных целей: описание нормального поведения сети, изоляции проблемы и определение источника проблемы. Основная цель такого формализованного подхода — изучить основные инструменты, концепции, конфигурационные команды и научить инженера анализировать сеть на основе результатов команды `show`.

Во втором томе книги описаны более сложные методы поиска и устранения неисправностей, а также рассказано, как видоизменить формализованный процесс под различные задачи. Более сложные задачи преднамеренно были вынесены во второй том потому, что когда читатель дойдет до них, он уже будет хорошо знаком со всеми технологиями уровня CCNA. Поиск и устранение неисправностей в сетях требуют знания разнообразных концепций, различных конфигураций и умения интерпретировать вывод различных команд, поэтому советы по проверке сети во втором томе даны ближе к концу каждой части — они резюмируют наиболее важные темы и демонстрируют преемственность различных технологий.

Ниже рассмотрены три важные темы, имеющие непосредственное отношение к формализованному процессу поиска и устранения неисправностей.

- *Протокол обнаружения устройств Cisco* (Cisco Discovery Protocol — CDP). Используется для проверки существующей документации сети, изучения сетевой топологии и оценки нормальной работы сети.
- Анализ состояния интерфейса. Все интерфейсы должны быть в рабочем состоянии, чтобы коммутатор мог пропустить через себя трафик. Сетевой инженер должен быть в состоянии определить, работает ли интерфейс, если нет, то найти причины отказа.
- Анализ маршрута коммутации фреймов предполагает, что специалист может проанализировать таблицу MAC-адресов и оценить, по какому маршруту (или через какой интерфейс) коммутатор перешлет фрейм.

Построение топологии сети с помощью протокола обнаружения устройств Cisco

Собственный *протокол обнаружения устройств Cisco* (Cisco Discovery Protocol — CDP) позволяет получить базовую информацию о соседних маршрутизаторах и коммутаторах, даже не зная пароль для доступа к ним. Чтобы получить информацию, маршрутизаторы и коммутаторы рассыпают сообщения CDP через все свои работающие интерфейсы. Такие сообщения содержат информацию об устройстве, которое его отправило; о других устройствах маршрутизатор или коммутатор узнает из принимаемых им аналогичных сообщений CDP.

С точки зрения процесса поиска и устранения неисправностей в сетях протокол CDP может использоваться для подтверждения или уточнения сетевой документации и схем, а также для обнаружения новых устройств и интерфейсов в сети. Обна-

ружение реальной схемы подключения устройств в сети и усовершенствование схем фактически является необходимым этапом для того, чтобы начать прогнозирование маршрутов трафика в сети.

В среде, поддерживающей многоадресатную передачу данных на канальном уровне, протокол CDP рассыпает многоадресатные фреймы; в других сетевых средах протокол CDP отправляет копию сообщения на любой известный устройству адрес канального уровня. Таким образом, любое устройство, поддерживающее протокол CDP и подключенное к общей среде с другим таким же устройством, может получить информацию о последнем.

Протокол CDP получает следующую полезную информацию о соседнем устройстве, называемом *соседом CDP* (CDP neighbor):



Информация, получаемая с помощью протокола CDP

- *идентификатор устройства* (device identifier), обычно это название устройства;
- *список адресов* (address list), представляющий собой адрес сетевого и канального уровней;
- *локальный интерфейс* (local interface) — интерфейс маршрутизатора или коммутатора, на котором была использована команда `show cdp` и через который было обнаружено соседнее устройство;
- *идентификатор порта* (port identifier) указывает, каким интерфейсом к общей среде подключено соседнее устройство (т.е. через какой порт был отправлен фрейм CDP, полученный локальным устройством);
- *список возможностей* (capabilities list) описывает тип устройства (например, соседнее устройство — это коммутатор или маршрутизатор);
- *платформа* (platform) показывает модель соседнего устройства.

В табл. 10.2 перечислены наиболее используемые варианты команды `show cdp`, отображающие информацию, указанную в списке выше.



Таблица 10.2. Варианты команды `show cdp`, используемые для получения информации о смежных устройствах

Команда	Описание
<code>show cdp neighbors [тип номер]</code>	Выводит одну строку информации для всех соседних устройств или для устройства, обнаруженного через указанный интерфейс
<code>show cdp neighbors detail</code>	Выдает подробную информацию (около 15 строк) для каждого устройства
<code>show cdp entry название</code>	Выдает ту же информацию, что и команда <code>show cdp neighbors detail</code> , но только для устройства с указанным именем (регистр символов имеет значение для имени)

Как и многие другие функции маршрутизаторов и коммутаторов, которые стандартно включены, протокол CDP создает брешь в системе безопасности. Чтобы не дать возможности атакующему получить информацию о коммутаторах сети, протокол CDP может быть легко отключен. Компания Cisco рекомендует отключать его на

тех интерфейсах, где он не очень нужен. Скорее всего, протокол CDP будет полезен только в соединениях с другими маршрутизаторами и коммутаторами, а также в интерфейсах, к которым подключены *IP-телефоны Cisco* (*Cisco IP Phone*). Этот протокол может быть включен или выключен на каждом из интерфейсов устройства с помощью команд `cdp enable` и `no cdp enable`. Команда `no cdp run` режима глобальной конфигурации устройства, соответственно, глобально выключает протокол CDP, а команда `cdp run` — включает.

На рис. 10.2 показана сеть, состоящая из двух коммутаторов, одного маршрутизатора и пары компьютеров. В примере 10.1 показаны результаты выполнения команд `show` для этой сети, перечисленных в табл. 10.2, а также нескольких команд, выдающих информацию о самом протоколе CDP, а не о соседних устройствах.

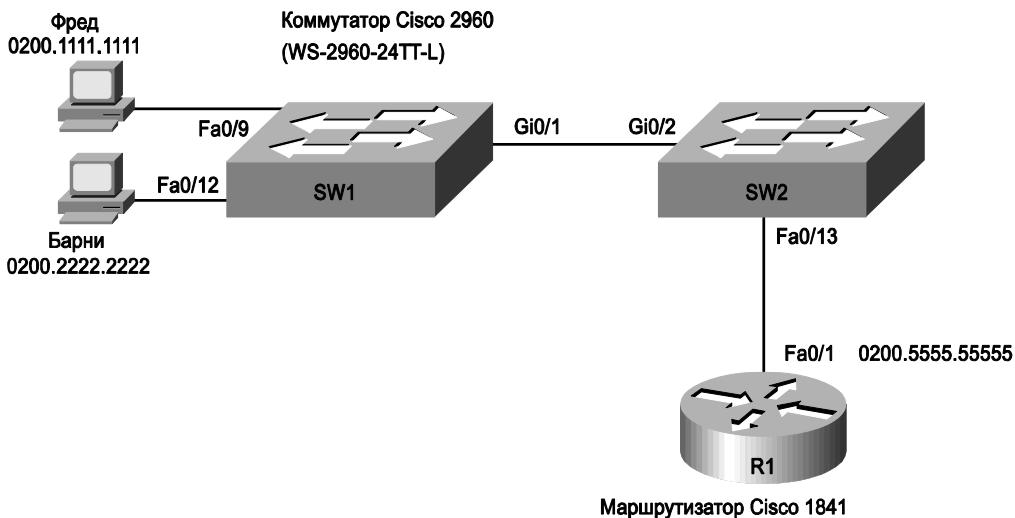


Рис. 10.2. Небольшая сеть, используемая в примерах для протокола CDP

Пример 10.1. Примеры выполнения команд `show cdp` для коммутатора SW2

```
SW2#show cdp ?
entry          Information for specific neighbor entry
interface      CDP interface status and configuration
neighbors      CDP neighbor entries
traffic        CDP statistics
|
<cr>
!
! Ниже команда show cdp neighbors выводит локальный интерфейс
! коммутатора SW2 и интерфейсы маршрутизатора R1 и коммутатора SW1
! (в колонке "port"), а также другие подробности об устройствах.
!
SW2#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID      Local Intrfce   Holdtme  Capability  Platform      Port ID

```

```

SW1      Gig 0/2      173      S I      WS-C2960-2  Gig 0/1
R1      Fas 0/13     139      R S I      1841      Fas 0/1
SW2#show cdp neighbors detail
-----
Device ID: SW1
Entry address(es):
Platform: Cisco WS-C2960-24TT-L, Capabilities: Switch IGMP
Interface: GigabitEthernet0/2, Port ID (outgoing port): GigabitEthernet0/1
Holdtime : 167 sec
Version :
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version
12.2(25)SEE2, RELEASE
    SOFTWARE (fc1)
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Fri 28-Jul-06 11:57 by yenanh
advertisement version: 2
Protocol Hello: OUI=0x00000C, Protocol ID=0x0112; payload len=27,
    value=00000000FFFFFFFFFF010221FF000
0000000000019E86A6F80FF0000
VTP Management Domain: 'fred'
Native VLAN: 1
Duplex: full
Management address(es):
! Ниже выводится информация о маршрутизаторе R1.
-----
Device ID: R1
Entry address(es):
    IP address: 10.1.1.1
Platform: Cisco 1841, Capabilities: Router Switch IGMP
Interface: FastEthernet0/13, Port ID (outgoing port): FastEthernet0/1
Holdtime : 131 sec
Version :
Cisco IOS Software, 1841 Software (C1841-ADVENTERPRISEK9-M), Version
12.4(9)T, RELEASE
    SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Fri 16-Jun-06 21:26 by prod_rel_team
advertisement version: 2
VTP Management Domain: ''
Duplex: full
Management address(es):
!
! Обратите внимание: команда show cdp entry R1 выводит ту же
! информацию, что и команда show cdp neighbors detail, но только для
! маршрутизатора R1.
SW2#show cdp entry R1
-----
Device ID: R1
Entry address(es):
    IP address: 10.1.1.1
Platform: Cisco 1841, Capabilities: Router Switch IGMP
Interface: FastEthernet0/13, Port ID (outgoing port): FastEthernet0/1
Holdtime : 176 sec
Version :
Cisco IOS Software, 1841 Software (C1841-ADVENTERPRISEK9-M), Version
12.4(9)T, RELEASE

```

```
SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Fri 16-Jun-06 21:26 by prod_rel_team

advertisement version: 2
VTP Management Domain: ''
Duplex: full
Management address(es):
SW2#show cdp
Global CDP information:
  Sending CDP packets every 60 seconds
  Sending a holdtime value of 180 seconds
  Sending CDPv2 advertisements is enabled
SW2#show cdp interfaces
FastEthernet0/1 is administratively down, line protocol is down
  Encapsulation ARPA
    Sending CDP packets every 60 seconds
    Holdtime is 180 seconds
FastEthernet0/2 is administratively down, line protocol is down
  Encapsulation ARPA
    Sending CDP packets every 60 seconds
    Holdtime is 180 seconds
!
!  Часть выводимой информации опущена
!
SW2#show cdp traffic
CDP counters :
  Total packets output: 54, Input: 49
  Hdr syntax: 0, Chksum error: 0, Encaps failed: 0
  No memory: 0, Invalid packet: 0, Fragmented: 0
  CDP version 1 advertisements output: 0, Input: 0
  CDP version 2 advertisements output: 54, Input: 49
```

В первой половине примера 10.1 можно увидеть иллюстрацию того, что описано в табл. 10.2. Команда `show cdp neighbors` выводит по одной строке ключевой информации о каждом устройстве: к какому локальному интерфейсу оно подключено, каким именно интерфейсом, модель и т.п. Например, в коммутаторе SW2 команда `show cdp neighbors` выводит запись для коммутатора SW1, в которой указано, что локальный интерфейс Gi0/2 (SW2) подключен к интерфейсу Gi0/1 коммутатора SW1 (см. также рис. 10.2). Рассматриваемая команда также выводит информацию о платформе устройства, т.е. можно видеть модель соседнего устройства компании Cisco. Владея такой базовой информацией, можно построить схему сети, подобную представленной на рис. 10.2, или подтвердить, что имеющаяся схема сети правильна.

Попробуем сравнить команды `show cdp neighbors detail` и `show cdp entry R1` (см. пример 10.1). Обе команды выводят абсолютно одинаковые сообщения за исключением того, что первая команда выводит информацию обо всех соседних устройствах, а вторая — только об одном, которое указано в командной строке. Обратите внимание: обе указанные команды выводят много дополнительной информации, в частности, полное название модели коммутатора (WS-2960-24TT-L) и IP-адрес, установленный для маршрутизатора 1841. Если бы у коммутатора SW1 был задан какой-либо адрес, он также был бы показан в выводимой командами информации.

Во второй половине примера 10.1 показаны примеры выполнения команды `show cdp` с разными параметрами, демонстрирующие их настройку и работу протокола CDP. В этих командах нет информации о соседних устройствах. Команды и их описание перечислены в табл. 10.3.

Таблица 10.3. Команды для проверки работы протокола CDP

Команда	Описание
<code>show cdp</code>	Показывает, включен ли протокол CDP глобально в устройстве, а также какие таймеры <i>обновлений</i> (update) и <i>хранения</i> информации (holdtime) используются
<code>show cdp interface [тип номер]</code>	Показывает, включен ли протокол CDP на соответствующих интерфейсах, а также какие таймеры <i>обновлений</i> (update) и <i>хранения</i> информации (holdtime) используются в этих интерфейсах
<code>show cdp traffic</code>	Показывает глобальную статистику обновлений CDP, которые были отправлены и получены устройством

Анализ состояния интерфейса на 1- и 2-м уровнях

Интерфейс коммутатора компании Cisco должен быть в рабочем состоянии, чтобы обрабатывать приходящие фреймы или пересыпать фреймы из других портов получателям. Кроме того, если интерфейс работает, иногда могут возникать ошибки и проблемы при передаче потоков трафика. Поэтому вполне очевидным этапом проверки работы, а также поиска и устранения неисправностей в сети является проверка состояния интерфейса и обнаружение перемежающихся ошибок в процессе функционирования устройства. В этом разделе описаны полезные команды группы `show`, используемые для отслеживания состояния интерфейсов коммутаторов, обнаружения причин их неработоспособности и поиска проблем в работающих портах.

Коды состояний интерфейсов и причины их неработоспособности

В коммутаторах компании Cisco используются два набора кодов состояний интерфейсов: один набор состоит из двух кодов (кодовых слов) для каждого состояния, и в нем используется то же самое соглашение о синтаксисе, что и в маршрутизаторах; второй набор включает в себя по одному коду (кодовому слову) для каждого состояния интерфейса. Оба набора кодовых слов помогут определить, работает интерфейс или нет.

Команды `show interfaces` и `show interfaces description` коммутатора выдают двухкомпонентные коды состояний интерфейса, точно так же, как и в маршрутизаторах. Такие коды описывают *состояние линии* (line status) и *состояние протокола* (protocol status) интерфейса и указывают соответственно, работает ли уровень 1 (линия) модели OSI и уровень 2 (протокол канального уровня). Для коммутаторов локальных сетей характерно, что команда показывает два одинаковых значения в обоих полях: два раза “up” (работает) или два раза “down” (не работает).

ВНИМАНИЕ!

В этой книге оба кода обычно представлены в удобной сокращенной записи, например, если уровень линии и уровень протокола работают, то состояние интерфейса записывается так: “up/up”.

Команда `show interfaces status` выводит для каждого интерфейса одну короткую строку одним кодовым словом его состояния. Такой код состояния интерфейса имеет однозначную привязку к двухкомпонентному традиционному коду состояния порта. Например, команда `show interfaces status` выдает кодовое слово состояния интерфейса “`connected`” (соединен), чтобы указать, что интерфейс находится полностью в рабочем состоянии. Это кодовое слово соответствует двухкомпонентному коду “`up/up`” (работает/работает) в командах `show interfaces` и `show interfaces description`.

Если перечисленные выше команды выдают код состояния интерфейса не `connect` или `up/up`, то это значит, что коммутатор не будет передавать и принимать фреймы через него. Для каждого из нерабочих состояний интерфейса есть небольшой набор типичных причин неработоспособности. Следует также помнить, что в сертификационном экзамене может быть приведен однокомпонентный код или двухкомпонентный код состояния из двух наборов сообщений, следовательно, нужно быть готовым к таким вопросам и помнить все коды на память. Различные комбинации кодов состояния интерфейсов и наиболее распространенные причины неработоспособности перечислены в табл. 10.4.

Таблица 10.4. Коды состояния интерфейсов коммутаторов локальных сетей



Состояние линии	Состояние протокола	Состояние интерфейса	Типичные причины
Administratively Down	Down	Disabled	В конфигурации интерфейса введена команда <code>shutdown</code>
Down	Down	Notconnect	Кабель не подключен; кабель нерабочий; использован кабель с неправильным расположением выводов; настройки скорости на двух концах соединения не совпадают; с одной стороны соединения у устройства выключено питание или введена команда <code>shutdown</code> в конфигурации интерфейса
Up	Down	Notconnect	Это состояние (<code>up/down</code>) в коммутаторах локальных сетей практически не встречается
Down	Down (err-disabled)	Err-disabled	Технология безопасности порта (port security) выключила порт в связи с нарушением режима безопасности
Up	Up	Connected	Интерфейс работает normally

Практически все причины состояния интерфейса `notconnect` (не подключен) были перечислены выше в этой главе. Например, чтобы найти специфические проблемы в подключении, следует помнить наизусть расположение выводов кабелей, показанное в главе 3, и сравнить имеющийся кабель с ним. Самой сложной ситуацией с точки зрения процесса поиска и устранения неисправностей является та, в которой скорость и режим дуплексности интерфейсов не совпадают.

Проблемы при несовпадении дуплексности и скорости интерфейсов

Интерфейсы коммутаторов могут получать настройки скорости и дуплексности из разных источников. Зачастую интерфейсы, подключаемые к медной среде передачи данных, могут работать с разными скоростями и разными режимами дуплекс-

ности за счет использования стандартного процесса автоматического согласования канала (стандарты IEEE 802.3X). Такие интерфейсы, как и *сетевые карты* (Network Interface Card — NIC), также могут быть явно настроены для определенного режима работы и не использовать автосогласование. В коммутаторах и маршрутизаторах компании Cisco скорость задается командой конфигурирования интерфейса `speed {10 | 100 | 1000}`, а режим дуплексности канала — командой `duplex {half | full}`. Следует помнить, что явное указание скорости и дуплексности интерфейса отключает процесс автосогласования характеристик для интерфейса устройства.

В выводимой командами `show interfaces` и `show interfaces status` информации показаны настройки скорости и дуплексность порта (пример 10.2).

Пример 10.2. Отображение настроек скорости и дуплексности интерфейсов коммутаторов

```
SW1#show interfaces status
Port Name Status Vlan Duplex Speed Type
Fa0/1 notconnect 1 auto auto 10/100BaseTX
Fa0/2 notconnect 1 auto auto 10/100BaseTX
Fa0/3 notconnect 1 auto auto 10/100BaseTX
Fa0/4 connected 1 a-full a-100 10/100BaseTX
Fa0/5 connected 1 a-full a-100 10/100BaseTX
Fa0/6 notconnect 1 auto auto 10/100BaseTX
Fa0/7 notconnect 1 auto auto 10/100BaseTX
Fa0/8 notconnect 1 auto auto 10/100BaseTX
Fa0/9 notconnect 1 auto auto 10/100BaseTX
Fa0/10 notconnect 1 auto auto 10/100BaseTX
Fa0/11 connected 1 a-full 10 10/100BaseTX
Fa0/12 connected 1 half 100 10/100BaseTX
Fa0/13 connected 1 a-full a-100 10/100BaseTX
Fa0/14 disabled 1 auto auto 10/100BaseTX
Fa0/15 notconnect 3 auto auto 10/100BaseTX
Fa0/16 notconnect 3 auto auto 10/100BaseTX
Fa0/17 connected 1 a-full a-100 10/100BaseTX
Fa0/18 notconnect 1 auto auto 10/100BaseTX
Fa0/19 notconnect 1 auto auto 10/100BaseTX
Fa0/20 notconnect 1 auto auto 10/100BaseTX
Fa0/21 notconnect 1 auto auto 10/100BaseTX
Fa0/22 notconnect 1 auto auto 10/100BaseTX
Fa0/23 notconnect 1 auto auto 10/100BaseTX
Fa0/24 notconnect 1 auto auto 10/100BaseTX
Gi0/1 connected trunk full 1000 10/100/1000BaseTX
Gi0/2 notconnect 1 auto auto 10/100/1000BaseTX

SW1#show interfaces fa0/13
FastEthernet0/13 is up, line protocol is up (connected)
Hardware is Fast Ethernet, address is 0019.e86a.6f8d (bia 0019.e86a.6f8d)
MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Full-duplex, 100Mbps, media type is 10/100BaseTX
input flow-control is off, output flow-control is unsupported
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:05, output 00:00:00, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
```

```
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
    85022 packets input, 10008976 bytes, 0 no buffer
    Received 284 broadcasts (0 multicast)
    0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 watchdog, 281 multicast, 0 pause input
    0 input packets with dribble condition detected
    95226 packets output, 10849674 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 PAUSE output
    0 output buffer failures, 0 output buffers swapped out
```

Обе показанные в примере команды могут быть полезны при проверке работоспособности сети, только с помощью команды `show interfaces status` можно обнаружить, как коммутатор определяет настройки скорости и дуплексности линии. В выводимой этой командой информации автосогласование указывается с помощью приставки `a-` для интерфейса, например, надпись `a-full` сигнализирует о том, что дуплексный режим работы был автоматически согласован, а просто `full` — о том, что такой режим был задан вручную в конфигурации интерфейса. В примере 10.2 выделены цветом строки для двух интерфейсов: для порта Fa0/12 настройки линии были указаны вручную, а порт Fa0/13 автоматически согласовал режим работы. Обратите внимание на то, что с помощью команды `show interfaces fa0/13` (без параметра `status`) можно просто посмотреть, какие параметры дуплексности и скорости используются для интерфейса FastEthernet0/13, но ничего нельзя сказать о том, как они были получены интерфейсом.

Когда стандарт IEEE автоматического согласования характеристик интерфейса поддерживается обоими устройствами на концах канала, они будут устанавливать максимальную поддерживаемую ими скорость. Аналогично оба устройства сначала попробуют установить дуплексный режим работы, а если это не удастся, то они согласуют полудуплексный канал. Если же одно из устройств использует автосогласование, а второе нет, то устройство с автоматическим согласованием канала будет пытаться установить режим дуплексности на основании текущей скорости интерфейса. Стандартными комбинациями параметров являются следующие:

Стандарты IEEE автосогласования характеристик интерфейсов



- если скорость не известна, будет использоваться скорость 10 Мбит/с и полу-дуплексный режим;
- если скорость каким-либо образом была определена и равна 10 или 100 Мбит/с, стандартно будет использоваться полудуплексный режим;
- если скорость каким-либо образом была определена и равна 1000 Мбит/с, стандартно будет использоваться дуплексный режим.

ВНИМАНИЕ!

Интерфейсы Ethernet со скоростями 1 Гбит/с и выше всегда используют дуплексный режим работы.

Коммутаторы компании Cisco могут определять скорость с помощью нескольких методов, даже если автосогласование не работает. Устройство может использовать скорость, указанную с помощью команды `speed`, — это первый метод. Второй метод заключается в том, что если автосогласование стандарта IEEE не срабатывает, то коммутатор может автоматически подбирать скорость, используя электрические сигналы в канале, чтобы определить конфигурацию дистанционного устройства.

Представим себе, что интерфейс `Gi0/2` коммутатора `SW2` (рис. 10.3) был настроен с использованием команд `speed 100` и `duplex full` (что для гигабитовых интерфейсов делать крайне не рекомендуется). Коммутатор `SW2` будет использовать указанные характеристики и отключит автосогласование стандарта IEEE, поскольку скорость и дуплексность интерфейса указаны явно. Если же в коммутаторе `SW1` для интерфейса `Gi0/1` не задана скорость командой `speed`, он все равно может распознать скорость (100 Мбит/с), несмотря на то, что устройство `SW2` не использует автосогласование, и будет ее использовать. В примере 10.3 показан результат выполнения команды `show` для коммутатора `SW1` в рассматриваемой ситуации.

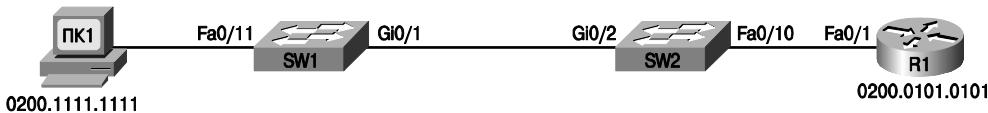


Рис. 10.3. Пример сети для автоконфигурации скорости и дуплексности интерфейса

Пример 10.3. Настройки дуплексности и скорости интерфейса коммутатора SW1

```
SW1#show interfaces gi0/1 status
```

Port	Name	Status	Vlan	Duplex	Speed	Type
Gi0/1		connected	trunk	a-half	a-100	10/100/1000BaseTX

В настройках скорости и дуплексности интерфейса видна приставка `a-`, свидетельствующая о том, что характеристики были выставлены за счет автосогласования. В данном случае сначала была определена автоматически скорость, потом операционная система устройства установила соответствующий ей режим дуплексности для интерфейса. Коммутатор `SW1` выставил скорость без использования автосогласования скорости стандарта IEEE, поскольку характеристики были явно указаны в конфигурации коммутатора `SW2` и таким образом автосогласование для него было отключено. Как и предполагалось, устройство `SW1` выставило стандартный режим дуплексности (полудуплексный) для порта согласно стандартным рекомендациям IEEE для интерфейсов со скоростью 100 Мбит/с.

Рассмотренный выше пример также иллюстрирует одну сложную проблему несоответствия дуплексности интерфейсов: коммутатор `SW1` работает в полудуплексном режиме, а `SW2` — в дуплексном. Обнаружить несовпадение режима дуплексности крайне проблематично и намного сложнее, чем выявить несовпадение скоростей, поскольку *коэффициенты дуплексности не совпадают на концах соединения Ethernet, интерфейс коммутатора все равно будет сообщать о рабочем состоянии, т.е. connect (или up/up в другой команде)*. Такой интерфейс будет работать, но, скорее всего, очень плохо, производительность его будет невысока и для него будут характерны

перемежающиеся отказы и проблемы. Причиной нестабильной работы интерфейса является использование в полудуплексном режиме работы логики *множественного доступа с обнаружением коллизий* (Carrier Sense Multiple Access with Collision Detection — CSMA/CD), которая ожидает окончания приема фрейма, чтобы начать собственную передачу, и предполагает, что в противном случае возникнет коллизия. В действительности коллизии в таком варианте работы соединения физически не возникнет, но коммутатор-то этого не знает! Вторая проблема состоит в том, что при наличии интенсивного трафика интерфейс коммутатора будет сигнализировать о нормальном подключенном состоянии, но трафик через него не будет передаваться или будет передаваться с ошибками.

Чтобы обнаружить несоответствие режимов дуплексности на концах канала, следует проверить настройки на обоих интерфейсах, посмотреть, увеличиваются ли счетчики *коллизий* (collision) и *запоздалых коллизий* (late collision), как показано в следующем разделе.

Проблемы уровня 1 в работающих интерфейсах

Некоторые проблемы первого уровня могут привести к тому, что интерфейс не переходит в подключенное состояние (“connect” или “up/up”). Если же интерфейс все же переходит в рабочее состояние, коммутатор пытается поддерживать его в этом режиме и создает для него различные счетчики. Такие счетчики порта могут помочь идентифицировать проблемы в интерфейсе, находящемся в подключенном состоянии (connect). В текущем разделе объясняны основные характеристики, которые следует отслеживать, и описано несколько наиболее часто встречающихся проблем.

Прежде всего рассмотрим несколько основных причин, почему фреймы Ethernet могут передаваться с ошибками. Когда такой фрейм передается по кабелю UTP, электрический сигнал может быть искажен. Кабель может быть поврежден, например, если он лежит под ковром на полу. Пользователь, которому посчастливилось сидеть на офисном стуле с колесиками, может периодически проезжать по такому кабелю и “улучшить” его качество. Сигнал в таком поврежденном кабеле может как просто затухать, так и вообще пропадать. Кроме того, в современном мире существует множество источников электромагнитного излучения, которые приводят к возникновению *интерференции* в кабеле (Electromagnetic Interference — EMI), например, проложенный рядом кабель питания будет вызывать интенсивную интерференцию и помехи. Интерференция очень сильно влияет на форму, интенсивность и характеристики сигнала в кабеле Ethernet.

Независимо от первичной причины искажения сигнала в кабеле, принимающее устройство может получить фрейм, биты которого отличаются от начального значения. Такие фреймы не пройдут через алгоритм контроля ошибок, реализуемый с использованием поля *контрольной суммы фрейма* (Frame Check Sequence — FCS) в концевике фрейма Ethernet (см. главу 3). Принимающее устройство отбрасывает такой фрейм и относит его к одной из стандартных ошибок. Коммутаторы компании Cisco обычно такие ошибки отображают как ошибки CRC (Cyclic Redundancy Check — контроль с помощью циклического избыточного кода) — это устаревшее название алгоритма FCS (пример 10.4).

Пример 10.4. Счетчики интерфейса для определения проблем уровня 1

```
SW1#show interfaces fa0/13
! Часть выводимых строк опущена для краткости
Received 284 broadcasts (0 multicast)
  0 runts, 0 giants, 0 throttles
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
  0 watchdog, 281 multicast, 0 pause input
  0 input packets with dribble condition detected
  95226 packets output, 10849674 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 PAUSE output
  0 output buffer failures, 0 output buffers swapped out
```

Кроме того, следует помнить, чем отличаются *коллизии* (collision) от *запоздалых коллизий* (late collision); оба типа ошибок отслеживаются счетчиками интерфейсов коммутаторов компании Cisco. Коллизии — это нормальный режим работы интерфейса в полудуплексном состоянии при использовании алгоритма CSMA/CD, следовательно, если счетчик коллизий интерфейса увеличивается, это не означает, что в канале есть какие-либо проблемы. Тем не менее, если в процессе разработки и развертывания сети стандарты были соблюдены, все коллизии должны появляться при передаче заголовка фрейма, т.е. до конца 64-го байта. Если же коммутатор уже успел передать 64 байта фрейма и после этого обнаружил коллизию, то такая коллизия называется *запоздалой* (late collision), и устройство увеличивает именно счетчик запоздалых коллизий для интерфейса. Помимо этого, коммутатор посыпает *сигнал оповещения о коллизии* (jamming signal), как предусмотрено алгоритмом CSMA/CD, приостанавливает передачу на случайный период времени и только после его истечения пробует повторно передать данные. Обратите внимание: счетчики коллизий размещены в разделе исходящих пакетов (output) для интерфейса.

Три наиболее распространенных проблемы локальных сетей (LAN) могут быть обнаружены с помощью указанных счетчиков: избыточное количество интерфейсов (т.е. передающих станций) в сети, несоответствие настроек дуплексности и сбойные пакеты (jabber). Избыточное количество интерфейсов в кабельном сегменте может также привести к увеличению входного счетчика ошибок, в частности счетчика CRC. Если такой счетчик ошибок увеличивается, а счетчик коллизий нет, то проблема может быть в интерференции сигнала в кабеле. (Коммутатор также классифицирует каждый фрейм с коллизией как одну из ошибок приема фрейма.)

Несоответствие настроек дуплексности и сбойные фреймы могут быть косвенно обнаружены по счетчикам коллизий и запоздалых коллизий. Сбойные фреймы (jabber) возникают в том случае, когда сетевая карта (NIC) игнорирует правила технологии Ethernet и передает фрейм за фреймом без паузы между ними. В таком случае оба счетчика, обычных и запоздалых коллизий, будут увеличиваться. В частности, неустойчивой считается сеть, в которой счетчик коллизий показывает, что 0,1% от передаваемых фреймов подверглись коллизиям. Убедиться в том, что настройки дуплексности не совпадают, можно с помощью команды show interface, пример вывода которой был показан выше, в разделе “Проблемы при несовпадении дуплексности и скорости интерфейсов”. Устранение неполадок, вызывающих сбойные фреймы в сети, намного сложнее и требует специализированных инструментов для поиска проблем в кабелях локальной сети.

ВНИМАНИЕ!

Чтобы оценить в процентном соотношении количество коллизий в интерфейсе, разделите значение счетчика коллизий, “collisions”, на значение счетчика отправленных пакетов “packets output” (см. выделенные строки в примере 10.4).

Увеличение значения счетчика запоздалых коллизий обычно означает одну из следующих проблем:

- интерфейс подключен к сегменту (к так называемому домену коллизий), в котором длина кабеля превышает разрешенную стандартом Ethernet;
- в конфигурации интерфейса указан полудуплексный режим работы, а у устройства на другом конце кабеля указан дуплексный режим.

В табл. 10.5 перечислены основные проблемы в интерфейсах, в том числе когда интерфейс находится в рабочем состоянии (“connect” или “up/up”).

Таблица 10.5. Основные проблемы уровня 1 в локальных сетях



Проблема	Счетчики, сигнализирующие о проблеме	Наиболее распространенные причины
Высокий уровень шума	Высокое значение счетчика входных ошибок, низкое — счетчика коллизий	Используется кабель неправильной категории (Cat 5, 5E, 6), кабель поврежден, электромагнитная интерференция (EMI)
Коллизии	Наблюдается больше, чем 0,1% коллизий	Дуплексный режим неправильно настроен (можно обнаружить рост счетчика на полудуплексном интерфейсе), большое количество сбойных фреймов, атака DoS
Запоздалые коллизии	Увеличивается значение счетчика запоздалых коллизий	Очень большой домен коллизий или длина кабеля превышает допустимую в стандарте, несоответствие режима дуплексности

Анализ маршрута коммутации фреймов на основе таблиц MAC-адресов

Как уже упоминалось в главе 7, коммутаторы обнаруживают MAC-адреса отправителей во входящих фреймах и заносят их в специализированные таблицы, чтобы в перспективе выполнять перенаправление и фильтрацию для всех входящих в устройство фреймов. Чтобы представлять себе, как именно данный коммутатор будет обрабатывать фрейм Ethernet и в какой интерфейс он его перенаправит, читатель должен уметь просматривать и интерпретировать таблицу MAC-адресов коммутаторов компании Cisco.

Команда `show mac address-table` показывает содержимое таблицы MAC-адресов коммутатора. Вывод этой команды содержит как некоторые дополнительные статические адреса, а именно MAC-адреса коммутатора, статически заданные адреса, например, те, которые были указаны для технологии безопасности портов (*port security*), так и динамически изученные устройством. Если нужно просмотреть только динамические записи MAC-адресов в таблице коммутации, следует использовать команду с дополнительным параметром `show mac address-table dynamic`.

Формализованный процесс поиска и устранения неисправностей начинается с попытки предсказать, что должно происходить в сети в нормальных условиях, а потом предполагает попытку изолирования проблемы, которая не дает нормально передавать потоки данных. В качестве примера обратитесь к рис. 10.2 и попробуйте записать на бумаге таблицы MAC-адресов для всех коммутаторов. Нужно записать физические адреса обоих компьютеров, а также MAC-адрес интерфейса Fa0/1 маршрутизатора R1. Далее следует представить себе, какие интерфейсы будут использоваться для передачи фреймов компьютеру Барни, маршрутизатору R1 и другим устройствам в сети. Несмотря на то что вроде бы маршруты следования фреймов вполне очевидны в этом примере, это полезная тренировка, которая позволит научиться моделировать поведение сети, а также представить, как будут выглядеть таблицы адресов коммутаторов. В примере 10.5 показаны таблицы MAC-адресов обоих коммутаторов, приведенных на рис. 10.2, по ним можно проверить, правильно ли было смоделировано поведение сетевых устройств.

Следующий этап в процессе устранения неисправностей в сетях заключается в изоляции проблем при передаче фреймов. В примере 10.5 показаны команды для небольшой сети (см. рис. 10.2), свидетельствующие о том, что проблем при передаче данных нет. Таблицы адресов для коммутаторов SW1 и SW2 выглядят так, как и ожидалось. Для интерфейса Fa0/9 коммутатора SW1 настроена технология безопасности (port security), т.е. MAC-адрес 0200.1111.1111 (адрес компьютера Фреда) добавлен в таблицу статических адресов, чтобы показать разницу между динамически изученным и статически заданным MAC-адресами.

Пример 10.5. Таблицы MAC-адресов коммутаторов SW1 и SW2

```
SW1#show mac address-table
      Mac Address Table
```

Vlan	Mac Address	Type	Ports
All	0100.0ccc.cccc	STATIC	CPU
All	0100.0ccc.cccc	STATIC	CPU
All	0180.c200.0000	STATIC	CPU
All	0180.c200.0001	STATIC	CPU
All	0180.c200.0002	STATIC	CPU
All	0180.c200.0003	STATIC	CPU
All	0180.c200.0004	STATIC	CPU
All	0180.c200.0005	STATIC	CPU
All	0180.c200.0006	STATIC	CPU
All	0180.c200.0007	STATIC	CPU
All	0180.c200.0008	STATIC	CPU
All	0180.c200.0009	STATIC	CPU
All	0180.c200.000a	STATIC	CPU
All	0180.c200.000b	STATIC	CPU
All	0180.c200.000c	STATIC	CPU
All	0180.c200.000d	STATIC	CPU
All	0180.c200.000e	STATIC	CPU
All	0180.c200.000f	STATIC	CPU
All	0180.c200.0010	STATIC	CPU
All	ffff.ffff.ffff	STATIC	CPU
1	0019.e859.539a	DYNAMIC	Gi0/1

! Три записи в таблице ниже: компьютер Фреда -
 ! статически указан в конфигурации для режима безопасности (port
 ! security), компьютер Барни (динамически определен)
 ! и MAC-адрес маршрутизатора R1 (динамически определен).

```
!
1      0200.1111.1111    STATIC    Fa0/9
1      0200.2222.2222    DYNAMIC   Fa0/12
1      0200.5555.5555    DYNAMIC   Gi0/1
Total Mac Addresses for this criterion: 24
!
! Следующая команда показывает только динамически определенные
! MAC-адреса, поэтому в ней нет адреса компьютера Фреда, поскольку он
! считается статически заданным согласно настройкам режима
! безопасности коммутатора.
!
SW1#show mac address-table dynamic
  Mac Address Table
-----
Vlan      Mac Address      Type      Ports
----      -----
1        0019.e859.539a    DYNAMIC   Gi0/1
1        0200.2222.2222    DYNAMIC   Fa0/12
1        0200.5555.5555    DYNAMIC   Gi0/1
Total Mac Addresses for this criterion: 3
!
=====
!
! Та же самая команда на коммутаторе SW2 выдает те же MAC-адреса,
! но чтобы их "достигнуть", используются другие интерфейсы.
SW2#show mac address-table dynamic
  Mac Address Table
-----
Vlan      Mac Address      Type      Ports
----      -----
1        0019.e86a.6f99    DYNAMIC   Gi0/2
1        0200.1111.1111    DYNAMIC   Gi0/2
1        0200.2222.2222    DYNAMIC   Gi0/2
1        0200.5555.5555    DYNAMIC   Fa0/13
Total Mac Addresses for this criterion: 4
! Выделенный выше MAC-адрес 0200.5555.5555 и строка таблицы будут
! подробно объяснены ниже.
```

В процессе моделирования того, какие MAC-адреса будут присутствовать в таблицах коммутаторов, следует представить себе, как именно будет передаваться фрейм с одного конца локальной сети на другой, и после этого записать, через какие порты коммутатора он будет проходить. Например, когда компьютер Барни пересыпает фрейм маршрутизатору R1, он попадет в коммутатор SW1 через интерфейс Fa0/12, следовательно, у коммутатора будет запись в таблице адресов о том, что MAC-адрес Барни 0200.2222.2222 связан с портом Fa0/12. Коммутатор SW1 отправит фрейм от компьютера Барни коммутатору SW2 в интерфейс Gi0/2, поэтому в таблице адресов SW2 также будет присутствовать MAC-адрес компьютера Барни (0200.2222.2222), и он будет связан с портом Gi0/2.

ВНИМАНИЕ!

Таблица MAC-адресов в примере 10.5 также содержит некоторое количество адресов, помеченных словом “CPU” (центральный процессор). Эти записи описывают служебные адреса коммутатора, используемые для управляющих протоколов, таких как CDP или STP. Такие записи таблицы адресов информируют коммутатор о том, что соответствующие им фреймы нужно отправить центральному процессору (CPU) устройства на обработку.

После того как содержимое таблиц адресов было смоделировано, следует проверить, что в действительности происходит в коммутаторах, как описано в следующем разделе.

Анализ маршрута фреймов

Чтобы определить, по какому маршруту передаются фреймы в рассматриваемой сети, следует вспомнить несколько основных моментов. Как было сказано выше, в этой книге подразумевается, что магистральные каналы (trunk) и сети VLAN не используются. Данное утверждение означает, что все интерфейсы работают в режиме доступа к сети (access), т.е. все они привязаны к одной и той же сети VLAN. Итак, несмотря на то, что в примере 10.5 нет соответствующего вывода, команда `show vlan brief` покажет, что все интерфейсы всех коммутаторов привязаны к сети VLAN 1.

Процесс коммутации фреймов можно описать в виде нескольких этапов.



Описание этапов передачи фреймов коммутаторами

- Этап 1** Определить, в какую сеть VLAN должен быть отправлен фрейм. Для интерфейсов, работающих в режиме доступа к сети, используется идентификатор, который связан с входным интерфейсом.
- Этап 2** Найти MAC-адрес получателя в таблице адресов устройства. Поиск адреса осуществляется только для указанной (на этапе 1) сети VLAN. Если MAC-адрес получателя:
 - а) найден (и это одноадресатный адрес — unicast), то следует переслать фрейм только через тот интерфейс, который указан в записи таблицы адресов;
 - б) не найден (и это одноадресатный адрес — unicast), то разослать фрейм через все порты (кроме того порта, откуда он пришел) в заданной сети VLAN;
 - в) это широковещательный (broadcast) или многоадресатный (multicast) адрес, разослать фрейм через все порты (кроме того порта, откуда он пришел) в заданной сети VLAN.

ВНИМАНИЕ!

В главе 3 второго тома процесс коммутации фреймов описан намного более подробно, в том числе с учетом влияния сетей VLAN, магистральных соединений и протокола STP на процесс пересылки данных.

Руководствуясь описанным выше процессом, предположим, что компьютер Барни отправил фрейм стандартному шлюзу, R1 (адрес 0200.5555.5555). Используя ту же логику, опишем процесс передачи для этого случая.

- Этап 1** Коммутатор SW1 получает фрейм через интерфейс Fa0/12 и определяет, что он связан с сетью VLAN 1.
- Этап 2** Коммутатор SW1 ищет в таблице MAC-адресов запись для адреса 0200.5555.5555 для соответствующей сети VLAN (VLAN 1) и интерфейса.
 - а) Коммутатор SW1 находит запись, которая связана с виртуальной сетью VLAN 1, определяет исходящий интерфейс, Gi0/1, и отправляет фрейм через него.

На данном этапе фрейм с адресом отправителя 0200.2222.2222 (компьютер Барни) передается коммутатору SW2. К нему следует применить ту же логику, что и раньше, и описать его действия, как показано ниже.

Этап 1 Коммутатор SW2 получает фрейм через интерфейс Gi0/2 и определяет, что он связан с сетью VLAN 1.

Этап 2 Коммутатор SW2 ищет в таблице MAC-адресов запись для адреса 0200.5555.5555 для соответствующей сети VLAN (VLAN 1) и интерфейса.

а) Коммутатор SW1 находит запись, которая связана с сетью VLAN 1, определяет исходящий интерфейс, Fa0/13, и отправляет фрейм через него.

На данном этапе интересующий нас фрейм передается по кабелю Ethernet от коммутатора SW2 к маршрутизатору R1.

Режим безопасности порта и фильтрация фреймов

Откровенно говоря, в реальной жизни редко приходится мысленно прослеживать путь фрейма от одного устройства к другому через коммутаторы LAN. Тем не менее в сертификационном экзамене могут попадаться вопросы, связанные с логикой передачи данных коммутатором.

При прослеживании пути фрейма, полученного через коммутаторы LAN, следует учитывать, что используемые фильтры могут предотвратить передачу фрейма. Даже когда открыты все интерфейсы, фреймы могут отбрасывать фильтры различных видов. Например, коммутаторы LAN могут использовать такие фильтры, как *справки управления доступом* (Access Control List — ACL), осуществляющие фильтрацию на основании MAC-адресов отправителя и получателя, отбрасывая некоторых фреймы. Кроме того, маршрутизаторы могут фильтровать пакеты IP, используя списки ACL IP. (Обратите внимание на то, что единственными списками ACL,ключенными в экзамене CCNA, являются списки ACL маршрутизатора, рассматриваемые в главах 7 и 8 второго тома.)

Кроме того, защита порта, которая тоже рассматривается в этой книге, также фильтрует фреймы. В некоторых случаях вы можете сразу сказать, что это защита порта приняла меры, но в других случаях доказательства не так очевидны. С заданным по умолчанию режимом shutdown фильтрация вполне очевидна, поскольку защита порта реагирует на нарушение завершением работы интерфейса. Но при задании режима protect (защита) или restrict (ограничение) коммутатор будет отбрасывать “неправильный” трафик, но оставит порт в нормальном рабочем состоянии (connect или up/up). Поэтому простые команды show interface или show interface status не помогут выяснить причину проблем.

Вернемся, например, к рис. 10.2, где компьютер Барни соединен с портом Fa0/12 коммутатора SW1. Предположим, компьютер Барни работает хорошо и посыпает пакеты IP, используя свой MAC-адрес 0200.2222.2222 как адрес отправителя фреймов, которые инкапсулируют эти пакеты. Затем кто-то настраивает защиту порта на интерфейсе Fa0/12 коммутатора SW1, установив режим при нарушении protect, и этой конфигурации MAC-адрес Барни не разрешен. В результате фреймы с MAC-адресом отправителя Барни будут считаться нарушением.

Что же произойдет? Коммутатор SW1 теперь будет отбрасывать все фреймы с MAC-адресом Барни. Но интерфейсы коммутатора SW1 не отключены. Быстрая проверка коммутатора SW1 командой show interfaces или show interfaces status не покажет изменений и не предоставит никаких свидетельств произошедшего. Для поиска свидетельств того, что посланные Барни фреймы отбрасывает защита порта, необходимо проверить защиту (show port-security interface).

Подготовка к экзамену

Повторите все ключевые темы

Повторите все ключевые темы данной главы, помеченные пиктограммой “Ключевая тема”. Ключевые темы и соответствующие им страницы перечислены в табл. 10.6.

Таблица 10.6. Ключевые темы главы 6

Элемент	Описание	Страница
Список	Информация, получаемая с помощью протокола CDP	310
Табл. 10.2	Варианты команды show cdp, используемые для получения информации о смежных устройствах	310
Табл. 10.4	Коды состояния интерфейсов коммутаторов локальных сетей	315
Список	Стандарты IEEE автосогласования характеристик интерфейсов	317
Табл. 10.5	Основные проблемы уровня 1 в локальных сетях	321
Список	Описание этапов передачи фреймов коммутаторами	324

Заполните таблицы и списки по памяти

Распечатайте приложение М (Appendix L) с компакт-диска или его раздел, относящийся к этой главе, и заполните таблицы и списки по памяти. В приложении Н (Appendix M) приведены заполненные таблицы и списки для самоконтроля.

Ключевые термины

Дайте определения перечисленных ниже терминов и проверьте правильность их написания в списке терминов:

сосед CDP (CDP neighbor), рабочее состояние интерфейса (“up/up”), отключение из-за ошибок (error disabled), изоляция проблемы (problem isolation), основная причина неисправности (root cause).

Список команд

В табл. 10.7 и 10.8 приведен список команд этой главы, а также даны их короткие описания. В главах 8 и 9 были перечислены команды, также имеющие отношение к темам данной главы, тем не менее их следует искать в конце соответствующих глав.

Таблица 10.7. Команды для конфигурирования коммутаторов Catalyst 2950

Команда	Описание
shutdown	Команды подрежима конфигурирования интерфейсов для выключения и включения интерфейса соответственно
no shutdown	
switchport port-security violation {protect restrict shutdown}	Команда подрежима конфигурирования интерфейса, указывающая, что необходимо предпринять, если фрейм с неразрешенным MAC-адресом пришел в порт с включенным режимом безопасности

Окончание табл. 10.7

Команда	Описание
cdp run	Команды режима глобального конфигурирования для включения и выключения протокола CDP на всем устройстве
no cdp run	
cdp enable	Команды подрежима конфигурирования интерфейсов для включения и выключения протокола CDP в определенном интерфейсе
no cdp enable	
speed {10 100 1000}	Команда подрежима конфигурирования интерфейса для установки скорости передачи данных вручную
duplex {auto full half}	Команда подрежима конфигурирования интерфейса для установки режима дуплексности вручную

В табл. 10.8 приведен список команд для поиска и устранения неисправностей.

Таблица 10.8. Команды для поиска и устранения неисправностей

Команда	Описание
show mac address-table [dynamic static] [address <i>аппаратный_адрес</i>] [interface <i>интерфейс</i>] [vlan <i>сеть_vlan</i>]	Показывает таблицу MAC-адресов устройства
show port-security [interface <i>интерфейс</i>] [address]	Отображает настройки режима безопасности интерфейса
show cdp neighbors [тип номер]	Выводит по одной строке краткой информации для каждого соседнего устройства или информацию об устройстве, доступном через указанный в команде интерфейс
show cdp neighbors detail	Выводит подробную информацию (около 15 строк) по каждому соседнему устройству
show cdp entry <i>имя_устройства</i>	Показывает ту же информацию, что и команда show cdp neighbors detail, но для одного указанного в параметре команды устройства
show cdp	Сообщает, включен ли протокол CDP глобально, и показывает стандартные таймеры рассылки обновлений и хранения информации
show cdp interface [тип номер]	Сообщает, включен ли протокол CDP в указанном интерфейсе, и показывает стандартные таймеры рассылки обновлений и хранения информации для этого интерфейса
show cdp traffic	Показывает статистику отправленных и полученных сообщений CDP
show interfaces [тип номер]	Показывает подробную информацию о состоянии интерфейса, настройках и его счетчиках
show interfaces status [тип номер]	Показывает краткую информацию о состоянии и настройках интерфейса, в том числе скорость и дуплексный режим, а также сообщает о том, были ли параметры автоматически согласованы

В этой главе...

- **Концепции беспроводных сетей.** Посвящен теоретическим основам передачи данных с помощью радиоволн по стандартам беспроводных локальных сетей.
- **Развертывание беспроводных сетей.** Описаны этапы развертывания малых беспроводных сетей без привязки к оборудованию какого-либо производителя.
- **Безопасность беспроводных сетей.** Описаны различные методы обеспечения безопасности беспроводных сетей и их развитие.

ГЛАВА 11

Беспроводные локальные сети

В предыдущих главах были подробно рассмотрены локальные сети Ethernet (проводные). Сегодня такие сети, несомненно, играют самую важную роль в сетевых технологиях, тем не менее, есть еще один тип пользовательского подключения, который приобретает с каждым годом все большую популярность — беспроводные локальные сети. В беспроводных сетях пользователи могут обмениваться информацией без использования каких-либо кабелей, следовательно, в таких сетях можно работать с любыми мобильными устройствами, и сами сети дешевле, поскольку исключаются затраты на прокладку кабельной системы, материалы и кабели. В этой главе описаны базовые концепции, стандарты, процедуры установки и методы обеспечения безопасности для наиболее распространенных технологий беспроводных сетей.

Контрольные вопросы: знаете ли вы уже темы главы

Этот раздел предназначен для того, чтобы читатель мог предварительно оценить свои знания и решить, нужно ли ему читать главу целиком. Если ответы на девять из десяти вопросов даны правильно, можно сразу же перейти к последнему разделу “Подготовка к экзамену”. Основные темы этой главы и предварительных контрольных вопросов перечислены в табл. 11.1. Отвечая на контрольные вопросы и используя таблицу, читатель сможет достаточно точно определить свои знания в той или иной области. Ответы на вопросы приведены в приложении А.

Таблица 11.1. Темы контрольных вопросов

Основная тема	Номера вопросов
Концепции беспроводных сетей	1–4
Развертывание беспроводных сетей	5–7
Безопасность беспроводных сетей	8, 9

1. В каком из стандартов IEEE беспроводных сетей используется только полоса частот U-NII (5,4 ГГц)?
 - a) 802.11a.
 - б) 802.11b.
 - в) 802.11g.
 - г) 802.11i.

2. В каком из перечисленных ниже вариантов указана правильная комбинация стандарта IEEE, метода и скорости передачи данных для двух беспроводных устройств?
 - а) 802.11b, модуляция OFDM, 54 Мбит/с.
 - б) 802.11g, модуляция OFDM, 54 Мбит/с.
 - в) 802.11a, модуляция DSSS, 54 Мбит/с.
 - г) 802.11a, модуляция DSSS, 11 Мбит/с.
3. В каком из приведенных ниже вариантов правильно указаны неперекрывающиеся каналы для стандарта 802.11b с модуляцией DSSS в США?
 - а) 1, 2 ,3.
 - б) 1, 5, 9.
 - в) 1, 6, 11.
 - г) а, б, г.
 - д) 22, 33, 44.
4. Какой из перечисленных ниже терминов описывает режим работы беспроводной сети, в котором мобильное устройство при перемещении переключается на разные точки доступа?
 - а) ESS.
 - б) BSS.
 - в) IBSS.
 - г) Правильных вариантов нет.
5. Какой из указанных параметров обычно нужно установить при конфигурировании беспроводной точки доступа?
 - а) SSID.
 - б) Скорость.
 - в) Стандарт беспроводной сети.
 - г) Желаемый диаметр зоны уверенного покрытия.
6. Какое из указанных ниже утверждений правильно описывает подключение ESS к проводной сети Ethernet?
 - а) Точка доступа подключается к коммутатору Ethernet перекрещенным кабелем (crossover).
 - б) Разным точкам доступа в одной и той же беспроводной сети должна быть назначена одна и та же сеть VLAN в коммутаторах Ethernet.
 - в) В точке доступа должен быть задан IP-адрес, чтобы она смогла передавать трафик дальше.
 - г) Если точка доступа работает в смешанном режиме 802.11g, ее нужно подключать к коммутатору Ethernet через канал Fast Ethernet или более быстрый.
7. В только что развернутой беспроводной сети пользователи не могут подключиться через точку доступа к проводной инфраструктуре. Какова наиболее вероятная причина такого поведения сети?

- а) Беспроводная точка доступа установлена на металлической крышке телекоммуникационного шкафа.
- б) Пользователь или группа пользователей находятся рядом с каким-либо заведением общественного питания, в котором работает микроволновая печь.
- в) Пользователям мешают подключиться к сети многометровые жгуты кабеля категории 5, которые остались в стенах, потолке и полу от предыдущего варианта сети.
- г) Точка доступа использует канал DSSS 1 вместо стандартного канала 6, а программное обеспечение в устройствах пользователей никто не перенастраивал, и там используется канал 6.

8. Какой из перечисленных ниже стандартов безопасности беспроводных сетей ссылается на стандарт IEEE?

- а) WPA.
- б) WPA2.
- в) WEP.
- г) 802.11i.

9. Какие из указанных ниже функций безопасности не были включены в оригинальный стандарт WEP, но вошли в современный стандарт WPA2?

- а) Динамический обмен ключами.
- б) Предустановленные ключи (PSK).
- в) Аутентификация 802.1x.
- г) Шифрование AES.

Основные темы

В этой главе рассматриваются преимущественно основы беспроводных локальных сетей. В первом разделе описаны основные концепции, протоколы и стандарты наиболее распространенных на сегодняшний день беспроводных технологий. В следующем разделе приведены основные этапы развертывания беспроводной сети, и в заключение главы рассмотрены вопросы безопасности беспроводной сети. Безопасность беспроводной инфраструктуры является чрезвычайно важной темой, поскольку намного проще перехватить радиосигналы, чем подключиться к проводной локальной сети Ethernet.

Концепции беспроводных сетей

Многие пользователи регулярно пользуются услугами и устройствами *беспроводных локальных сетей* (Wireless LAN — WLAN). Компании, производящие и продающие персональные компьютеры, отмечают, что несколько последних лет наблюдается тенденция роста продаж портативных компьютеров (laptop): чем дальше, тем больше продается портативных устройств и меньше обычных компьютеров. Пользователям компьютера нужно подключение к какой-либо близлежащей сети, где бы они ни находились: на работе, дома, в гостинице, в кафе или книжном магазине. Быстрое увеличение количества планшетов и других подобных устройств, которые подключаются через сеть WLAN, скрыто обусловило нынешний рост популярности беспроводных сетей.

Например, на рис. 11.1 приведена структура сети современного книжного магазина. Клиентам магазина предоставляется бесплатный доступ к Интернету по беспроводной технологии, а устройства в сети самого магазина соединены проводной локальной сетью.

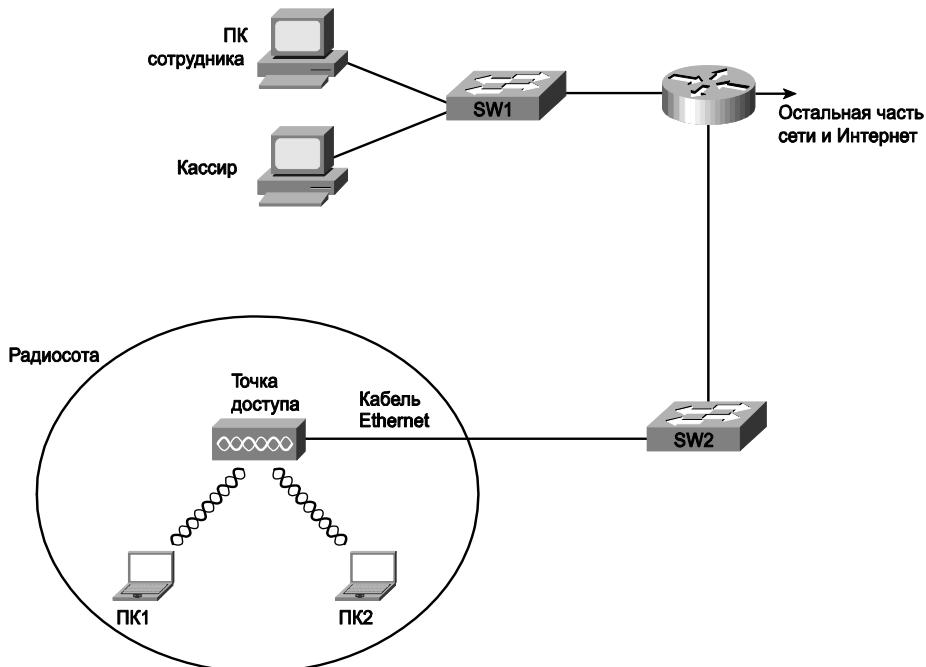


Рис. 11.1. Простая сеть книжного магазина

Портативные компьютеры клиентов (или другие устройства) взаимодействуют с устройством WLAN, называемым *точкой доступа* (Access Point — AP). Точка доступа использует радиоканал для отправки и получения фреймов от клиентского устройства, например компьютера. Кроме того, точка доступа подключена к той же сети Ethernet, что и устройства, обеспечивающие работу магазина, следовательно, и покупатели, и сотрудники могут искать информацию на дистанционных веб-сайтах.

В первом разделе главы описаны основы технологий беспроводных сетей, в частности, повествование начинается со сравнения беспроводных и проводных сетей, а в оставшейся части раздела в основном обсуждаются их основные отличия.

Сравнение с технологиями сетей Ethernet

Беспроводные локальные сети (WLAN) во многих своих аспектах похожи на локальные сети технологии Ethernet, например, оба типа сетей позволяют устройствам взаимодействовать между собой. Для обеих разновидностей сетей стандарты установлены *Институтом инженеров по электротехнике и электронике* (The Institute of Electrical and Electronics Engineers — IEEE): стандарт IEEE 802.3 для сетей Ethernet и 802.11 — для беспроводных сетей (WLAN). В обоих стандартах описан формат фреймов сети (заголовок и концевик), указано, что заголовок должен иметь длину 6 байтов и содержать MAC-адреса отправителя и получателя. Оба стандарта указывают, как именно устройства в сети должны определять, когда можно передавать фрейм в среду, а когда нельзя.

Основное отличие двух типов сетей состоит в том, что для передачи данных в беспроводных сетях используется технология излучения энергии, называемой радиоволнами, а в сетях Ethernet используется передача электрических импульсов по медному кабелю (или импульсов света в оптическом волокне). Для передачи радиоволн не нужна какая-либо среда, обычно говорят, что “они передаются в эфире”, чтобы подчеркнуть, что никакой физической сети не надо. В действительности любые физические объекты (т.е. вещества) на пути радиосигнала — стены, металлические конструкции и т.п. — являются препятствием, значительно ухудшающим качество радиосигнала в беспроводной технологии.

Есть еще несколько существенных отличий между проводными и беспроводными сетями, правда, они относятся уже скорее к побочным эффектам технологий. Так, например, в главе 7 было описано, как в сетях Ethernet работает *дуплексный* (full-duplex — FDX) метод передачи, когда к порту коммутатора подключено единственное сетевое устройство. Такая схема работы исключает необходимость использования технологии обнаружения коллизий в линии (CSMA/CD). В беспроводной технологии, когда несколько устройств излучают радиоволны в одном и том же пространстве и на той же частоте, сигнал различить практически невозможно и приходится использовать *полудуплексный* (half-duplex — HDX) механизм взаимодействия устройств. Чтобы решить вопрос с использованием той же частоты передачи, в беспроводных сетях используется механизм *множественного доступа с предотвращением коллизий* (Carrier Sense Multiple Access with Collision Avoidance — CSMA/CA), в котором используется логика передачи HDX и пытаются избегать ситуаций, в которых возникают коллизии.

Стандарты сетей WLAN

IEEE определяет стандарты LAN как часть стандартов 802.11. В этом разделе перечислены основные детали каждого из четырех стандартов WLAN 802.11: 802.11a, 802.11b, 802.11g и 802.11n.

На сегодняшний день наибольшее влияние на стандарты беспроводных сетей оказали четыре организации, приведенные в табл. 11.2.



Таблица 11.2. Организации по стандартизации сетей WLAN

Организация	Роль
ITU-R (International Telecommunications Union, Radiocommunication Sector — Сектор радиосвязи Международного союза электросвязи)	Международная организация по стандартизации радиоэлектронных средств связи она регулирует, в частности, использование частотных диапазонов
IEEE (The Institute of Electrical and Electronics Engineers, Inc. — Институт инженеров по электротехнике и радиоэлектронике)	Стандартизовал беспроводные локальные сети (802.11)
Wi-Fi Alliance (Альянс Wi-Fi)	Промышленный консорциум, отвечающий за совместимость устройств, в которых реализованы стандарты WLAN в рамках программы по сертификации продуктов Wi-Fi
Federal Communications Commission (FCC — Федеральная комиссия связи США)	Федеральное агентство США, регулирующее использование различных частотных диапазонов в США

Из всех перечисленных выше организаций только IEEE фактически занимается стандартизацией различных современных технологий беспроводных коммуникаций. Его стандарты принимают во внимание частотные диапазоны, регулируемые различными международными и местными агентствами, такими как Комиссия FCC в США и Сектор ITU-R, который независимо контролируется Организацией Объединенных Наций.

Первая спецификация беспроводной сети была выпущена IEEE в 1997 году, когда былratифицирован стандарт 802.11. Как видно из названия, в нем нет буквы-суффикса в конце, а во всех последующих стандартах есть. Такое соглашение об именовании спецификаций было изначально позаимствовано из названий стандартов для локальных сетей Ethernet. Аналогично в проводных сетях изначальный стандарт содержал просто номер, 802.3, а во все последующие стандарты добавлялась буква в конце, вплоть до спецификации 802.3u, одного из относительно последних стандартов сети Fast Ethernet.

Оригинальный стандарт 802.11 использовался очень недолго и был вытеснен более современными спецификациями, в порядке принятия стандартов их можно указать так (каждый новый постепенно вытесняет предыдущий): 802.11b, 802.11a, 802.11g и 802.11n. Следует отметить, что стандарт 802.11n был принят в 2009 году, а продукты, его использующие, появились уже в 2007 году (так называемые “достандартные” разработки). В табл. 11.3 указаны ключевые параметры всех принятых на сегодняшний день стандартов.



Таблица 11.3. Сравнение стандартов 802.11a, 802.11b и 802.11g

Характеристика	802.11a	802.11b	802.11g	802.11n
Год принятия	1999	1999	2003	2009
Максимальная скорость при модуляции DSSS (Мбит/с)	—	11	11	—
Максимальная скорость при модуляции OFDM (Мбит/с)	54	—	54	150
Полоса частот (ГГц)	5	2,4	2,4	Обе
Количество неперекрывающихся каналов	23	3	3	9 ¹

В таблице указано несколько характеристик, для которых пока еще не были даны определения, но они описаны ниже в главе.

Режимы работы сети стандарта 802.11

В беспроводной сети могут использоваться два режима работы: *одноранговая сеть* (ad hoc) и *инфраструктура* (infrastructure). В одноранговой схеме беспроводное устройство взаимодействует с одним или несколькими такими же устройствами, обычно в течение небольших промежутков времени. В такой ситуации устройства отправляют фреймы в беспроводной сети WLAN напрямую друг другу, как показано на рис. 11.2.

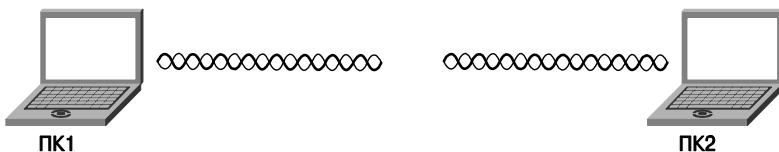


Рис. 11.2. Одноранговая сеть

В режиме инфраструктуры каждое из устройств взаимодействует с точкой доступа (AP), а сама точка подключена к проводной сети по каналу Ethernet. Данный режим работы позволяет устройствам в беспроводной сети связываться как с серверами в остальной проводной сети, так и получать доступ к Интернету (см. рис. 11.1).

ВНИМАНИЕ!

Устройства в беспроводной сети в режиме инфраструктуры не могут пересыпать фреймы напрямую друг другу и отправляют их точке доступа, которая может перенаправить их нужному устройству-получателю.

В инфраструктурном режиме есть два варианта обслуживания — так называемые наборы служб (service sets). Первый, называемый *базовым набором служб* (Basic Service Set — BSS), позволяет использовать одну точку доступа для создания беспроводной локальной сети, например, показанной на рис. 11.1. Второй, *расширенный набор служб* (Extended Service Set — ESS), позволяет использовать в сети более одной точки доступа (AP или ТД), зачастую с перекрывающимися сотами покрытия, позволяющими использовать *роуминг* (roaming) в сети (рис. 11.3).

¹ Подразумеваются каналы на 40 МГц. — Примеч. авт.

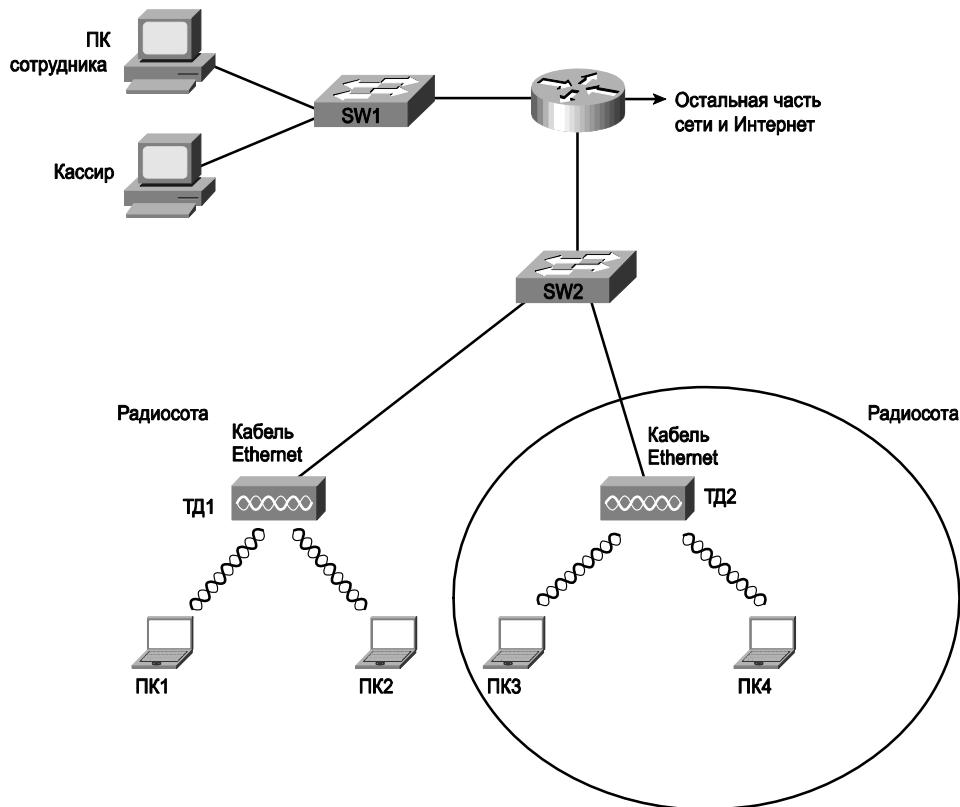


Рис. 11.3. Набор служб ESS в инфраструктурном режиме беспроводной сети

В сетях ESS разрешен роуминг, что означает, что пользователи могут перемещаться в *области покрытия* (coverage area) и оставаться в одной и той же беспроводной сети, следовательно, не нужно менять IP-адрес при переключении на другую точку доступа. Все, что должно уметь устройство для роуминга, — это отслеживать уменьшение силы сигнала используемой точки доступа и обнаруживать новые точки доступа с более высоким уровнем сигнала и уметь переключаться на них.

В табл. 11.4 перечислены рассмотренные выше режимы работы беспроводной сети.

Ключевая тема Таблица 11.4. Режимы работы сетей WLAN, их формальные названия и описание

Режим	Название набора служб	Описание
Одноранговый (Ad hoc)	Независимый базовый набор служб (Independent Basic Service Set — IBSS)	Два устройства могут взаимодействовать напрямую, точка доступа не нужна
Инфраструктурный (одна точка доступа)	Базовый набор служб (Basic Service Set — BSS)	Создается одна беспроводная локальная сеть с одной точкой доступа, и все устройства связаны с ней
Инфраструктурный (больше одной точки доступа)	Расширенный набор служб (Extended Service Set — ESS)	Множество точек доступа создают одну беспроводную сеть, позволяя использовать роуминг

Беспроводная передача данных (уровень 1)

В беспроводных сетях передача на первом уровне осуществляется за счет излучения радиосигнала — радиоволн. В беспроводных *сетевых картах* (Network Interface Card — NIC), точках доступа и других устройствах такой сети есть радиоканал и антenna для приема и излучения радиоволн, в которых закодированы пользовательские данные. Технология кодирования сигнала в беспроводных сетях основана на той же идее, что и каналы стандарта Ethernet.

Точно так же как ток в медном проводе или свет в оптическом волокне, радиоволны в беспроводных сетях представляют собой сигнал, повторяющийся с определенной частотой, как показано на рис. 11.4. В графическом представлении кривая, изображающая периодический сигнал, характеризуется частотой (сколько раз в течение секунды повторился сигнал), амплитудой (высотой волны, т.е. мощностью сигнала) и фазой (т.е. начальной точкой на кривой). Для беспроводных сетей самым важным параметром является частота, измеряемая в герцах (Гц).

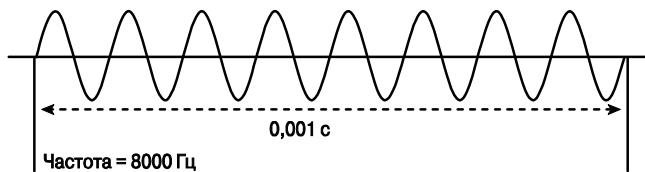


Рис. 11.4. Графическое представление сигнала с частотой 8 КГц

Различные беспроводные устройства излучают сигнал на разных частотах, в зависимости от того, для чего предназначено устройство, например, карта беспроводной сети и радиотелефон. Следовательно, при работе таких устройств будут появляться побочные эффекты. В качестве примера рассмотрим телевидение — телевизионная вышка излучает сигнал, принимаемый телевизорами. Чтобы предотвратить наложение такого сигнала на другие и интерференцию с другими радиоисточниками, национальные государственные агентства регулируют и отслеживают использование частотных диапазонов внутри страны. В США, например, эта задача возложена на Федеральную комиссию по связи США (Federal Communications Commission — FCC).

Комиссия FCC или другое государственное учреждение (в других странах) регулирует использование наборов частот внутри страны, называемых обычно *частотными диапазонами* (frequency bands). Например, в США радиостанции диапазонов FM и AM обязаны регистрироваться в Комиссии FCC и использовать строго определенные частоты или диапазоны. Радиостанции также обязаны излучать радиосигнал только определенной мощности, чтобы станции в других городах могли использовать те же частоты для своего вещания, но в определенной географической области только одна радиостанция может использовать какую-либо выделенную частоту.

Частотный диапазон был назван “диапазоном” потому, что в него входит несколько последовательных частот, например радиостанции FM нужна полоса порядка 200 КГц (килогерц), чтобы осуществлять вещание. Когда такая станция запрашивает вещательную частоту у Комиссии FCC, она получает базовую частоту и для нее резервируется по 100 КГц вниз и вверх от такой базовой, т.е. диапазон. Например, станция FM анонсирует, что “на частоте 96,5 FM круглые сутки звучат только лучшие хиты”. В действительности базовый сигнал передается на частоте 96,5 МГц, а в передатчике используются частоты от 96,4 до 96,6 МГц, что дает диапазон шириной 0,2 МГц, или 200 КГц.

Чем шире набор частот в диапазоне частот, тем больший объем информации может быть передан в нем. Например, если сигнал вещания радиостанции требует всего порядка 200 КГц (т.е. 0,2 МГц) из *полосы пропускания* (bandwidth), то в телевизионном вещании нужно передать много больше информации, поэтому полоса частот приблизительно равна 4,5 МГц.

ВНИМАНИЕ!

Термин *полоса пропускания* (bandwidth), используемый для описания скорости сетевых интерфейсов, позаимствован из радиоэлектроники, в которой частотный диапазон, или полоса пропускания, является мерой того, сколько данных может быть передано в некоторый период времени.

Комитет FCC и эквивалентные ему государственные организации в других странах лицензируют использование некоторых частотных диапазонов, а другие оставляют нелицензированными. Лицензированные диапазоны имеют множество применений, в частности, большинство радиостанций АМ и FM, *ультракоротковолновые радиосистемы* (Ultra High Frequency — UHF) (например, радиосвязь полиции в США) и мобильные телефоны используют частоты этого диапазона. Нелицензированные частоты могут использоваться любыми устройствами, тем не менее устройства должны следовать правилам регулирующих организаций страны. В частности, устройство, работающее в нелицензируемом диапазоне, все равно должно излучать сигнал определенной мощности, в противном случае оно будет причиной интерференции радиосигналов с другими устройствами этого же диапазона. Так, например, микроволновые печи зачастую излучают энергию на частоте 2,4 ГГц, хотя это побочный эффект в процессе приготовления пищи, а не попытка передачи данных. Тот же (нелицензируемый) диапазон используется в некоторых стандартах беспроводных локальных сетей и многими беспроводными телефонами, поэтому можно столкнуться с тем, что вы не слышите собеседника или не можете подключиться к сети, когда кто-то разогревает себе обед.

Комитет FCC не требует лицензирования для трех частотных диапазонов, которые обычно указываются в виде определенной базовой частоты, хотя в действительности, согласно определению, диапазон включает в себя достаточно обширный набор частот. В табл. 11.5 перечислены диапазоны, имеющие то или иное отношение к беспроводным локальным сетям.

 **Таблица 11.5. Нелицензируемые диапазоны частот, определенные Комитетом FCC**

Базовая частота диапазона	Название	Примеры устройств
0,9 МГц	Промышленный, научный и медицинский диапазон (Industrial, Scientific and Medical — ISM)	Старые беспроводные телефоны
2,4 ГГц	ISM	Новые беспроводные телефоны и беспроводные сети стандартов 802.11, 802.11b, 802.11g, 802.11n
5 ГГц	Нелицензируемая национальная информационная инфраструктура (Unlicensed National Information Infrastructure — U-NII)	Новые беспроводные телефоны и беспроводные сети стандартов 802.11a и 802.11n

Кодирование в сетях WLAN и неперекрывающиеся каналы DSSS

Когда беспроводная сетевая карта или точка доступа пересыпает данные, она модулирует (т.е. изменяет) частоту, амплитуду или фазу радиосигнала, чтобы закодировать 0 или 1. Подробности алгоритмов и методов модулирования выходят за рамки рассмотрения данной книги, но для практической работы и сдачи экзамена следует знать названия трех наиболее распространенных методов кодирования, поскольку эта информация понадобится при проектировании и развертывании беспроводных сетей.

Метод расширения спектра со скачкообразным изменением частоты (Frequency Hopping Spread Spectrum — FHSS) использует все частоты диапазона за счет того, что “перескакивает” (hopping) на другую базовую частоту передачи. За счет того, что для каждой последующей передачи используется немного отличающаяся частота, устройство, вполне вероятно, не будет попадать на частоту, используемую другим передатчиком. В первом стандарте беспроводных сетей, 802.11, использовалась модуляция FHSS, в современных стандартах (802.11a, 802.11b и 802.11g) используются другие методы.

Метод расширения спектра прямой последовательности (Direct Sequence Spread Spectrum — DSSS) — это второй общий механизм кодирования сигнала в беспроводных сетях. Он был разработан для нелицензируемого диапазона 2,4 ГГц и использует один из нескольких раздельных каналов (т.е. частот). В этом диапазоне частотная полоса составляет 82 МГц, т.е. сам диапазон находится в частотах 2 402–2 483 МГц. Согласно требованиям Комитета FCC в этом диапазоне может быть 11 пересекающихся каналов DSSS, как показано на рис. 11.5.

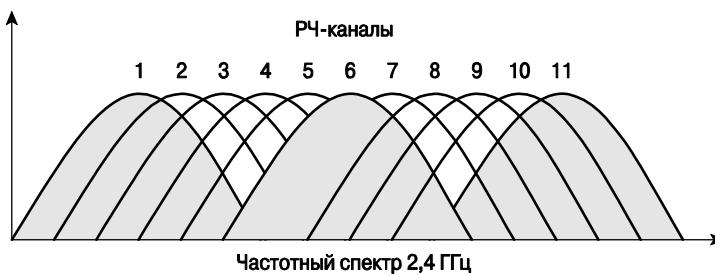


Рис. 11.5. Одиннадцать пересекающихся каналов DSSS в диапазоне 2,4 ГГц

Несмотря на то что большинство каналов, показанных на рисунке, пересекается, три из них (крайние слева, справа и центральный канал) пересекаются достаточно слабо, чтобы мешать друг другу. Эти три канала (1, 6 и 11) могут быть использованы в одном и том же пространстве для беспроводных коммуникаций и не будут инфицировать друг с другом.

Важное свойство трех неперекрывающихся каналов состоит в том, что, когда разрабатывается структура беспроводной сети с набором служб ESS (т.е. в одной и той же области есть больше одной точки доступа), точки доступа с перекрывающимися областями покрытия должны использовать неперекрывающиеся каналы (рис. 11.6).

В такой схеме сети устройства в одной зоне BSS (так называют устройства, подключенные к одной и той же точке доступа) могут обмениваться данными, в соседних зонах BSS тоже может идти интенсивный обмен данными. Тем не менее интерференции в сети не будет, поскольку все точки доступа используют несколько отличающиеся частоты неперекрывающихся каналов. Например, компьютеры ПК1

и ПК2 могут находиться рядом, но взаимодействовать с разными точками доступа (ТД), используя две разные частоты канала в один и тот же момент времени. Такой метод кодирования является типичным для беспроводных сетей стандарта 802.11b, в каждой ячейке покрытия максимальная скорость передачи данных для этой технологии составляет 11 Мбит/с. При использовании неперекрывающихся каналов каждая зона BSS может работать на скорости 11 Мбит/с, следовательно, общая пропускная способность будет составлять 33 Мбит/с. Общую, или кумулятивную, пропускную способность беспроводной инфраструктуры называют *емкостью* (capacity).

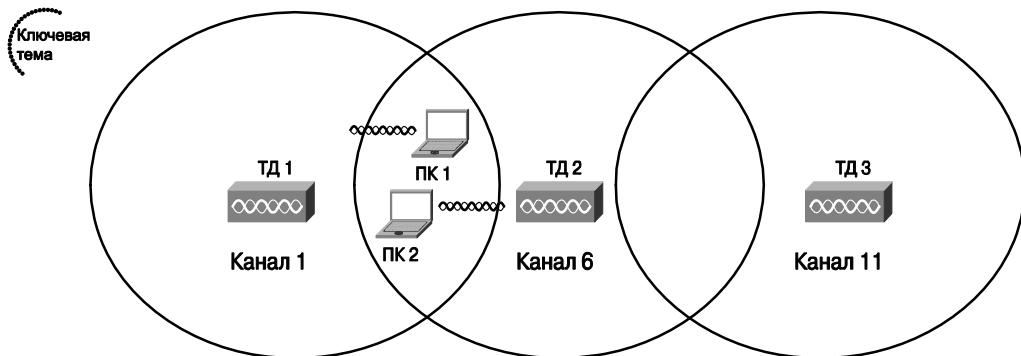


Рис. 11.6. Использование неперекрывающихся каналов DSSS диапазона 2,4 ГГц в сети ESS

Третьим самым распространенным методом кодирования в беспроводных сетях WLAN является *мультиплексирование с ортогональным частотным разделением сигналов* (Orthogonal Frequency Division Multiplexing — OFDM). Аналогично механизму DSSS, в беспроводных сетях с кодированием OFDM используется множество непересекающихся каналов. В табл. 11.6 перечислены методы кодирования сигнала и соответствующие им стандарты.

Таблица 11.6. Методы кодирования и стандарты беспроводных сетей IEEE

Название и аббревиатура класса	В каком стандарте используется
Метод расширения спектра со скачкообразным изменением частоты (Frequency Hopping Spread Spectrum — FHSS)	802.11
Метод расширения спектра сигнала прямой последовательности (Direct Sequence Spread Spectrum — DSSS)	802.11b, 802.11g
Мультиплексирование с ортогональным частотным разделением сигналов (Orthogonal Frequency Division Multiplexing — OFDM)	802.11a, 802.11g и 802.11n

ВНИМАНИЕ!

В стандарте 802.11n используется метод OFDM с несколькими антеннами, поэтому метод зачастую называют методом со *многими входами и многими выходами* (Multiple Input Multiple Output — MIMO).

Интерференция в беспроводных сетях

В беспроводных сетях интерференция может быть вызвана разными источниками. Радиоволны могут свободно распространяться в пространстве, тем не менее, когда они проходят через какую-либо плотную материю, стены, бетонные блоки, перекрытия и тому подобное, часть энергии волны поглощается препятствием, следовательно, сила сигнала уменьшается и уменьшается размер области покрытия. Некоторые объекты могут отражать или рассеивать радиоволны, например, если в них много металла, что приводит к появлению “мертвых зон” (областей, где беспроводная связь вообще не работает), и опять же уменьшать размер области покрытия.

Более того, на беспроводные коммуникации влияют источники радиоволн в том же частотном диапазоне. Эффект очень похож на тот, который можно наблюдать в дальних автомобильных поездках, слушая радио. Сначала получатель принимает сильный и чистый сигнал и качество звучания любимой радиостанции бесподобно. По мере удаления от антенны радиостанции сигнал слабеет, ухудшается звук, появляются помехи, треск и т.п. Вдруг вы подъезжаете к области покрытия радиостанции следующего крупного города на маршруте, вещающей на той же частоте, и не слышите ни первую, ни вторую станцию из-за интерференции сигналов. В беспроводных локальных сетях интерференция означает, что данные могут быть переданы очень редко, требуется огромное количество повторных попыток передачи, следовательно, эффективность сильно уменьшается.

Ключевым параметром для обнаружения интерференции является *соотношение “сигнал-шум”* (Signal-to-Noise Ratio — SNR). Оно описывает, насколько уровень полезного сигнала выше, чем у нежелательных сигналов (т.е. шума) в какой-либо области. Чем выше значение параметра SNR, тем чаще устройства WLAN могут успешно отправлять данные.

Зона покрытия, скорость и емкость

Зона покрытия беспроводной сети — это область в пространстве, в которой два устройства WLAN могут успешно обмениваться данными. Какую зону покрытия создает каждая конкретная точка доступа, зависит от множества факторов, несколько из них описаны ниже.

Прежде всего следует помнить, что мощность передатчика точки доступа или беспроводной сетевой карты не должна превышать некоторого значения, определяемого регулирующими агентствами, например, такими, как FCC. Комитет FCC ограничивает мощность передачи, чтобы обеспечить справедливое и равноправное использование нелицензируемых диапазонов. Например, если два соседа купят себе точки доступа компании Linksys и установят их у себя в частных домах, чтобы пользоваться беспроводной сетью, то такие устройства будут соответствовать требованиям FCC и не помешают друг другу. Тем не менее, если один из соседей установит для точки доступа антенну с высоким коэффициентом усиления, которая, скорее всего, не соответствует требованиям FCC, он получит значительно большую зону покрытия, возможно, “захватит” в нее еще нескольких соседей. В результате чья-то соседняя точка доступа может не работать из-за интерференции.

ВНИМАНИЕ!

Сила сигнала точки доступа оценивается с помощью параметра *эффективной изотропно-излучаемой мощности* (Effective Isotropic Radiated Power — EIRP). Он представляет собой мощность сигнала на выходе радиоканала с учетом усиления за счет антенны и потерь мощности сигнала в кабеле. Фактически значение EIRP описывает излучаемый антенной сигнал.

Материал окружающих объектов и их местоположение относительно точки доступа также влияют на ее зону покрытия. Например, если поместить точку доступа около какого-либо крупного металлического объекта (шкафа, стойки и т.п.), будет наблюдаться как рассеяние, так и отражение сигнала, и зона покрытия заметно уменьшится. Аналогично бетонные конструкции с арматурой внутри в современных офисных зданиях также значительно уменьшают области покрытия от точек доступа, а за счет каких-либо архитектурных излишеств также может возникать интерференция. Для точек доступа выпускаются антенны различного типа, которые позволяют изменять форму области покрытия: круговые, штырьковые и др.

Следующая особенность беспроводных технологий — чем слабее сигнал, тем ниже скорость передачи данных, поэтому стандарты сетей WLAN поддерживают передачу на разных скоростях. Устройство, расположенное рядом с точкой доступа, будет принимать сильный сигнал, следовательно, оно сможет передавать и принимать информацию на высокой скорости, а устройство, размещенное на границе зоны покрытия, где сигнал очень слабый, все-таки сможет принимать и передавать данные, но на невысокой скорости. На рис. 11.7 показана зона покрытия и изменение скорости передачи данных для сети BSS стандарта IEEE 802.11b.

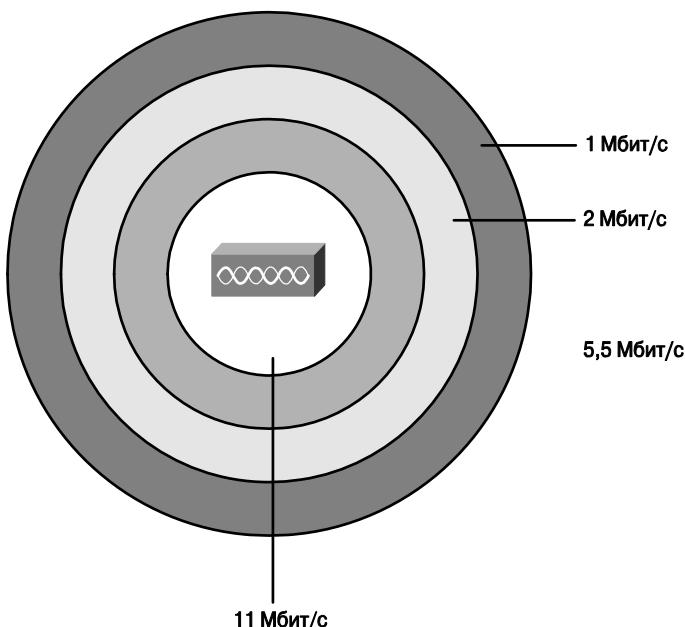


Рис. 11.7. Зона покрытия и скорость

Два основных метода увеличения размеров области покрытия точки доступа: использование специализированных антенн и увеличение мощности выдаваемого радиоканалом сигнала. Например, можно установить antennу с большим коэффициентом усиления, в таком случае увеличится мощность излучаемого сигнала. Чтобы увеличить зону покрытия в два раза, antennа должна усиливать сигнал в четыре раза. Это, конечно, полезная возможность, но выходная мощность (EIRP) излучаемого antennной сигнала все равно не должна превышать требования FCC (в США).

Действительный размер зоны покрытия при беспроводной связи зависит от великого множества факторов, описание которых выходит за рамки данной книги. Например, зона покрытия также зависит от используемого частотного диапазона стандарта WLAN, преград между беспроводными устройствами, интерференции от других источников радиосигнала, antenn точек доступа и беспроводных карт клиентских станций и параметров методов кодирования DSSS и OFDM. Строго говоря, в тех стандартах сетей WLAN, где используются более высокие частоты (диапазон U-NII стандартов 802.11a и спецификации 802.11n), данные могут передаваться на более высоких скоростях, но плата за скорость — меньший размер зоны покрытия. Но обратите внимание на то, что более новый стандарт 802.11n способен обеспечить более широкую зону покрытия, чем все прежние стандарты. Чтобы обеспечить покрытие необходимой территории в сети ESS с высокочастотной передачей сигнала, потребуется больше точек доступа, следовательно, увеличатся затраты на построение беспроводной инфраструктуры.

В табл. 11.7 перечислены основные стандарты IEEE беспроводных сетей,ratифицированные на момент выпуска этой книги, указана максимальная скорость и количество неперекрывающихся каналов.

Таблица 11.7. Скорости и частотные диапазоны для разных стандартов беспроводных сетей

Стандарт IEEE	Максимальная скорость передачи данных (Мбит/с)	Частота (ГГц)	Количество неперекрывающихся каналов
802.11b	11	2,4	3
802.11a	54	5	23
802.11g	54	2,4	3
802.11n	72,2	5	21
802.11n ²	150	5	9

ВНИМАНИЕ!

Первый стандарт беспроводных сетей, 802.11, поддерживал скорости 1 и 2 Мбит/с.

И последний фактор, влияющий на качество работы беспроводной сети, который мы рассмотрим, — количество неперекрывающихся каналов. Количество таких (практически неперекрывающихся, хотя некоторое перекрытие есть) каналов в стандарте (см. рис. 11.5 и 11.6) беспроводной сети определяет общую комбинированную пропускную способность структуры. Например, для сети исключительно стандарта 802.11g действительная скорость передачи может составлять 54 Мбит/с; в отдельных ситуациях три устройства могут находиться рядом, но использовать три разные точки

² При использовании на 40 МГц, а не на 20 МГц, как в других строках таблицы. — Примеч. авт.

доступа из одной и той же сети. Теоретически в такой ситуации общая пропускная способность будет составлять 3×54 Мбит/с, т.е. 162 Мбит/с в одной и той же сети. Исходя из тех же рассуждений, в беспроводной сети стандарта 802.11a данные могут передаваться на скорости 54 Мбит/с, но в 12 неперекрывающихся каналах; следовательно, теоретическая максимальная пропускная способность (т.е. емкость сети) будет составлять $12 \times 54 = 648$ Мбит/с.

Доступ к среде в беспроводной сети (уровень 2)

Изначально в технологии локальных сетей Ethernet использовалась разделяемая (shared) среда, коаксиальный кабель, и предполагалось, что только одно устройство может передавать данные в один момент времени. Чтобы контролировать такую *полудуплексную* (Half-Duplex — HDX) среду, в технологии используется специальный алгоритм — *множественный доступ с обнаружением коллизий* (Carrier Sense Multiple Access with Collision Detection — CSMA/CD). С развитием технологии Ethernet и появлением новых стандартов и устройств, в частности, когда появились коммутаторы и структуры, где только одно устройство подключено к одному порту коммутатора, полудуплексная технология стала использоваться значительно реже и ее начал вытеснять *дуплексный* метод передачи данных (Full Duplex — FDX). В режиме дуплексной передачи данных коллизий быть не может, поэтому алгоритм CSMA/CD отключен.

В беспроводных коммуникациях устройства не могут быть разнесены по разным кабельным сегментам, чтобы избежать коллизий, поэтому коллизии будут всегда, вне зависимости от используемого стандарта WLAN. Если два или более устройства WLAN пересыпают данные одновременно в *перекрывающихся* (overlapping) частотных диапазонах, то возникает коллизия, и ни один из переданных устройствами сигналов не может быть расшифрован получателем. Что еще усугубляет положение, так это то, что устройство, передающее что-либо, не может одновременно принимать данные. Таким образом, если два устройства в беспроводной сети создали коллизию, у них нет прямого метода ее обнаружения.

Для решения проблемы доступа к среде передачи данных в беспроводных сетях был разработан алгоритм, называемый *множественным доступом с предотвращением коллизий* (Carrier Sense Multiple Access with Collision Avoidance — CSMA/CA). Механизм предотвращения коллизий минимизирует статистическую вероятность возникновения коллизий в сети, но алгоритм CSMA/CA не исключает коллизии совсем, следовательно, в стандартах беспроводных сетей должны быть предусмотрены процессы, отвечающие за обработку коллизий. Поскольку передающее устройство не может обнаружить, была коллизия или нет, при передаче фрейма в беспроводных сетях каждый переданный фрейм должен быть подтвержден. Все беспроводные устройства прослушивают эфир на предмет подтверждений, которые должны быть отправлены сразу после того, как фрейм передан. Если подтверждение не получено, устройство-отправитель предполагает, что фрейм был утерян или попал в коллизию, и пересыпает его повторно.

Ниже описаны ключевые этапы алгоритма CSMA/CA, некоторые детали опущены, чтобы упростить понимание и запоминание принципа его работы.

- Этап 1** Прослушивание среды (эфира), чтобы убедиться, что она не занята, т.е. в данный момент нет радиопередачи на используемых устройством частотах.

- Этап 2** Установка случайного времени (и таймера) ожидания, чтобы статистически уменьшить вероятность ситуации, в которой несколько устройств попытаются одновременно начать передачу данных.
- Этап 3** Когда случайный интервал времени истек, прослушать среду еще раз, чтобы убедиться, что она не занята. Если среда свободна, передать фрейм.
- Этап 4** После пересылки фрейма полностью дождаться подтверждения его получения.
- Этап 5** Если подтверждение не получено, повторно переслать фрейм с использованием алгоритма CSMA/CA, т.е. ожидания в течение соответствующего периода времени перед передачей данных.

На этом мы заканчиваем наше краткое введение в концепции современных беспроводных сетей. В следующем разделе будут описаны основные этапы установки новых сетей WLAN.

Развертывание беспроводных сетей

При развертывании беспроводных сетей (WLAN) наиболее важной характеристикой инфраструктуры является ее безопасность. Для сетей WLAN характерны те же проблемы с безопасностью, что и для проводных сетей Ethernet, плюс множество собственных особенностей. Например, кто-то может припарковать свою машину рядом с офисом и принимать сигналы беспроводной сети из здания и считывать данные. Это одна из основных причин, почему во всех корпоративных беспроводных сетях рекомендуется использовать максимальные меры безопасности.

Несмотря на то что вопросы безопасности в беспроводных сетях жизненно важны, главная задача при установке новой сети — чтобы она для начала просто заработала. Как только устройство может связаться с точкой доступа, передать и принять данные, можно заниматься вопросами безопасности. Приблизительно в таком ключе и построен текущий раздел, основное внимание удалено вопросам планирования и реализации сети WLAN, а средства безопасности и их настройка пока не затрагиваются. Вопросы безопасности полностью вынесены в раздел “Безопасность беспроводных сетей” заключительной части главы.

Этапы реализации беспроводной сети

Представленный ниже список можно использовать в качестве руководства по установке беспроводной сети BSS.

Этапы реализации беспроводной сети



- Этап 1** Убедиться, что обычная проводная сеть работает, проверить службы DHCP, сети VLAN и наличие доступа от всех узлов к Интернету.
- Этап 2** Установить беспроводную точку доступа, настроить и проверить ее связь с проводной сетью, в том числе настроить IP-адрес, маску подсети и стандартный шлюз в точке доступа.
- Этап 3** Настроить параметры беспроводной сети в точке доступа, в том числе *идентификатор набора служб* (Service Set Identifier — SSID), но пока не настраивать параметры безопасности.
- Этап 4** Установить и настроить один беспроводной клиент (например, портативный компьютер), опять же не настраивая параметры безопасности.
- Этап 5** Убедиться в том, что беспроводная сеть работает между клиентским устройством и точкой доступа.

Этап 6 Настроить параметры безопасности в точке доступа и клиентском устройстве.

Этап 7 Убедиться в том, что беспроводная сеть по-прежнему работает при наличии функций безопасности.

Как и было обещано, в текущем разделе будут подробно описаны первые пять этапов, а в заключительном разделе главы обсуждаются концепции и механизмы безопасности беспроводных сетей без излишней детализации.

Этап 1. Проверка работоспособности существующей проводной сети

Во многих главах этой книги рассказывается, как разобраться в технологиях, распланировать и реализовать проводные сети, состоящие из маршрутизаторов и коммутаторов, поэтому повторять эту информацию еще раз не имеет смысла. Тем не менее будет полезно остановиться на паре моментов, связанных с использованием существующей проводной инфраструктуры в рамках создаваемой сети WLAN.

Прежде всего следует отметить, что порт Ethernet коммутатора, к которому подключена точка доступа, обычно работает в режиме доступа (access port) к сети, т.е. привязан к определенной сети VLAN. Вполне очевидно, что в сети ESS, когда используется несколько точек доступа и они подключены к разным устройствам, все используемые для беспроводной сети порты коммутаторов должны быть привязаны к одной и той же сети VLAN. На рис. 11.8 показана типичная схема беспроводной сети ESS и указан идентификатор сети VLAN (VLAN ID).

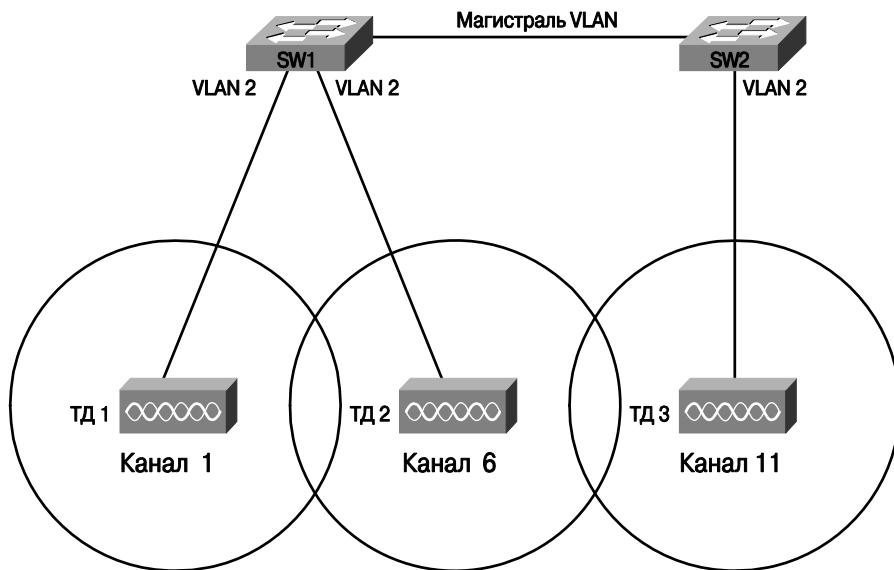


Рис. 11.8. Беспроводная сеть ESS, в которой все точки доступа находятся в сети VLAN 2

Чтобы проверить работоспособность существующей сети, нужно просто подключить сетевую карту персонального компьютера к тому самому кабелю, которым планируется подсоединить точку доступа. Если компьютер получает IP-адрес, маску и другую необходимую информацию от сервера DHCP и может обмениваться пакетами с другими узлами, то существующая проводная сеть готова к подключению точки доступа.

Этап 2. Конфигурирование параметров проводной сети точки доступа и информация IP

Точка доступа работает на втором уровне модели OSI, и ей не требуется IP-адрес для выполнения своих функций, точно так же, как и коммутатору Ethernet. Тем не менее в крупных и средних сетях рекомендуется присваивать коммутатору IP-адрес для упрощения системы управления устройствами, аналогично точкам доступа в крупных сетях также присваиваются адреса, чтобы можно было управлять ими удаленно.

Настройка информации протокола IP в точке доступа очень похожа на процедуру установки адреса в коммутаторе Ethernet, описанную в главе 9. В частности, к минимальным параметрам, которые нужно установить в устройстве, относятся IP-адрес, маска подсети, адрес стандартного шлюза и, возможно, IP-адрес сервера DNS.

Точка доступа подключается к коммутатору *прямым* (straight-through) кабелем. Настройки скорости порта коммутатора Ethernet особого значения не имеют, тем не менее рекомендуется подключать точку доступа к интерфейсу как минимум Fast Ethernet, поскольку производительность на высоких скоростях в сети WLAN будет выше.

Этап 3. Конфигурирование параметров беспроводной сети точки доступа

В большинстве случаев беспроводные точки доступа можно просто установить, и они будут работать без какой-либо дополнительной настройки. Например, во многих домах установлены беспроводные точки доступа потребительского класса, подключенные к высокоскоростному каналу Интернета. Зачастую оконечное оборудование для такого подключения реализовано в одном устройстве, например, в широкополосном маршрутизаторе с беспроводным интерфейсом модели Linksys Dual-Band Wireless A+G Broadband Router (компания Linksys является подразделением компании Cisco, производящим и продающим сетевые устройства потребительского класса). Многие люди просто покупают такие устройства, включают питание и подключают правильными кабелями его к проводной инфраструктуре, не меняют никаких настроек, и точка доступа сразу же работает!

И в точках доступа потребительского класса, и в устройствах корпоративного уровня может быть настроено множество параметров. К наиболее часто используемым настройкам из упоминавшихся выше в текущей главе можно отнести:

- стандарт IEEE (a, b, g или их комбинация);
- номер используемого канала;
- идентификатор сети (SSID);
- уровень мощности излучаемого сигнала.

В этой главе практически все перечисленные параметры уже более или менее подробно обсуждались, мало внимания было уделено только идентификатору SSID. Каждой беспроводной сети нужно дать некоторое уникальное название, чтобы ее можно было идентифицировать. Поскольку простую беспроводную сеть с одной точкой доступа называют *базовым набором служб* (Basic Service Set — BSS), а сеть, состоящую из нескольких точек, — *расширенным набором служб* (Extended Service Set — ESS), то такой идентификатор решили назвать *идентификатором набора служб* (Service Set Identifier — SSID), хотя чаще его называют для краткости просто идентификатором сети. Идентификатор SSID представляет собой текстовую строку длиной не более 32 символов. При конфигурировании беспроводной сети ESS для

всех точек доступа должен быть указан один и тот же идентификатор SSID, чтобы в сети работал роуминг.

Следует также заметить, что многие современные точки доступа поддерживают несколько стандартов беспроводной сети, а в некоторых точках доступа разрешено использовать разные стандарты одновременно. Тем не менее в таком смешанном режиме обычно используются стандарты 802.11b/g в одной и той же точке доступа. Общая производительность беспроводной сети ухудшается. На практике обычно конфигурируют точки доступа для работы со стандартом только 802.11g и в той же зоне покрытия добавляют несколько точек для двух стандартов, b и g, производительность инфраструктуры в таком случае практически не пострадает.

Этап 4. Установка и конфигурирование одного беспроводного клиента

Беспроводным клиентом называют любое радиоустройство, которое может подключиться к точке доступа и работать в беспроводной сети. Чтобы стать беспроводным клиентом, рабочей станции нужна беспроводная сетевая карта (NIC), поддерживающая стандарт, используемый точкой доступа беспроводной сети. В такой сетевой карте есть радиоканал, настраивающийся на частоты используемого стандарта, и антенна. Практически во всех современных портативных персональных компьютерах (laptop) есть встроенная беспроводная сетевая карта, поэтому они могут быть клиентами сетей WLAN.

В точке доступа обычно нужно указывать минимум конфигурационных настроек, для клиента зачастую не нужно вообще. Стандартно в клиентском устройстве отключены все параметры безопасности. Когда клиент запускается, он сканирует все частотные каналы, чтобы обнаружить точки доступа для поддерживаемого им стандарта. Например, если обратиться к рис. 11.6, где показаны три точки доступа, работающие на разных каналах, клиент может в действительности обнаружить их все. Далее клиент выберет из трех одну, от которой он будет принимать наиболее сильный сигнал. Идентификатор SSID также получит клиентское устройство от точки доступа, опять же в таком случае настраивать какие-то параметры не нужно.

Для клиентов WLAN можно использовать беспроводные сетевые интерфейсы от множества производителей. Чтобы быть уверенными, что клиенты смогут работать с беспроводными точками доступа компании Cisco, она запустила *программу совместимых расширений компании Cisco* (Cisco Compatible Extensions Program — CCX). Эта программа спонсируется компанией Cisco, и в ее рамках любой производитель оборудования для беспроводных сетей может отправить свои продукты в лабораторию независимой сторонней компании, которая проведет тесты, чтобы проверить, работает ли, например, беспроводная сетевая карта с точками доступа компании Cisco.

В операционной системе компании Microsoft беспроводная карта также может не требовать настроек благодаря такому средству, как *модуль автоматической конфигурации* (Microsoft Auto Configuration Module — ACM). Это средство, являющееся частью операционной системы, позволяет компьютеру автоматически обнаруживать идентификаторы SSID для всех беспроводных сетей, точки доступа которых находятся в диапазоне досягаемости сетевой карты. Модуль ACM может также автоматически обнаружить и подключаться к точкам доступа с самым сильным сигналом без какого-либо участия пользователей. (Эта функция заменила такое устаревшее средство, как *утилита автоматического конфигурирования беспроводной сети* (Microsoft Zero Configuration Utility — ZCF)).

Кроме того, большинство производителей беспроводных сетевых карт прилагают к ним программное обеспечение для управления картой, которое можно использовать вместо встроенных в операционную систему утилит, таких как ACM компании Microsoft.

Этап 5. Проверка работоспособности сети WLAN с использованием клиента

Первое действие при проверке работоспособности беспроводного клиента в сети — убедиться, что есть доступ к тем же хостам в сети, которые использовались для проверки работоспособности проводной сети на первом этапе. Карта Ethernet компьютера при этом должна быть отключена от сети, чтобы проверялись именно беспроводные коммуникации. Если на этом этапе компьютер получает ответы от дистанционных хостов, например, с помощью команды `ping` или через веб-браузер от сервера, то сеть WLAN как минимум работает.

Если проверка не дает положительного результата, можно использовать несколько методов поиска и устранения неисправностей. Один из наиболее распространенных методов зачастую также используется на стадии планирования сети и называется *картированием сети* (site survey). В процессе картирования беспроводной сети при ее развертывании инженеры обходят место размещения потенциальной сети и выбирают удачные места для установки точек доступа, устанавливают передатчики и измеряют силу сигнала в разных направлениях, в разных точках здания и т.п. Исходя из такого подхода, если новый клиент в беспроводной сети не работает, можно проверить следующие моменты.

Стандартные проблемы при установке сети WLAN и их привязка к картированию сети



- Находится ли точка доступа в центре зоны, к которой относится клиент?
- Нет ли рядом с клиентом или точкой доступа чего-нибудь большого и металлического?
- Нет ли рядом с клиентом или точкой доступа источника помех (и интерференции), например, микроволновой печи или игровой системы?
- Достаточно ли велика зона покрытия точки доступа и находится ли в ней клиент?

Как вариант можно взять портативный компьютер с беспроводной сетевой картой и, используя утилиты для такой карты от производителя, походить по помещению или зданию, поглядывая на индикатор мощности сигнала. Программное обеспечение для большинства беспроводных сетевых плат показывает мощность и качество сигнала, поэтому такая “прогулка” поможет выявить “мертвые зоны” и области наилучшего приема сигнала от точки доступа.

Кроме картирования сети, есть еще несколько стандартных действий, обычно предпринимаемых в таком случае.

Другие стандартные проблемы при развертывании беспроводной сети



- Проверьте, включены ли радиоинтерфейсы точки доступа и беспроводной сетевой карты. В большинстве портативных компьютеров есть переключатель для включения/выключения радиоканала или соответствующая программная настройка. Такая возможность нужна для энергосбережения в портативном компьютере, т.е. увеличения времени автономной работы без подключения

к сети электропитания. Следовательно, если радиоканал выключен, то пользователи не смогут подключиться к беспроводной сети.

- Проверьте версию программного обеспечения (firmware) точки доступа. Желательно, чтобы использовалась самая свежая версия прошивки устройства.
- Проверьте конфигурацию точки доступа, в частности, настройки радиоканала, чтобы убедиться, что используемый канал не перекрывается с каналом другой точки доступа в этой же зоне.

На этом мы закончим рассмотрение первых пяти этапов установки простой беспроводной локальной сети. В последнем разделе описаны методы обеспечения безопасности в сети WLAN, т.е. два последних этапа установки беспроводной сети.

Безопасность беспроводных сетей

В любой современной сети нужна хорошая система безопасности, но требования к безопасности в беспроводных сетях, в силу их природы, намного выше. В этом разделе описаны основные требования к безопасности сетей WLAN, развитие технологий безопасности беспроводных сетей и настройка функции безопасности.

Проблемы безопасности сетей WLAN

В беспроводных сетях есть несколько угроз безопасности, которые напрочь отсутствуют в проводных инфраструктурах Ethernet. Одни из угроз безопасности дают злоумышленникам возможность нанести вред, украв информацию на серверах в проводной корпоративной сети, другие позволяют нарушить работу служб, организовав атаку *отказа в обслуживании* (Denial-of-Service — DoS). Третья могут быть спровоцированы исполненным благих намерений, но плохо информированным сотрудником, который установил беспроводную точку доступа без ведома отдела администрирования сети компании и не настроил в ней функции безопасности. Такая точка позволит любому подключившемуся получить доступ к проводной корпоративной сети.

В сертификационном тесте уровня CCNA компании Cisco требуется знание следующих базовых терминов из сферы безопасности сетей, в частности беспроводных.

- **“Хакеры на колесах”** (war drivers). Этот тип злоумышленников обычно просто хочет воспользоваться бесплатным доступом к Интернету. Такие хакеры просто ездят по какому-то району, обычно на машине, и пытаются найти точку доступа с отключенной защитой или со слабой системой безопасности.
- **Хакеры** (hackers). Конечной целью таких злоумышленников обычно является доступ к какой-либо информации или провокация отказа служб в сети. Конечной целью атаки, чаще всего, является доступ к внутренней сети организации и хостам проводной сети через беспроводную инфраструктуру — в этом случае атака намного проще, чем получение доступа через канал Интернета, защищенный брандмауэрами.
- **Сотрудники** (employees). Конечно же, сотрудники злоумышленниками не являются, тем не менее, они непреднамеренно могут упростить хакерам доступ к внутренней корпоративной сети. Работник компании может пойти в любой компьютерный магазин, купить недорогую точку доступа, установить ее в офисе и создать маленькую беспроводную сеть со стандартными настройка-

ми, т.е. без заданных параметров безопасности. В результате хакер может получить доступ к внутренней корпоративной сети, сидя за столиком кафе через дорогу. Кроме того, если в клиентском устройстве не используется шифрование, передающиеся между легальным компьютером и корпоративной сетью данные могут быть легко перехвачены и скопированы злоумышленниками вне здания.

- **Незарегистрированная точка доступа (rogue AP).** Атакующий захватывает пакеты существующей беспроводной сети, получая таким образом идентификатор SSID, и взламывает ключи безопасности (если они есть). После этого он устанавливает свою собственную точку доступа с теми же настройками, чтобы сотрудники подключались к ней. Таким образом, впоследствии пользователи могут вводить в каких-то службах свои имена и пароли, и такая информация будет перехвачена и использована на следующих этапах взлома сети.

Чтобы уменьшить риск таких атак, в сетях WLAN используются три основных инструмента:

- *взаимная аутентификация (mutual authentication);*
- *кодирование (encryption);*
- *средства обнаружения вторжений (intrusion tool).*

Между точкой доступа и клиентом должна использоваться взаимная аутентификация. В аутентификации используется секретный пароль, называемый ключом, который должен быть установлен на клиенте и точке доступа. Получив кодированное сообщение, точка доступа с помощью сложных математических алгоритмов проверяет, правильный ли ключ передал клиент. Аналогично клиент, получая сообщение от точки доступа, может убедиться в правильности ключа, это и есть взаимная аутентификация — когда два устройства аутентифицируют друг друга. Протокол обмена информацией в этом варианте никогда не пересыпает ключ через беспроводную сеть, следовательно, злоумышленник, даже используя специализированные средства анализа сети и трафика, копируя и анализируя все фреймы, не сможет узнать ключ. Кроме того, поскольку и клиент аутентифицирует точку доступа, он не подключится к незарегистрированной точке, так как в ней нет нужного ключа.

Не менее важным элементом безопасности беспроводной сети является шифрование (encryption). В шифровании используется *закрытый ключ* (secret key) и математический алгоритм для шифрования содержимого фрейма сети WLAN. Устройство-получатель также использует некоторый математический алгоритм для расшифровки данных. Не владея закрытым ключом, злоумышленник сможет перехватить фрейм, но не сможет прочитать его содержимое.

Вспомогательные средства безопасности беспроводных сетей включают в себя различные программные и аппаратные средства обнаружения вторжений. Различают два основных варианта таких средств: *системы обнаружения вторжений* (Intrusion Detection System — IDS) и *системы предотвращения вторжений* (Intrusion Prevention System — IPS); кроме того, существуют специфические средства именно для беспроводных сетей. У компании Cisco есть специализированный термин для описания совокупности таких сетей — *архитектура структурированной беспроводной сети* (Structured Wireless-Aware Network — SWAN). Под этим термином подразумевается

множество инструментов, часть из которых специально предназначена для решения проблем с обнаружением и идентификацией незарегистрированных точек доступа и связанных с ними угроз безопасности. В табл. 11.8 перечислены основные угрозы и методы их нейтрализации.



Таблица 11.8. Угрозы безопасности в беспроводной сети и методы их нейтрализации

Угроза безопасности	Решение проблемы
“Хакеры на колесах”	Защищенные методы аутентификации
Воровство информации хакерами из беспроводных сетей	Устойчивые методы шифрования
Получение доступа к проводной сети хакерами через беспроводную инфраструктуру	Защищенные методы аутентификации
Установка незарегистрированных точек доступа сотрудниками	Системы обнаружения вторжений (Intrusion Detection System — IDS) и архитектура Cisco SWAN
Установка незарегистрированных точек доступа злоумышленниками	Защищенные методы аутентификации, системы IDS и архитектура Cisco SWAN

Развитие стандартов безопасности сетей WLAN

Стандарты безопасности беспроводных сетей развивались постепенно в ответ на все возрастающие требования к системам защиты и усовершенствование средств атаки. В ранних стандартах беспроводных сетей средства их защиты были очень несовершенными. В этом разделе описаны четыре наиболее важных набора стандартов для сетей WLAN в хронологическом порядке, а также их проблемы и основные решения.

ВНИМАНИЕ!

Стандарты WLAN ориентированы в основном на внедрение средств аутентификации и шифрования в соответствующих системах безопасности; эти темы в текущем разделе не рассматриваются. Инструменты, связанные с контролем вторжений (IDS и IPS), в большей мере относятся к методам обеспечения безопасности сети организации и также не рассматриваются ниже.

Первый стандарт безопасности для беспроводных сетей назывался *безопасностью, аналогичной защите проводных сетей* (Wired Equivalent Privacy — WEP), и был очень несовершенным. Три последующих спецификации в основном решали проблемы, обнаруженные в первом стандарте, WEP. Если смотреть на развитие стандартов в хронологическом порядке, то компания Cisco первой предложила усовершенствования стандарта в некоторых собственных (т.е. закрытых и нестандартных) протоколах. Позже промышленный союз производителей беспроводного оборудования, называемый Альянсом Wi-Fi (Wi-Fi Alliance), присоединился к инициативе компании и выпустил всеобщий промышленный стандарт. В конце концов IEEE также завершил работу над открытым стандартом, 802.11i, и ратифицировал его. В табл. 11.9 перечислены четыре основных стандарта сетей WLAN.



Таблица 11.9. Стандарты безопасности беспроводных сетей

Название	Год	Кто выпустил стандарт
Безопасность, аналогичная защите проводных сетей (WEP)	1997	IEEE
Временное решение от компании Cisco в ожидании стандарта 802.11i	2001	Компания Cisco, протокол стандарта 802.1x — расширяемый протокол аутентификации (Extensible Authentication Protocol (EAP) Института IEEE
Защищенный беспроводной доступ (Wi-Fi Protected Access — WPA)	2003	Альянс Wi-Fi
802.11i (WPA2)	2004	IEEE

Слово *стандарт* используется в этой книге и во многих других достаточно небрежно при описании методов обеспечения безопасности в беспроводных сетях. Некоторые спецификации в действительности являются настоящими открытыми стандартами, например спецификации IEEE. Другие спецификации были изданы Альянсом Wi-Fi и стали промышленными стандартами де-факто. Кроме того, компания Cisco создала несколько промежуточных временных решений для своих продуктов, чтобы ускорить развитие беспроводных сетей, но такие спецификации не являются стандартами в общепринятом понимании этого термина. Тем не менее все варианты решений позволили улучшить оригинальный метод безопасности WEP и оказали существенное влияние на развитие технологий беспроводных сетей, поэтому мы их опишем.

Стандарт WEP

Технология WEP была частью первого стандарта 802.11 и обеспечивала службы аутентификации пользователей и шифрования данных. Как впоследствии выяснилось, она использовала слабо защищенные методы аутентификации и шифрования и на сегодняшний день может быть взломана за считанные минуты с помощью широко распространенного хакерского программного обеспечения. Две основные проблемы средств безопасности WEP состоят в следующем.

- Используются **статические предварительно распределляемые ключи** (Preshared Static Key — PSK). Значение ключа должно быть предварительно указано в каждом клиентском устройстве и точке доступа, и нет никаких методов динамического обмена ключами без вмешательства человека. Как следствие, многие пользователи и системные администраторы не заботятся о периодической смене ключей, в особенности в крупных организациях, где есть большое или очень большое количество беспроводных подключений.
- **Ключи легко взламываются** (т.е. расшифровываются). Длина ключа не очень велика — 64 бита, из которых только 40 действительно относятся к самому ключу. Поэтому легко предсказать значение ключа, если в течение определенного времени прослушивать фреймы беспроводной сети. Опять же, если ключ никогда не меняется или меняется очень редко, хакер может накопить большое количество примеров запросов на аутентификацию, что еще сильнее упрощает процесс расшифровки ключа.

Из-за указанных недостатков технологии WEP, а также поскольку новые стандарты включают в себя усовершенствованные функции безопасности, механизм WEP на сегодняшний день не следует использовать.

Маскировка идентификатора SSID и фильтрация MAC

Итак, когда выяснилось, что в стандарте WEP есть множество проблем, многие производители включили в свои продукты несколько функций защиты, которые к оригинальному стандарту никакого отношения не имели. Тем не менее многие потребители ассоциировали эти функции с технологией WEP просто потому, что время их выпуска практически совпало с ней. Ни одна из функций так и не стала частью какого-либо стандарта, и они не обеспечивают какой-то реальной безопасности сети, однако их нужно рассмотреть, поскольку они упоминаются во многих описаниях.

Первая функция, *маскировка идентификатора SSID* (SSID cloaking), изменяет процесс ассоциации клиентского устройства с точкой доступа. Перед тем как использовать точку доступа, клиент должен знать о ней некоторый минимум необходимой информации, в частности значение идентификатора SSID сети. В нормальных условиях процесс ассоциации выглядит указанным ниже образом.

- Этап 1** Точка доступа рассыпает *фрейм-бакен* (beacon frame), обычно каждые 100 мс, в котором содержится значение SSID и другая конфигурационная информация.
- Этап 2** Клиент прослушивает все каналы, чтобы обнаружить фреймы-бакены и найти все близлежащие точки доступа.
- Этап 3** Клиент ассоциируется с точкой доступа, от которой получен самый сильный сигнал (стандартное поведение), или с точкой доступа с максимальным сигналом для предпочтительного идентификатора SSID.
- Этап 4** Как только клиент ассоциировался с точкой доступа, выполняется процесс аутентификации клиента.

По существу, клиент узнает о существовании точек доступа и связанных с ними идентификаторами SSID из фреймов-бакенов. Такой механизм упрощает работу технологии роуминга, позволяя клиенту перемещаться в пространстве и ассоциироваться с новой точкой доступа, когда сигнал от старой заметно падает. Тем не менее фреймы-бакены — это отличное подспорье для злоумышленников, которые легко и быстро могут получить информацию о точках доступа и попытаться подключиться к ним, чтобы получить доступ к сети.

Маскировка идентификатора SSID — это специальная функция точки доступа, которая отключает периодическую рассылку фреймов-бакенов. Такой подход вроде бы должен решить проблемы со злоумышленниками, сканирующими точки доступа в сети. Тем не менее легальные клиенты тоже должны найти точки в сети. Следовательно, клиент должен быть настроен со специальным значением идентификатора SSID, называемым нулевым, или пустым (null). Клиент отправляет *сообщение-запрос* (probe), которое заставляет точку доступа передать свое значение SSID. Короче говоря, очень просто заставить точку доступа анонсировать свой идентификатор SSID, даже в том случае, когда маскировка включена. Таким образом, хакеры все равно могут обнаружить все точки доступа в сети.

ВНИМАНИЕ!

В сетях разных организаций используется технология маскировки идентификатора SSID, чтобы предотвратить попытки доступа к беспроводной сети из любопытства. В открытых точках доступа, наоборот, рассылаются фреймы-бакены, чтобы пользователи могли легко найти нужную.

Еще одна дополнительная функция, часто реализуемая совместно с технологией WEP, — фильтрация MAC-адресов. В точке доступа может быть настроен список разрешенных в беспроводной сети MAC-адресов, остальные адреса будут отфильтровываться. Фильтрация MAC-адресов может отбить охоту у любопытных пользователей подключиться к беспроводной сети, но она не поможет отразить реальную атаку. Злоумышленник может использовать беспроводную сетевую карту, в которой разрешается менять MAC-адрес, скопировать легальные фреймы себе, узнать из них нужный MAC-адрес, установить его в своем адаптере и таким образом обойти фильтр.

Временное решение компании Cisco до принятия стандарта 802.11i

Из-за вполне очевидных недостатков технологии WEP многие производители оборудования, например, компания Cisco, промышленная ассоциация Альянс Wi-Fi и другие попытались решить проблему за счет своих собственных стандартов, которые соперничали с медленно разрабатываемыми спецификациями IEEE. В решении компании Cisco использовались некоторые собственные улучшения механизма шифрования совместно со стандартной аутентификацией пользователя IEEE 802.1x. К основным улучшениям компанией Cisco исходной технологии можно отнести:

- механизм динамического обмена ключами (вместо статических предварительно распределемых);
- использование аутентификации стандарта 802.1x;
- генерация нового ключа для каждого передаваемого пакета.

Использование механизма динамического обмена ключами значительно улучшает систему, поскольку клиент и точка доступа могут менять пароль очень часто, причем без вмешательства человека. В результате, даже если ключ взломан (т.е. расшифрован злоумышленником), им можно воспользоваться только в короткий отрезок времени. Более того, если ключи распределяются динамически, для каждого пакета может генерироваться собственный ключ, которым он зашифрован. В таком случае, даже если злоумышленник получит (расшифрует или подберет) ключ, он сможет расшифровать только один-единственный пакет, что сильно улучшает систему безопасности.

Компания Cisco разработала несколько функций, основанных на известной на тот момент (момент разработки) информации о стандарте безопасности беспроводных сетей IEEE 802.11i. Кроме того, в разработке компании используется аутентификация пользователей, т.е. после аутентификации устройства с помощью ключа (проверки того, что в устройстве установлен правильный ключ) пользователь должен ввести свое имя и пароль. Такой дополнительный этап добавляет еще один уровень безопасности в систему: даже если ключи аутентификации временно скомпрометированы, злоумышленник должен знать имя и пароль аутентификации пользователя, чтобы получить доступ к беспроводной сети.

Защищенный доступ Wi-Fi (WPA)

В усовершенствованном компанией Cisco варианте технологии WEP использовались как собственные протоколы, так и открытый стандарт IEEE 802.1x. После того как компания включила новый механизм защиты в свои точки доступа, Альянс Wi-Fi разработал общий стандарт безопасности для совмещения устройств от разных изготовителей. IEEE в это время как раз разрабатывал новую спецификацию безо-

пасности для сетей WLAN, 802.11i, но очень медленно, а производители оборудования должны были реагировать на потребности быстрорастущего рынка и не могли долго ждать. Поэтому Альянс Wi-Fi взял копию стандарта 802.11i, который как раз находился в стадии разработки, изучил его, сделал некоторые предположения и допущения и издал его как рекомендацию, которая впоследствии стала стандартом де-факто. Затем Альянс провел обычную процедуру сертификации оборудования разных производителей на предмет того, соответствует ли оно требованиям нового стандарта или нет, а стандарт получил название *защищенный беспроводной доступ* (Wi-Fi Protected Access — WPA).

Технология WPA фактически содержит те же функции, которые имелись во временном решении компании Cisco, но отличающиеся в деталях. В стандарте WPA также используется динамический обмен ключами на основе *протокола целостности временного ключа* (Temporal Key Integrity Protocol — TKIP); в решении от компании Cisco использовалась нестандартная реализация протокола TKIP. В стандарте WPA также разрешено использовать либо стандартную аутентификацию пользователей IEEE 802.1X, либо простую аутентификацию устройств с использованием *предварительно распределемых ключей* (preshared keys). В качестве метода шифрования использовался *алгоритм проверки целостности сообщений* (Message Integrity Check — MIC), который очень похож на собственный метод компании Cisco.

У технологии WPA есть два больших достоинства. Во-первых, функции безопасности значительно лучше, чем в стандарте WEP; во-вторых, программа сертификации устройств Альянса Wi-Fi была с энтузиазмом воспринята производителями и имела огромный успех. Все старались пройти сертификацию Альянса, следовательно, поддерживали и внедряли технологию WPA в свои устройства. В результате производители персональных компьютеров могли выбрать для установки практически любую из множества сетевых карт, а потребители могли купить точку доступа любого производителя и быть уверенными, что она заработает в их сети и будет поддерживать технологию WPA.

ВНИМАНИЕ!

Собственное решение компании Cisco и промышленный стандарт WPA несовместимы.

Стандарт IEEE 802.11i и WPA-2

IEEEratифицировал стандарт 802.11i в 2005 году, дополнительные связанные с ним спецификации появились позже. Как в собственном решении компании Cisco и в промышленном стандарте WPA Альянса Wi-Fi, в спецификации 802.11i используется механизм динамического обмена ключами, более мощный алгоритм шифрования и аутентификации пользователей. Тем не менее многие детали спецификаций отличаются, поэтому стандарт 802.11i не совместим ни с технологией WPA, ни с собственным решением компании Cisco.

Существенным и важным улучшением по сравнению с временными решением от компании Cisco и стандартом WPA стало использование *улучшенного стандарта шифрования* (Advanced Encryption Standard — AES) в технологии 802.11i. Метод AES обеспечивает намного лучшее шифрование, чем технология компании Cisco, не говоря уже о стандарте WPA, использует ключи большей длины и мощный алгоритм.

Альянс Wi-Fi продолжает играть важную роль в сертификации продуктов, в частности выполняет проверку совместимости со спецификацией 802.11i, но использует другое название для этого стандарта. Поскольку успех технологии WPA в качестве промышленного стандарта был ошеломляющим, а термин “WPA” стал очень популярен, Альянс назвал стандарт 802.11i “WPA2”, подразумевая под ним вторую версию стандарта WPA. Следовательно, покупая или конфигурируя устройства, в документации и настройках вы скорее увидите название WPA2, а не 802.11i.

В табл. 11.10 перечислены ключевые особенности разных стандартов безопасности беспроводных сетей.

Таблица 11.10. Сравнение характеристик стандартов безопасности беспроводных сетей



Стандарт	Метод распределения ключей	Аутентификация устройств	Аутентификация пользователей	Шифрование
WEP	Статическое	Да (слабая)	Нет	Да (слабое)
Cisco	Динамическое	Да	Да (802.1x)	Да (TKIP)
WPA	И статическое, и динамическое	Да	Да (802.1x)	Да (TKIP)
802.11i (WPA2)	И статическое, и динамическое	Да	Да (802.1x)	Да (AES)

Подготовка к экзамену

Повторите все ключевые темы

Повторите все ключевые темы данной главы, помеченные пиктограммой “Ключевая тема”. Ключевые темы и соответствующие им страницы перечислены в табл. 11.11.

Таблица 11.11. Ключевые темы главы 11

Элемент	Описание	Страница
Табл. 11.2	Организации по стандартизации сетей WLAN	334
Табл. 11.3	Сравнение стандартов 802.11a, 802.11b и 802.11g	335
Табл. 11.4	Режимы работы сетей WLAN, их формальные названия и описание	336
Табл. 11.5	Нелицензируемые диапазоны частот, определенные Комитетом FCC	338
Рис. 11.6	Использование неперекрывающихся каналов DSSS диапазона 2,4 ГГц в сети ESS	340
Список	Этапы реализации беспроводной сети	345
Список	Стандартные проблемы при установке сети WLAN и их привязка к картированию сети	349
Список	Другие стандартные проблемы при развертывании беспроводной сети	349
Табл. 11.8	Угрозы безопасности в беспроводной сети и методы их нейтрализации	352
Табл. 11.9	Стандарты безопасности беспроводных сетей	353
Табл. 11.10	Сравнение характеристик стандартов безопасности беспроводных сетей	357

Заполните таблицы и списки по памяти

Распечатайте приложение М (Appendix L) с компакт-диска или его раздел, относящийся к этой главе, и заполните таблицы и списки по памяти. В приложении Н (Appendix M) приведены заполненные таблицы и списки для самоконтроля.

Ключевые термины

Дайте определения перечисленных ниже терминов и проверьте правильность их написания в списке терминов:

стандарты 802.11a, 802.11b, 802.11g, 802.11i, 802.11n; точка доступа (access point), одноранговый режим (ad hoc mode), базовый набор служб (Basic Service Set — BSS), метод предотвращения коллизий CSMA/CA (CSMA/CA), метод расширения спектра сигнала прямой последовательности (Direct Sequence Spread Spectrum — DSSS), расширенный набор служб (Extended Service Set — ESS), метод расширения спектра со скачкообразным изменением частоты (Frequency Hopping Spread Spectrum — FHSS), режим инфраструктуры (infrastructure mode), мультиплексирование с ортогональным частотным разделением сигналов (Orthogonal Frequency Division Multiplexing — OFDM), идентификатор набора служб (Service Set Identifier — SSID), Альянс Wi-Fi (Wi-Fi Alliance), технология WPA (Wi-Fi Protected Access — WPA), стандарт WEP (Wired Equivalent Privacy — WEP), клиент беспроводной сети (WLAN client), технология WPA2 (WPA2).

В этой части рассмотрены следующие темы экзамена Cisco ICND1¹...

Разработка схемы IP-адресации и служб IP в небольшой сети филиала:

- описаны задачи и роль адресации в сети;
- разработка и применение схемы адресации в сети;
- присвоение допустимых IP-адресов хостам, серверам, сетевым устройствам в среде локальной сети и их проверка;
- описана работа и преимущества использования частной и открытой IP-адресации;
- выявление и исправление проблем IP-адресации.

¹ Текущие темы сертификационного экзамена приведены на сайте <http://www.cisco.com>. — Примеч. авт.

Часть III. IPv4-адресация и создание подсетей

Глава 12. “Перспективы создания подсетей IPv4”

Глава 13. “Анализ классовых сетей IPv4”

Глава 14. “Преобразование маски подсети”

Глава 15. “Анализ существующих масок подсети”

Глава 16. “Разработка маски подсети”

Глава 17. “Анализ существующих подсетей”

Глава 18. “Поиск всех идентификаторов подсети”

В этой главе...

- **Введение в подсети.** Описывается весь процесс создания подсетей и разделение сети на меньшие группы, называемые подсетями.
- **Анализ потребности в подсетях и адресации.** Анализируется, где в реальной топологии сети необходимы подсети. Кроме того, обсуждается концепция размера подсети, который определяют потребности бизнеса.
- **Выбор проекта.** Правила IP-адресации и создания подсетей позволяют сетевым инженерам выбрать подходящий проект. В частности, выбрать используемую сеть IP и маску. В этом разделе обсуждается, что следует учесть при выборе.
- **Реализация плана.** Завершается обсуждение проектирования и начинается описание реализации проекта, включая перечень идентификаторов подсетей, используемых в конкретных местах сетевой топологии, а также какие именно IP-адреса использовать для различных устройств.

ГЛАВА 12

Перспективы создания подсетей IPv4

Большинство простых задач по сетям требует, чтобы при работе и поиске неисправностей использовался уже существующий план подсетей и IP-адресации. Экзамены CCENT и CCNA оценивают вашу готовность использовать уже существующую информацию об IP-адресации и подсетях для решения типичных задач, таких как контроль сети, реакция на возможные проблемы и их устранение.

Даже если не вы разрабатывали сеть, с которой предстоит работать, чем лучше понимаешь ее проект, тем проще ее использовать. Процесс мониторинга какой-нибудь сети требует непрерывного ответа на вопрос: работает ли сеть так, как задумано? Если проблема есть, следует задаться таким вопросом: что происходит, когда сеть работает нормально и что сейчас не так? Оба вопроса требуют понимания проекта сети, включая подробности IP-адресации и подсетей.

В текущей главе рассматривается общий процесс проектирования подсетей и IP-адресации. Далее, в главах 13–18, исследуются различные аспекты создания подсетей. Каждая из этих глав рассматривает один из двух подходов к теме: *оперативный подход* (operational approach), требующий анализа существующей адресации и подсети, и *проектный подход* (design approach), требующий размышлений о выборе, который необходимо сделать при разработке схемы адресации и подсетей корпоративной сети.

Контрольные вопросы: знаете ли вы уже темы главы

Этот раздел предназначен для того, чтобы читатель мог предварительно оценить свои знания и решить, нужно ли ему читать главу целиком. Если ответы на девять из десяти вопросов даны правильно, можно сразу же перейти к последнему разделу “Подготовка к экзамену”. Основные темы этой главы и предварительных контрольных вопросов перечислены в табл. 12.1. Отвечая на контрольные вопросы и используя таблицу, читатель сможет достаточно точно определить свои знания в той или иной области. Ответы на вопросы приведены в приложении А.

Таблица 12.1. Темы контрольных вопросов

Основная тема	Номера вопросов
Анализ потребности в подсетях и адресации	1–3
Выбор проекта	4–8

- Хост A — это компьютер, подключенный к коммутатору SW1 и присвоенный сети VLAN 1. Чему из приведенного ниже обычно назначается IP-адрес в той же подсети, что и хост A? (Выберите два ответа).

- а) Интерфейс WAN локального маршрутизатора.
 - б) Интерфейс LAN локального маршрутизатора.
 - в) Все остальные хосты, подключенные к тому же коммутатору.
 - г) Другие хосты, подключенные к тому же коммутатору, а также к сети VLAN 1.
2. Почему формула расчета количества хостов в подсети ($2^H - 2$) требует вычитания 2 адресов хостов?
- а) Чтобы зарезервировать два адреса для избыточных стандартных шлюзов (маршрутизаторов).
 - б) Чтобы зарезервировать два адреса, необходимых для работы DHCP.
 - в) Чтобы зарезервировать адреса для идентификатора подсети и стандартного шлюза (маршрутизатора).
 - г) Чтобы зарезервировать адреса для широковещательного адреса подсети и идентификатора подсети.
3. Сеть класса В должна быть разделена на подсети так, чтобы в результате она обеспечила 100 подсетей по 100 хостов на подсеть. Какие из следующих ответов перечисляют подходящую комбинацию количеств битов сети, подсети и хоста? (Выберите два ответа).
- а) Сеть = 16, подсеть = 7, хост = 7.
 - б) Сеть = 16, подсеть = 8, хост = 8.
 - в) Сеть = 16, подсеть = 9, хост = 7.
 - г) Сеть = 8, подсеть = 7, хост = 17.
4. Какая из приведенных ниже сетей IP является частной? (Выберите несколько ответов.)
- а) 172.31.0.0.
 - б) 172.32.0.0.
 - в) 192.168.255.0.
 - г) 192.1.168.0.
 - д) 11.0.0.0.
5. Какая из приведенных ниже сетей IP является открытой? (Выберите несколько ответов.)
- а) 9.0.0.0.
 - б) 172.30.0.0.
 - в) 192.168.255.0.
 - г) 192.1.168.0.
 - д) 1.0.0.0.
6. Какие части структуры IP-адресов должны уже существовать в сети класса В 172.16.0.0 прежде, чем она будет разделена сетевым инженером на подсети? (Выберите несколько ответов.)
- а) Сети.

б) Подсети.

в) Хоста.

г) Широковещания.

7. Сетевой инженер уделяет время обдумыванию всей сети класса В 172.16.0.0 и ее разделению на подсети. Затем он решает, как разделить эту сеть класса В на подсети, создает план адресации и подсетей на бумаге, демонстрируя свой выбор. Если сравнить его представление об этой сети до создания подсетей и после, то каковы будут изменения структуры частей адресов в этой сети?

а) Часть подсети станет меньше.

б) Часть хоста станет меньше.

в) Часть сети станет меньше.

г) Часть хоста будет удалена.

д) Часть сети будет удалена.

8. Какой из следующих терминов не используется для обозначения одного числа в каждой подсети, обычно однозначно определяющего подсеть? (Выберите несколько ответов.)

а) Идентификатор подсети (subnet ID).

б) Номер подсети (subnet number).

в) Широковещательный адрес подсети (subnet broadcast).

г) Имя подсети (subnet name).

д) Адрес подсети (subnet address)

Основные темы

Введение в подсети

Предположим, вам случилось попасть в магазин, когда там продавали самый длинный в мире бутерброд. Вы хотите есть, поэтому и зашли сюда. Теперь у вас есть один бутерброд, но длиной он больше двух километров. Вы понимаете, что это немного больше, чем необходимо на обед. Чтобы сделать бутерброд более употребляемым (и переносимым), вы делите его на меньшие части и раздаете их другим людям вокруг вас, которые также не против пообедать.

На самом деле основная концепция создания подсетей очень похожа на случай с бутербродом. Вы начинаете с одной сети, но это только одна большая сеть. Как единый большой объект, она не очень полезна. Чтобы сделать ее более полезной, вы разделяете ее на меньшие части, называемые *подсетями* (subnet), а получив эти подсети, используете их в различных частях объединенной корпоративной сети.

Этот раздел — краткое введение в создание подсетей IP. Вначале будут представлены общие концепции проектирования подсетей, когда одну сеть (или подсеть) действительно разделяют на подсети. В остальной части этого раздела описаны многочисленные этапы, которые необходимо пройти, чтобы создать подсеть именно такого проекта. К концу этого раздела вы должны иметь представление о том, что происходит на последующих этапах создания подсетей, обсуждаемых в остальной части данной главы.

Создание подсетей на простом примере

Сеть IP (IP network) — другими словами, есть класс A, B или C — это просто набор последовательно пронумерованных IP-адресов, которые подчиняются неким предварительно установленным правилам. Правила классов A, B и C, приведенные в главе 5, устанавливают, что у всех адресов определенной сети есть одинаковое значение некоторых из октетов адресов. Например, сеть класса B 172.16.0.0 состоит из IP-адресов, которые начинаются с части 172.16: 172.16.0.0, 172.16.0.1, 172.16.0.2 и так далее до 172.16.255.255. Другой пример: сеть класса A 10.0.0.0 включает все адреса, которые начинаются с 10.

Подсеть IP (IP subnet) — это просто подмножество сетей класса A, B или C. На самом деле термин *подсеть* — это сокращение от *подразделенная сеть*. Например, одна подсеть сети класса B 172.16.0.0 могла бы быть набором всех IP-адресов, которые начинаются с 172.16.1 и включали бы адреса 172.16.1.0, 172.16.1.1, 172.16.1.2 и так далее до 172.16.1.255. Другая подсеть той же сети класса B могла бы включать все адреса, начинающиеся с 172.16.2.

Чтобы дать общее представление, на рис. 12.1 приведена базовая документация окончательного проекта подсети, которая получится после разделения сети класса B 172.16.0.0.

Проект демонстрирует пять подсетей: по одной для каждой из трех локальных сетей и по одной для каждой из двух последовательных связей. Текстовые примечания — это пояснения, используемые инженером для подсетей: каждая подсеть включает адреса с одинаковым значением первых трех октетов. Например, число 172.16.1.__ для сети LAN слева означает “все адреса начиная с 172.16.1”. Обратите также внимание на то, что данный проект использует не все адреса сети класса B 172.16.0.0, таким образом, инженер оставил достаточно много места для роста.

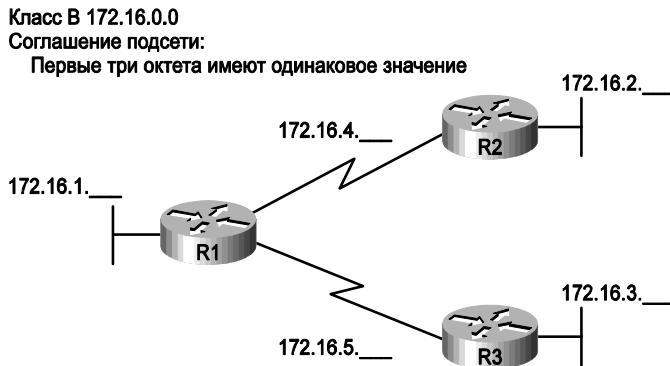


Рис. 12.1. Пример плана подсети

Оперативный или проектный подход к созданию подсетей

Большинство информационных задач требует, чтобы подсети создавались с учетом оперативного представления. Таким образом, прежде чем вы получите свою задачу, некто другой разработает то, как будет работать IP-адресация и подсети в данной конкретной корпоративной сети. Со временем этот проект может измениться, но когда вы создаете подсеть, необходимо интерпретировать то, что некто уже выбрал.

Чтобы полностью понять IP-адресацию и подсети, необходимо рассмотреть их как с точки зрения проектного подхода, так и оперативного. Например, рис. 12.1 просто утверждает, что первые три октета во всех этих подсетях совпадают. Некий инженер, который работал до вас, уже выбрал проект. Почему он выбрал именно это соглашение? Какие альтернативы существуют? Может быть, эти альтернативы были бы сейчас лучше для данной объединенной сети? Все эти вопросы имеют отношение больше к проектному подходу создания подсетей, а не к оперативному.

Чтобы помочь оценить обе точки зрения, в некоторых главах этой части больше внимания уделяется проблемам проектирования, а не другим операциям при интерпретации некоего существующего проекта. В данной главе описан весь процесс проектирования, чтобы представить всю картину создания подсетей IP. Далее, в остальных главах этой части, каждая тема данной главы будет описана подробно либо с точки зрения оперативного подхода, либо проектного.

В трех остальных разделах текущей главы исследуется каждый из этапов, показанных на рис. 12.2.

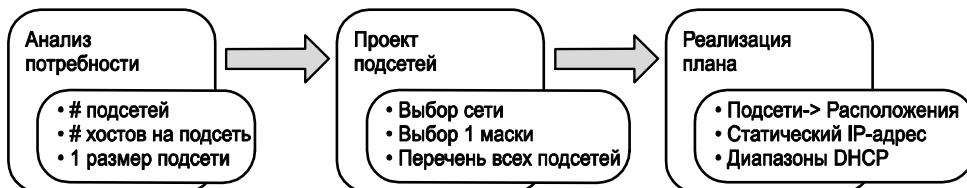


Рис. 12.2. Планирование, проектирование и реализация подсети

ПРИМЕЧАНИЕ АВТОРА

В этой главе демонстрируется набор функций, вовлеченных в формальный процесс проектирования Cisco, называемый *подготовка, план, проект, реализация, работа и оптимизация* (Prepare, Plan, Design, Implement, Operate, Optimize — PPDIOO).

Анализ потребности в подсетях и адресации

В данном разделе обсуждается значение четырех простых вопросов, применяемых при анализе потребности в адресации и создании подсетей для любой новой или изменяющейся корпоративной сети.

1. Какие хосты должны группироваться в подсеть?
2. Сколько подсетей требует данная сеть?
3. Сколько IP-адресов хоста требует каждая подсеть?
4. Будет ли использован для простоты одинаковый размер подсети или нет?

Правила расположения хостов в определенной подсети

У каждого устройства, подключенного к объединенной сети IP, должен быть IP-адрес. К этим устройствам относятся компьютеры, используемые конечными пользователями, серверы, мобильные телефоны, портативные компьютеры, телефоны IP, планшеты и такие сетевые устройства, как маршрутизаторы, коммутаторы и брандмауэры. Короче говоря, в IP-адресе нуждается любое устройство, которое использует протокол IP для передачи и получения пакетов.

ВНИМАНИЕ!

При обсуждении IP-адресации у термина *сеть* (network) есть вполне специфическое значение: сеть IP класса A, B или C. Во избежание недоразумений при использовании термина *сеть* при описании набора хостов, маршрутизаторов, коммутаторов и так далее в этой книге используются термины *объединенная сеть* (internetwork) и *корпоративная сеть* (enterprise network).

IP-адреса должны назначаться согласно некоторым простым правилам и на серьезных основаниях. Для эффективной работы маршрутизации и правил IP-адресации адреса группируют в группы, называемые подсетями. Эти правила приведены ниже.

**Основные факты о подсетях**

- Адреса в той же подсети не отделяются маршрутизатором.
- Адреса в различных подсетях разделены по крайней мере одним маршрутизатором.

На рис. 12.3 представлена общая концепция с хостами A и B в одной подсети и хостом C в другой. Обратите, в частности, внимание на то, что хосты A и B не отделены друг от друга никакими маршрутизаторами, а хост C отделен от хостов A и B по крайней мере одним маршрутизатором, следовательно, он находится в другой подсети.

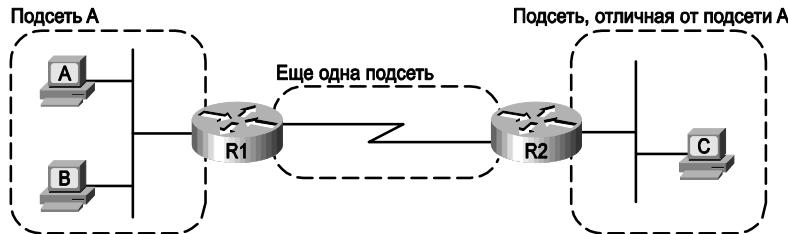


Рис. 12.3. Компьютеры A и B — в одной подсети, а компьютер C — в другой

Концепция, согласно которой хост на том же канале должен находиться в той же подсети, очень похожа на концепцию почтового индекса. Все почтовые адреса в одном городе имеют одинаковый почтовый код (почтовый индекс). Адреса в другом городе, расположенном поблизости или на другом конце страны, имеют другой почтовый код. Почтовый код позволяет почтовой службе автоматизировать сортировку почты, чтобы доставлять ее в соответствующее место. По той же причине хосты одной локальной сети находятся в той же подсети, а хосты разных локальных сетей — в разных подсетях.

Обратите внимание на то, что двухточечный канал связи WAN на рисунке также нуждается в подсети. Маршрутизатор R1 на рис. 12.3 подключен к подсети LAN слева и к подсети WAN — справа. Маршрутизатор R2 подключен к той же подсети WAN. Для этого оба маршрутизатора, R1 и R2, будут иметь IP-адреса на своих интерфейсах WAN, и адреса эти будут в той же подсети.

И наконец, поскольку основная задача маршрутизаторов — перенаправить пакеты из одной подсети в другую, маршрутизаторы обычно подключены к нескольким подсетям. В данном случае, например, маршрутизатор R1 соединен с одной подсетью LAN слева и одной подсетью WAN — справа. Для этого маршрутизатор R1 будет настроен с двумя разными IP-адресами на каждом интерфейсе. Эти адреса будут находиться в разных подсетях, поскольку интерфейсы соединяют маршрутизатор с разными подсетями.

Определение количества подсетей

Чтобы определить количество требуемых подсетей, инженер должен обдумать документацию объединенной сети и применить приведенные ниже правила. Для этого ему нужен доступ к схемам сетей, подробностям конфигурации VLAN и, если используются глобальные сети WAN Frame Relay, подробности о *постоянных виртуальных каналах* (Permanent Virtual Circuit — PVC). На основании этой информации, используя соответствующие правила, можно спланировать одну или все подсети.

Какие места в сетевой топологии нуждаются в подсети

- Сеть VLAN.
- Двухточечный последовательный канал связи.
- Канал PVC Frame Relay



ВНИМАНИЕ!

Технология Frame Relay предоставляет и другие возможности создания подсетей, помимо одной подсети на каждый канал PVC, но в этой главе основное внимание следует сосредоточить на создании подсетей с учетом только одной подсети на каждый канал PVC.

Предположим, например, что для проектирования подсети у сетевого инженера есть только схема, приведенная на рис. 12.4.

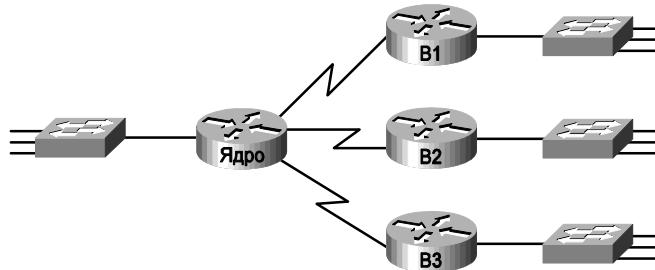
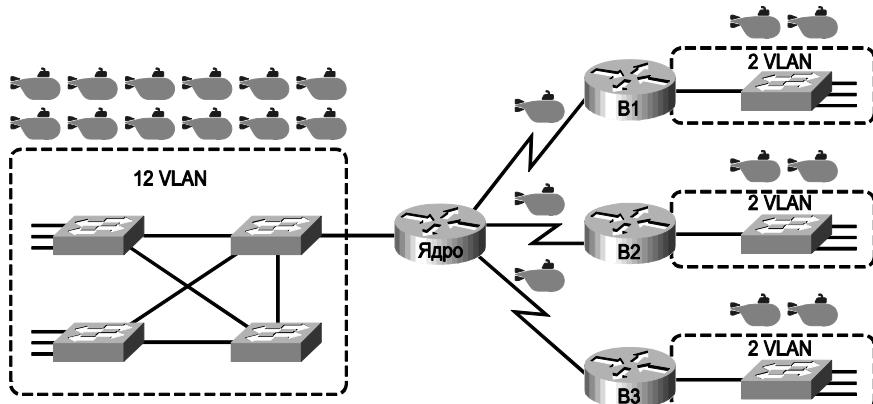


Рис. 12.4. Площадка четырех объединенных сетей с маленькой центральной площадкой

На основании только этой схемы количество необходимых подсетей не может быть предсказано полностью. Конечно, три подсети будут необходимы для каналов связи сетей WAN, по одной на канал. Но каждый коммутатор сети LAN может быть подключен к одной сети VLAN или к нескольким. Как можно убедиться, на каждой площадке необходима по крайней мере одна подсеть для сети LAN, но может понадобиться и больше.

Теперь рассмотрим более подробную версию той же схемы, представленную на рис. 12.5. В данном случае на рисунке показано количество сетей VLAN в дополнение к равноправному уровню 3 топологии (маршрутизаторы и каналы связи, подключенные к маршрутизаторам). Здесь также показано, что у центральной площадки есть еще несколько коммутаторов, но ключевой факт представлен слева: независимо от количества имеющихся коммутаторов, центральная площадка имеет в общей сложности 12 сетей VLAN. Аналогично на рисунке каждая ветвь представлена как имеющая две сети VLAN. Наряду с теми же тремя подсетями WAN эта объединенная сеть требует 21 подсеть.



Легенда:



Рис. 12.5. Площадка четырех объединенных сетей с несколько большей центральной площадкой

И наконец, в реальном случае следовало бы рассмотреть нынешние потребности объединенной сети с учетом ее ожидаемого роста в будущем. Любой план подсетей должен включать реалистичную оценку количества подсетей, необходимых для удовлетворения будущих потребностей.

Определение количества хостов в каждой подсети

Определение количества хостов в подсети требует знания нескольких простых концепций, небольшого последующего исследования и опроса. Каждое устройство, подключенное к подсети, нуждается в IP-адресе. Для совершенно новой сети можно просмотреть бизнес-план — количество людей в подразделении, заявленные устройства — и таким образом получить некоторое представление о возможном количестве устройств. При расширении существующей сети, чтобы добавить новые площадки, можно использовать существующие площадки как объект для сравнения, а затем выяснить, какие площадки станут больше или меньше. И не забывайте учитывать IP-адрес интерфейса маршрутизатора в каждой подсети и IP-адрес коммутатора для дистанционного управления им.

Вместо того чтобы собрать данные по каждой площадке, для планирования зачастую используют лишь несколько типичных площадок. Предположим, например, что имеется несколько больших коммерческих офисов и несколько меньших. В этом случае можно досконально изучить только один большой офис и только один малый. Добавьте в анализ тот факт, что магистральные линии в подсети нуждаются только в двух адресах, а также в большом количестве уникальных в своем роде подсетей, и вот достаточно информации, чтобы планировать проект адресации и подсетей.

Например, на рис. 12.6 показано, что инженер построил схему, демонстрирующую количество хостов подсети LAN в наибольшей ветви, B1. Для двух других ветвей инженер не потрудился выяснить количество необходимых хостов. Пока количество необходимых IP-адресов площадок B2 и B3 остается ниже оценки 50, инженер может запланировать на основании большей площадки B1 по 50 хостов в каждой ветви подсети LAN и иметь достаточно много адресов на подсеть.

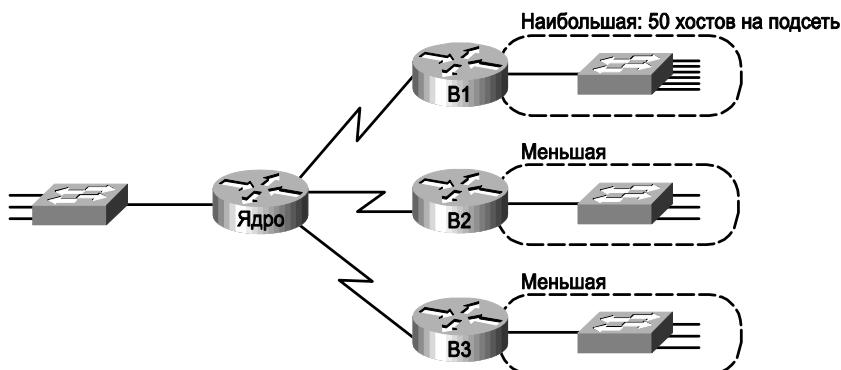


Рис. 12.6. Большая ветвь B1 с 50 хостами в подсете

Будут ли подсети одного размера

Последний выбор на начальном этапе планирования — будете ли вы использовать упрощенный проект по принципу “все подсети одного размера”. Размер подсети (или ее длина) — это количество IP-адресов, пригодных для использования в подсети. Проект может подразумевать использование подсетей одинакового размера или разных размеров. У каждого из вариантов есть свои преимущества и недостатки.

Определение размера подсети

Прежде чем закончить чтение этой книги, читатель изучит все подробности определения размера подсети, а пока достаточно знать лишь несколько специфических фактов о размере подсетей. Более подробную информацию по этой теме см. в главах 13–15.

Инженер назначает каждой подсети *маску подсети* (subnet mask), и эта маска, между прочим, как раз и определяет размер подсети. Маска резервирует количество битов *хоста* (host bit), задача которых — различать IP-адреса хостов в этой подсети. Поскольку с помощью x битов можно нумеровать 2^x сущностей, если маска определяет H битов хоста, подсеть может содержать 2^H индивидуальных числовых значений.

Однако размер подсети не 2^H , а $2^H - 2$, поскольку два числа в каждой подсети зарезервированы для других целей. Каждая подсеть резервирует наименьшее значение для *адреса подсети* (subnet number) и самое большое — для *широковещательного адреса подсети* (subnet broadcast address). В результате количество пригодных для использования IP-адресов в подсети составляет $2^H - 2$.

ВНИМАНИЕ!

Термины *номер подсети* (subnet number), *идентификатор подсети* (subnet ID) и *адрес подсети* (subnet address) описывают число, представляющее или идентифицирующее подсеть.

На рис. 12.7 представлена общая концепция трех частей структуры IP-адреса, с акцентом на часть хоста и результирующий размер подсети.



Рис. 12.7. Концепции размера подсети

Все подсети одного размера

Чтобы использовать в сети подсети одного размера, достаточно применить одинаковую маску для всех подсетей, так как именно маска определяет размер подсети. Но какая маска?

При выборе единой маски следует учитывать одно требование: она должна обеспечить количество IP-адресов хостов, достаточное для поддержки наибольшей подсети. Для этого количество битов хоста (H), определенное маской, должно быть достаточно большим, чтобы значение $2^H - 2$ было большим или равным количеству IP-адресов хоста, необходимому в наибольшей подсети.

Рассмотрим, например, рис. 12.8. На нем показано необходимое количество хостов в подсети LAN и игнорируются последовательные каналы. Ветви подсети требуют только по 50 адресов хоста, но основная подсеть площадки требует 200 адресов хоста. Для наибольшей подсети необходимо по крайней мере 8 битов хоста. Семи битов было бы недостаточно, поскольку $2^7 - 2 = 126$, а восьми битов хоста было бы вполне достаточно, поскольку $2^8 - 2 = 254$. Этого даже более чем достаточно для обеспечения 200 хостов в подсети.

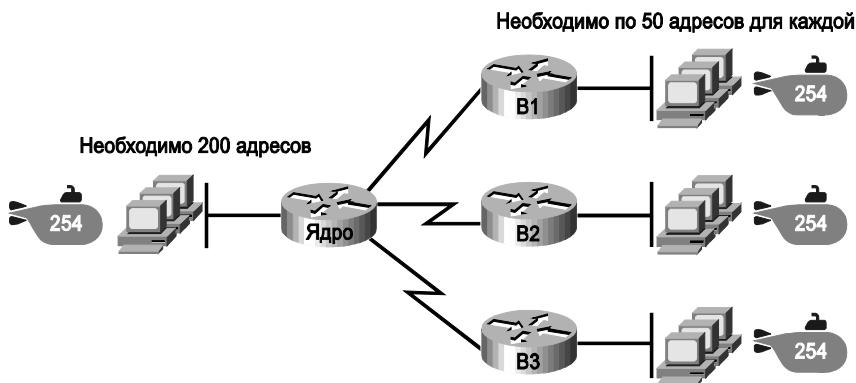


Рис. 12.8. Сеть с подсетями одного размера

В чем наибольшее преимущество при использовании подсетей одного размера? Оперативная простота. Другими словами, все остается простым. Сотрудники, обслуживающие сеть, легко привыкнут к работе с одинаковой и только одной маской. Они легко ответят на все вопросы о создании подсетей, обсуждаемые в этой книге: вычисление идентификатора подсети, вычисление диапазона адресов в подсети, определение количества хостов в подсети и т.д. Это намного проще, чем если бы маски у всех подсетей были разными.

Наибольшим недостатком единого размера подсетей является растрата впустую IP-адресов. Например, на рис. 12.8 показано, что все ветви подсети LAN обеспечивают 254 адреса, в то время как наибольшая подсеть нуждается только в 50 адресах. Подсети WAN нуждаются только в двух IP-адресах, но каждая поддерживает 254 адреса, снова растрачивая впустую большое количество IP-адресов.

Как бы то ни было, растрата впустую IP-адресов фактически не создает проблем в большинстве случаев. Большинство организаций в своих корпоративных объединенных сетях используют частные сети IP, и единая закрытая сеть класс А или В вполне может обеспечить множество IP-адресов, даже при потерях.

Подсети разного размера (маски подсети переменной длины)

Чтобы получить несколько подсетей разного размера в одной сети класса А, В или С, инженер должен создать одну подсеть, используя одну маску, другую — используя другую маску, и т.д. Различные маски означают различное количество битов хоста, используя результат формулы $2^H - 2$ для вычисления различного количества хостов в этих подсетях.

Рассмотрим, например, требования, перечисленные ранее на рис. 12.8. Там представлена одна подсеть LAN слева, требующая 200 адресов хостов, три ветви подсетей,

которым требуется 50 адресов, и три последовательных канала, требующих по 2 адреса. Применение трех масок при создании трех подсетей разного размера, как показано на рис. 12.9, удовлетворит эти потребности с меньшей растратой впустую IP-адресов.

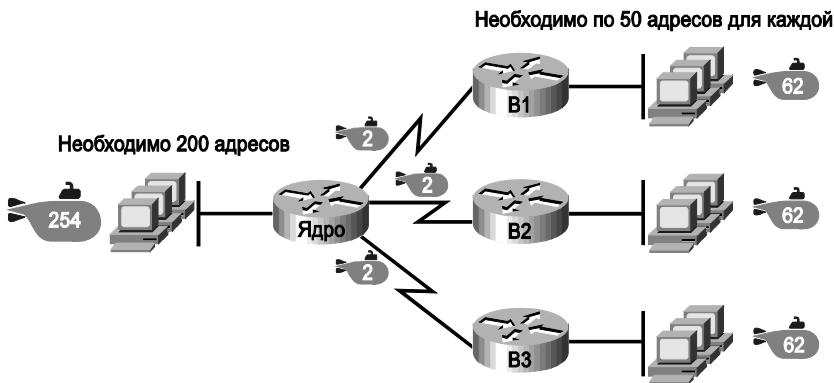


Рис. 12.9. Три маски, три размера подсети

Меньшие подсети теперь растратывают меньше IP-адресов по сравнению с прежним проектом на рис. 12.8. Подсети на рисунке справа, которые нуждаются в 50 IP-адресах, имеют подсети с 6 битами хоста, для $2^6 - 2 = 62$ доступных адресов на подсеть. Каналы WAN используют маски с 2 битами хоста, для $2^2 - 2 = 2$ доступных адресов на подсеть.

Но некоторые адреса все еще тратятся впустую, поскольку подсеть нельзя задать некий произвольный размер. Размер всех подсетей вычисляется по формуле $2^H - 2$, где H — количество битов хоста, определенных маской для каждой подсети.

В этой книге считается, что лучше иметь все подсети одинакового размера

При объяснении создания подсетей в этой книге подразумевается, что разработчик решил использовать в одной классовой сети IP одну маску, создавая все подсети одинакового размера. Почему? Во-первых, это упрощает процесс изучения создания подсетей. Во-вторых, некоторые типы анализа сети, а именно вычисление количества подсетей в классовой сети, имеют смысл только в случае использования единой маски. Таким образом, оставшаяся часть книги сосредоточена на примерах и описаниях, подразумевающих использование одной маски в каждой классовой сети IP.

Маски подсети переменной длины (Variable Length Subnet Mask — VLSM), подразумевающие практику использования различных масок для разных подсетей в той же классовой сети IP, рассматриваются во втором томе книги.

Выбор проекта

Теперь, когда вы знаете, как проанализировать потребность в IP-адресации и подсетях, перейдем к следующему этапу — применению правил IP-адресации и созданию подсетей согласно этим потребностям и выбранным маскам. Другими словами, зная, как можно создать конкретный проект подсетей, который отвечает этим требованиям, сколько необходимо подсетей и адресов хостов в наибольшей подсети? Короткий ответ — см. три задачи, представленные на рис. 12.10, справа.

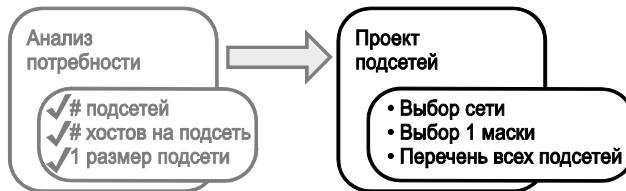


Рис. 12.10. Переход к этапу проектирования и от вопросов к ответам

Выбор классовой сети

В первоначальном проекте того, что сегодня известно как Интернет, при реализации внутренней сети TCP/IP компании использовали зарегистрированные *открытые классовые сети IP* (public classful IP network). К середине 1990-х годов более популярными стали альтернативные *частные сети IP* (private IP network). В этом разделе обсуждаются причины выбора из этих двух альтернатив, поскольку он влияет на выбор того, какую сеть IP компания будет впоследствии разделять на подсети и реализовывать в своей корпоративной объединенной сети.

Открытые сети IP

Первоначальный проект Интернета обязывал, чтобы любая подключившаяся к нему компания использовала *зарегистрированную открытую сеть IP* (registered public IP network). Для этого компания готовила некие документы, описывая объединенную сеть компании, количество существующих хостов, а также планы на рост. После передачи документов на рассмотрение компания получала сеть класса А, В или С.

Открытые сети IP и сопровождающие их административные процессы гарантируют, что все компании, которые подключаются к Интернету, будут использовать уникальные IP-адреса. В частности, как только компании присваивается открытая сеть IP, только эта компания должна использовать адреса в данной сети. Гарантия уникальности означает, что маршрутизация Интернета будет работать хорошо, поскольку нет никаких совпадающих открытых IP-адресов.

Рассмотрим, например, рис. 12.11. Компании 1 присвоена открытая сеть класса А 1.0.0.0, а компании 2 — открытая сеть класса А 2.0.0.0. Для открытой адресации в Интернете изначально предполагается, что после присвоения открытой сети никакие другие компании не смогут использовать адреса в сетях класса А 1.0.0.0 или 2.0.0.0.

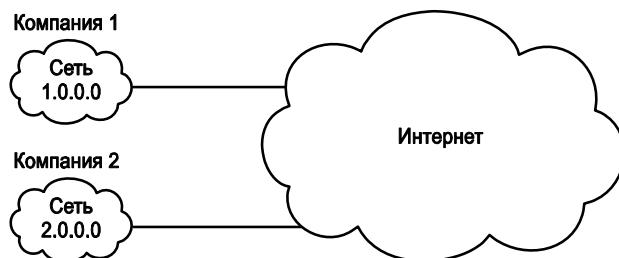


Рис. 12.11. Две компании с уникальными открытыми сетями IP

Этот первоначальный процесс присвоения адресов гарантировал уникальность IP-адресов по всей планете. Идея аналогична тому факту, что номер телефона должен быть уникальным в своей области, почтовый адрес должен быть уникальным и адрес электронной почты также должен быть уникальным. При вызове звонит телефон только того, кого вызывают, другие телефоны молчат. Аналогично компании 1 присвоена сеть класса А 1.0.0.0, и она назначает адрес 1.1.1.1 определенному компьютеру, причем этот адрес должен быть уникальным. Пакет, посланный через Интернет получателю 1.1.1.1, должен достичь только этого компьютера в компании 1, а не попасть на некий другой хост.

Исчерпание свободных IP-адресов

К началу 1990-х годов мир исчерпывал открытые сети IP, которые могли бы быть присвоены. Количество новых хостов, подключенных к Интернету, росло в темпе с двузначным числом *в месяц*. Компании продолжали следовать правилам, запрашивая открытые сети IP, и стало ясно, что текущая схема присвоения адресов не могла функционировать без небольшого изменения. Проще говоря, количества сетей класса А, В и С, обеспечиваемых 32-разрядным IP-адресом версии 4 (IPv4), оказалось недостаточно для предоставления одной открытой классовой сети на организацию, обеспечивая также достаточно много IP-адресов для каждой компании.

ВНИМАНИЕ!

Мир исчерпал открытые IPv4-адреса в начале 2011 года. Агентство IANA, которое присваивает блоки открытых IPv4-адресов пяти регистров Интернета в мире, присвоило последнее из пространств IPv4-адресов в начале 2011 года.

Сообщество Интернета упорно трудилось на протяжении 1990-х годов над решением этой проблемы и придумало несколько решений, включая перечисленные ниже.



Средства продления существования IPv4

- Новая версия IP (IP Version 6 [IPv6]) с намного большими адресами (128 битов).
- Назначение каждой компании части открытой сети IP вместо всей открытой сети IP.
- *Трансляция сетевых адресов* (Network Address Translation — NAT), позволяющая использовать частные сети IP.

Ныне эти три решения имеют большое значение для реальных сетей. Однако, чтобы не отклоняться от темы проектирования подсети, эта глава сосредоточивается на третьей возможности — частных сетях IP, — которые применяются компаниями при использовании NAT.

Технология NAT, подробно рассматриваемая в главе 23, позволяет некоторым компаниям использовать те же частные сети IP с теми же IP-адресами, что и у других компаний, при наличии подключения к Интернету. Например, на рис. 12.12 представлены те же две компании, подключенные к Интернету, что и на рис. 12.10, но теперь обе используют ту же частную сеть класса А 10.0.0.0.

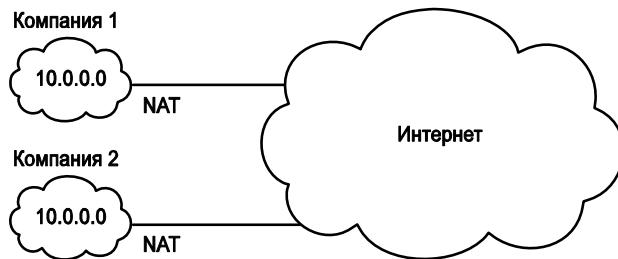


Рис. 12.12. Многократное использование той же закрытой сети 10.0.0.0 с помощью NAT

Обе компании используют ту же классовую сеть IP (10.0.0.0) и могут реализовать свой проект подсети внутренне, согласно собственным корпоративным объединенным сетям, не обсуждая их планы. Эти две компании могут даже использовать совпадающие IP-адреса в сети 10.0.0.0. В то же время, как ни удивительно, обе компании вполне могут даже общаться друг с другом через Интернет.

Технология под названием *трансляция сетевых адресов* (Network Address Translation — NAT) позволяет компаниям многократно использовать те же сети IP, как показано на рис. 12.12. Технология NAT осуществляет это за счет трансляции IP-адресов в пакетах при их передаче от компании к Интернету, используя небольшое количество открытых IP-адресов для поддержки десятков тысяч частных IP-адресов. Этой сжатой информации недостаточно, чтобы понять, как работает NAT; но чтобы не отвлекаться от создания подсетей, отложим обсуждение работы технологии NAT до главы 23, а пока просто констатируем, что большинство компаний применяют технологию NAT и поэтому могут использовать частные сети IP для своих объединенных сетей.

Частные сети IP

Документ RFC 1918 определяет набор частных сетей IP, как указано в табл. 12.2. По определению, эти частные сети IP.

- никогда не будут присваиваться организациям как открытая сеть IP;
- могут быть использованы организациями, применяющими технологию NAT при передаче пакетов в Интернет;
- могут использоваться организациями, которым никогда не придется посыпать пакеты в Интернет.

Таким образом, при использовании технологии NAT (а почти все подключенные к Интернету организации используют NAT) компания вполне может выбрать одну или несколько частных сетей IP из зарезервированных номеров частных сетей. Документ RFC 1918 определяет список, который приведен в табл. 12.2.

Таблица 12.2. Документ RFC 1918. Частное пространство адресов

Частные сети IP	Класс сетей	Количество сетей
10.0.0.0	A	1
172.16.0.0 – 172.31.0.0	B	16
192.168.0.0 – 192.168.255.0	C	256

ВНИМАНИЕ!

Согласно неофициальному опросу, который я запустил на своем блоге в конце 2010 года, примерно половина посетителей указала, что у них используется частная сеть класса А 10.0.0.0, а не другая частная или открытая сеть.

Выбор сети IP на этапе проектирования

Ныне одни организации используют частные сети IP вместе с технологией NAT, а другие — открытые сети IP. Новые корпоративные объединенные сети используют частные IP-адреса с технологией NAT как часть соединения с Интернетом. Те организации, у которых уже есть зарегистрированные открытые сети IP, как правило, полученные до начала исчерпания адресов в 1990-х годах, продолжают использовать эти открытые адреса в своих корпоративных сетях.

Как только решено использовать частную сеть IP, остается лишь выбрать ту, у которой достаточно IP-адресов. У компании может быть маленькая объединенная сеть, но решено будет выбрать частную сеть класса А 10.0.0.0. Это может показаться расточительным, ведь у сети класса А более 16 миллионов IP-адресов, а нужно лишь несколько сотен. Но это не повлечет никакого штрафа и не создаст проблем с использованием закрытой сети, которая слишком велика для текущих или будущих потребностей.

В большинстве примеров этой книги используются адреса частных сетей IP. На этапе выбора количества сетей достаточно выбрать подходящую частную сеть класса A, B или C из списка закрытых сетей в документе 1918 RFC.

Независимо от математической и концептуальной точки зрения, методы разделения на подсети открытых и частных сетей IP одинаковы.

Выбор маски

Если бы разработчик следовал темам этой главы, то он знал бы следующее:

- необходимое количество подсетей;
- необходимое количество хостов на подсеть;
- что решено использовать только одну маску для всех подсетей, чтобы все подсети были одинакового размера (одинаковое количество хостов на подсеть);
- номер классовой сети IP, которая в результате будет разделена.

Этот раздел завершает описание процесса проектирования, по крайней мере, части, описанной в данной главе, обсуждением выбора одной маски, используемой для всех подсетей. Сначала для сравнения рассмотрим стандартные маски, используемые по умолчанию, когда сеть не разделена на подсети. Затем рассмотрим концепцию заимствования битов хоста для создания битов подсети. И наконец, закончим раздел примером создания маски подсети на основании анализа требований.

Классовые сети IP до создания подсетей

До разделения сети на подсети классовая сеть является единой группой адресов. Другими словами, инженер еще не разделил сеть на множество меньших подмножеств, называемых *подсетями*.

У адресов не разделенной классовой сети есть только две части: часть сети и часть хоста. Если сравнить два любых адреса классовой сети, то можно обнаружить следующее:

- у адресов одинаковое значение в части сети;
- у адресов различные значения в части хоста.

Настоящие величины частей сети и хоста адресов могут быть легко предсказаны, как показано на рис. 12.13.

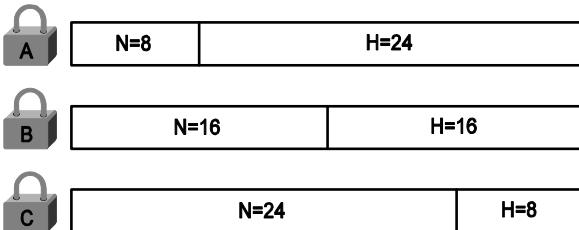


Рис. 12.13. Формат адреса не разделенной на подсети сети класса A, B и C

На рис. 12.13 значения N и H представляют количество битов сети и хоста соответственно. Правила классов определяют количество октетов сети (1, 2 или 3) для классов A, B и C соответственно. Количество октетов хоста составляет 3, 2 или 1 соответственно.

Продолжая анализ классовой сети перед созданием подсетей, можно вычислить количество адресов в сети по той же формуле, $2^H - 2$, что и ранее. В частности, размер не разделенных на подсети класса A, B и C приведен ниже.

- Класс А. $2^{24} - 2 = 16\ 777\ 214$.
- Класс B. $2^{16} - 2 = 65\ 534$.
- Класс C. $2^8 - 2 = 254$.

Заемствование битов хоста для создания битов подсети

Чтобы разделить сеть, инженеру следует обдумать части сети и хоста, как показано на рис. 12.13, а затем добавить посередине третью часть: часть подсети. Однако он не может изменить размер сетевой части или размер всего адреса (32 бита). Чтобы создать часть подсети в структуре адреса, необходимые биты заимствуются из части хоста. Общая концепция представлена на рис. 12.14.

Прямоугольники на рис. 12.14 означают части адреса. N — это количество битов сети. Остаются прямоугольники по 8, 16 битов или 24 бита, в зависимости от класса. Концептуально дизайнер перемещает разделительную (пунктирную) линию в поле хоста между битами частей подсети (S) сетью и хоста (H), оставшимися справа. В целом эти три части должны составить 32, поскольку IPv4-адреса состоят из 32 битов.

Выбор достаточного количества битов подсети и хоста

Процесс проектирования требует выбрать, где поместить пунктирную линию, представленную на рис. 12.14. Но какой выбор правильный? Сколько битов подсети и хоста следует выбрать? Ответы зависят от требований, собранных на прежних этапах процесса планирования:

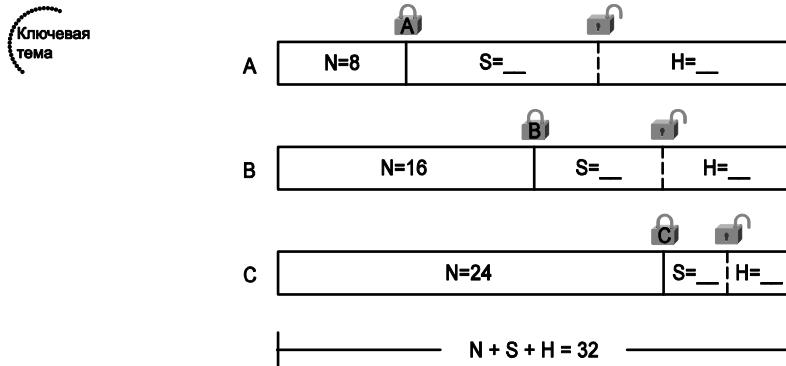


Рис. 12.14. Формат адреса разделенной на подсети сети класса A, B и C

- необходимое количество подсетей;
- количество хостов на подсеть.

Биты в части подсети позволяют уникально нумеровать различные подсети, которые разработчик хочет создать. С 1 битом подсети можно нумеровать 2^1 или 2 подсети. С 2 битами — 2^2 или 4 подсети, с 3 битами — 2^3 или 8 подсетей и т.д. Количество битов подсети должно быть достаточно большим для уникальной нумерации всех подсетей, как определено на этапе планирования.

В то же время количество оставшихся битов хоста должно быть достаточно большим для нумерации IP-адресов хостов в наибольшей подсети. Помните: в этой главе подразумевается использование одной маски для всех подсетей. Эта единая маска должна обеспечить и необходимое количество подсетей, и необходимое количество хостов в наибольшей подсети. Эта концепция представлена на рис. 12.15.

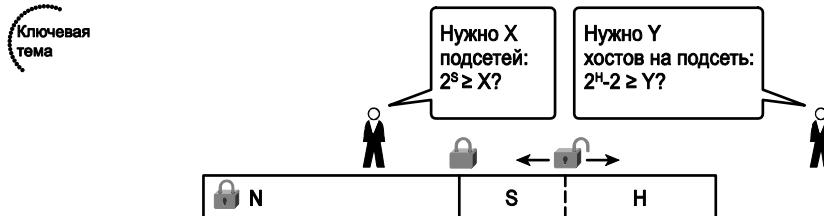


Рис. 12.15. Общая логика при выборе размера части подсети в адресе

На рис. 12.15 представлена концепция выбора количества битов подсети (S) и хоста (H) с последующей математической проверкой. Значение 2^s должно быть больше количества необходимых подсетей, иначе маска не обеспечит достаточно много подсетей в этой сети IP. Кроме того, значение $2^h - 2$ должно быть больше количества необходимых хостов на подсеть.

ВНИМАНИЕ!

Идея вычисления количества подсетей как 2^s применима только в тех случаях, когда для всех подсетей единой классовой сети используется одна маска, как подразумевается в этой главе.

Для эффективной разработки маски или интерпретации маски, выбранной кем-то еще, необходимо хорошо помнить степени числа 2. В табл. 12.3 приведен список степеней числа 2 до 2^{12} наряду со столбцом $2^H - 2$, полезным при вычислении количества хостов на подсеть. В приложении Б приведена таблица со степенями числа 2 до 2^{24} .

Таблица 12.3. Степени числа 2. Справочник для выбора маски

Количество битов	2^x	$2^x - 2$
1	2	0
2	4	2
3	8	6
4	16	14
5	32	30
6	64	62
7	128	126
8	256	254
9	512	510
10	1024	1022
11	2048	2046
12	4096	4094

Пример проекта: 172.16.0.0, 200 подсетей, 200 хостов

Для подкрепления теоретического обсуждения рассмотрим пример выбора маски подсети. В данном случае план и выбранный проект диктуют следующее:

- использовать одну маску для всех подсетей;
- наличие 200 подсетей;
- наличие 200 IP-адресов хостов на подсеть;
- использовать частную сеть класса В 172.16.0.0.

Для выбора маски следует задаться вопросом: сколько битов подсети (S) необходимо для нумерации 200 подсетей?

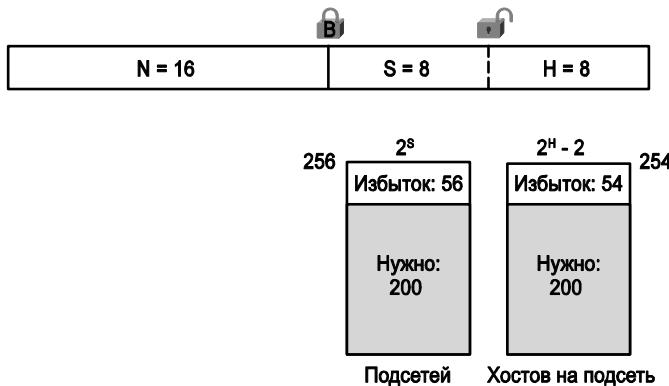
Как можно заметить в табл. 12.3, значение $S = 7$ не является достаточно большим ($2^7 = 128$), но $S = 8$ вполне достаточно ($2^8 = 256$). Таким образом, для подсети необходимо по крайней мере 8 битов.

Затем, на основании количества хостов в подсети, следует задаться вопросом: сколько битов хоста (H) необходимо для нумерации 200 хостов в подсети?

В принципе математический механизм тот же, но в формуле расчета количества хостов на подсеть вычитается 2. Как можно заметить в табл. 12.3, значение $H = 7$ не является достаточно большим ($2^7 - 2 = 126$), но значения $H = 8$ вполне достаточно ($2^8 - 2 = 254$). Полученная маска представлена на рис. 12.16.

Маски и форматы масок

Хотя инженеры считают, что IP-адреса состоят из трех частей (сеть, подсеть и хост), при выборе проекта маска подсети предоставляет инженеру способ распространить сделанный выбор на все устройства в подсети.

Рис. 12.16. Пример выбора маски $S = 8, H = 8$

Маска подсети — это 32-разрядное двоичное число с несколькими двоичными единицами слева и двоичными нулями справа. По определению количество двоичных нулей равно количеству битов хоста. Фактически именно так маска выражает идею размера части хоста в адресе при наличии подсети. Начальные биты в маске равны двоичным единицам, эти позиции двоичного разряда представляют совместно части сети и подсети в адресе при наличии подсети.

Поскольку сетевая часть всегда стоит на первом месте, затем идут часть подсети и часть хоста, маска подсети в бинарной форме не может чередовать единицы и нули. У каждой маски подсети есть одна неизменная строка двоичных единиц слева, а остальная часть битов занята двоичными нулями.

После выбора классовой сети и количества битов подсетей и хоста в подсети создать двоичную маску подсети несложно. Достаточно написать N единиц, S единиц, а затем H нулей (под N , S и H подразумевается количество битов сети, подсети и хоста). На рис. 12.17 представлена маска на основании условий предыдущего примера, в котором сеть класса В разделяется на подсеть при 8 битах подсети и 8 битах хоста.

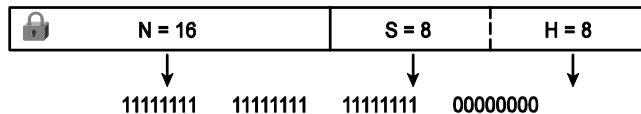


Рис. 12.17. Создание двоичной маски подсети для сети класса В

Кроме двоичной маски, представленной на рис. 12.17, маски могут быть также записаны в двух других форматах: уже знакомое *десятичное представление с разделительными точками* (Dotted-Decimal Notation — DDN), применяемое в IP-адресах, а также более краткая *префиксная* (prefix) форма. Эти форматы подробнее обсуждаются в главе 14, но еще важнее то, что там обсуждаются преобразования различных форматов.

Создание списка всех подсетей

Последняя задача этапа проектирования подсети — определение фактических подсетей, создаваемых на основании всех сделанных ранее выборов. На прежних этапах проектирования был определен класс А, В или С используемой сети, выбрана единная маска подсети, обеспечивающая достаточно много подсетей и достаточно

много IP-адресов хостов в каждой подсети. Но каковы эти подсети? Как идентифицировать или описать подсеть? Данный раздел отвечает на эти вопросы.

Подсеть состоит из группы последовательных чисел, большинство из которых (номеров) применяется как IP-адреса хостов. Однако каждая подсеть резервирует первые и последние номера в группе, и эти два номера не могут использоваться как IP-адреса. В частности, каждая подсеть содержит следующее.

Элементы, совместно определяющие подсеть



- *Адрес подсети* (subnet address), называемый также *идентификатором подсети* (subnet ID) или *номером подсети* (subnet number), — число, идентифицирующее подсеть. Это наименьший номер в подсети. Он не может использоваться как IP-адрес хоста.
- *Широковещательный адрес подсети* (subnet broadcast или subnet broadcast address), называемый также *направленным широковещательным адресом* (directed broadcast address), — последний, самый большой номер в подсети. Он также не может использоваться как IP-адрес хоста.
- *IP-адреса* (IP address) — все номера между идентификатором подсети и широковещательным адресом подсети, применяемые как IP-адреса хостов.

Рассмотрим, например, приведенный ранее случай, в котором результаты проектирования были следующими:

- сеть 172.16.0.0 (класс В);
- маска 255.255.255.0 (для всех подсетей).

Прибегнув к математике, можно вычислить определенные факты о каждой подсети, существующей в этой сети. В данном случае в табл. 12.4 приведены десять первых таких подсетей. Затем следует пропуск множества подсетей и приведены две последние подсети (в цифровой форме — наибольшие).

Таблица 12.4. Десять первых подсетей, а также несколько последних для сети 172.16.0.0 и маски 255.255.255.0

Адрес подсети	IP-адрес	Широковещательный адрес
172.16.0.0	172.16.0.1 – 172.16.0.254	172.16.0.255
172.16.1.0	172.16.1.1 – 172.16.1.254	172.16.1.255
172.16.2.0	172.16.2.1 – 172.16.2.254	172.16.2.255
172.16.3.0	172.16.3.1 – 172.16.3.254	172.16.3.255
172.16.4.0	172.16.4.1 – 172.16.4.254	172.16.4.255
172.16.5.0	172.16.5.1 – 172.16.5.254	172.16.5.255
172.16.6.0	172.16.6.1 – 172.16.6.254	172.16.6.255
172.16.7.0	172.16.7.1 – 172.16.7.254	172.16.7.255
172.16.8.0	172.16.8.1 – 172.16.8.254	172.16.8.255
172.16.9.0	172.16.9.1 – 172.16.9.254	172.16.9.255
Много пропущено...		
172.16.254.0	172.16.254.1 – 172.16.254.254	172.16.254.255
172.16.255.0	172.16.255.1 – 172.16.255.254	172.16.255.255

Имея номер сети и маску, для вычисления идентификаторов подсетей и других подробностей о всех подсетях следует применить математику. В реальной жизни большинство инженеров используют калькуляторы подсети или инструменты планирования подсети. Для экзаменов CCENT и CCNA необходимо быть готовым самостоятельно вычислить эту информацию; в главе 18 описано вычисление всех подсетей данной сети.

Реализация плана

Следующий этап, планирование реализации, является последним этапом перед фактической настройкой устройств при создании подсети. Сначала инженер должен выбрать, где использовать каждую подсеть. Какую, например, из указанных в табл. 12.4 подсетей следует использовать для каждой VLAN филиалов в некотором городе? Кроме того, какие из IP-адресов должны быть статическими, а какие можно использовать случайно? И наконец, какой диапазон в каждой подсети должен быть настроен на сервере DHCP и динамически предоставляться хостам для использования в качестве их IP-адресов? На рис. 12.18 приведен краткий список задач планирования реализации.

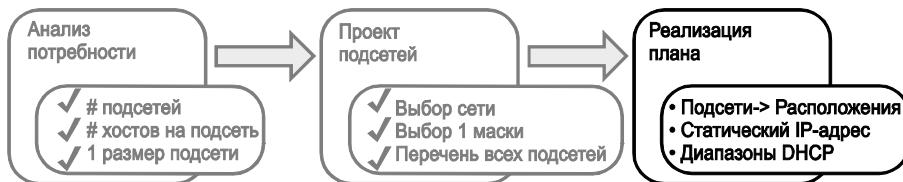


Рис. 12.18. Факты, сопутствующие этапу реализации плана

Назначение подсетей различным местам

Задача проста: просмотрите свою схему сети, выявите каждое расположение, которое нуждается в подсети, и выберите для них из таблицы по одной из возможных подсетей. Затем запишите, чтобы не забыть, в электронной таблице или другом специализированном инструменте планирования подсетей, какие подсети вы используете и где. Вот и все! На рис. 12.19 приведен пример законченного проекта, согласно табл. 12.4 и исходному проекту из примера, представленного ранее на рис. 12.1.

Класс В 172.16.0.0

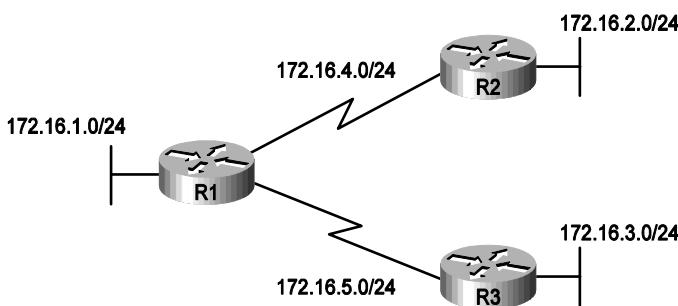


Рис. 12.19. Пример подсетей, назначенных различным расположениям

Хотя в этом проекте вполне возможно использовать пять любых подсетей из табл. 12.4, в реальных сетях обычно придерживаются некой более осмысленной стратегии назначения подсетей. Например, можно было бы назначить всем подсетям LAN более низкие номера, а подсетям WAN более высокие. Либо можно было выделить большие диапазоны подсетей для различных подразделений. Либо можно было следовать той же стратегии, но игнорировать организационное деление в компании, уделяя больше внимания географии.

Например, для компании, расположенной в основном в Америке и с меньшим присутствием в Европе и Азии, можно было бы зарезервировать диапазоны подсетей на основании континентов. Такой выбор особенно полезен при последующей попытке использовать средство под названием *суммирование маршрутов* (route summarization), которое подробно обсуждается во втором томе книги. Рис. 12.20 дает общее представление об использовании подсетей, описанных в табл. 12.4.

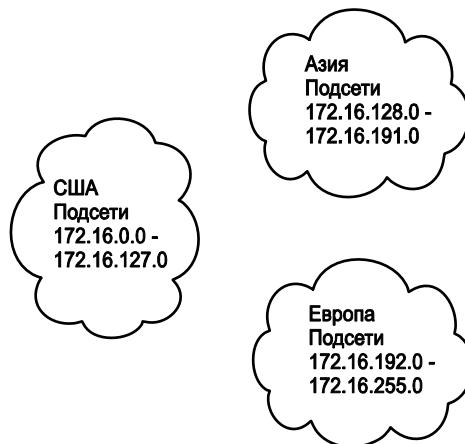


Рис. 12.20. Резервирование подсетей на географическом основании для более позднего использования

Выбор статических и динамических диапазонов в подсети

Устройства получают свой IP-адрес и маску одним из двух способов: динамически, с помощью протокола DHCP, или статически, через конфигурацию. Чтобы протокол DHCP работал, сетевой инженер должен указать серверу DHCP подсеть, для которых он должен назначить IP-адреса. Кроме того, эта конфигурация ограничивает сервер DHCP только некоторым подмножеством адресов в подсете. Для статических адресов можно просто настроить устройство, указав ему используемый IP-адрес и маску.

Чтобы по возможности не усложнять ситуацию, как правило, используется стратегия отделения статических IP-адресов с одной стороны диапазона адресов подсети и адресов DHCP, назначаемых динамически, с другой стороны. На самом деле не имеет значения, находятся ли статические адреса на нижнем конце диапазона адресов или на верхнем.

Предположим, например, что инженер решает выделить для подсетей LAN (см. рис. 12.19) пул DHCP, начинающийся сверху диапазона (а именно с адреса, заканчивающегося на .254) до .101. (Адрес, заканчивающийся на .255, естественно, зарезервирован для брандмауэра.)

зверирован.) Инженер выбирает статические адреса с нижнего конца диапазона (с адреса, заканчивающегося на .1) до .100. Идея представлена на рис. 12.21.

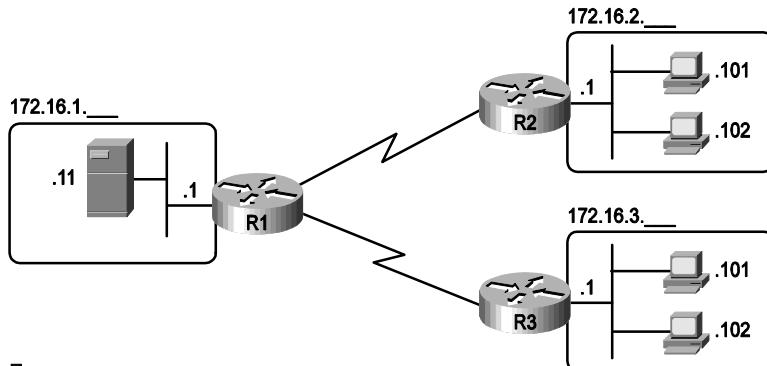


Рис. 12.21. Статические адреса — нижние, DHCP — верхние

Все три маршрутизатора на рис. 12.21 имеют статические IP-адреса, завершающиеся .1. Единственный другой статический IP-адрес на рисунке присвоен серверу в левой части рисунка, это адрес 172.16.1.11 (сокращен на рисунке как .11).

В каждой сети LAN на рисунке справа есть по два компьютера, для динамического назначения IP-адресов которых используется DHCP. Серверы DHCP, как правило, назначают адреса, начиная снизу диапазона адресов. Таким образом, хосты в каждой сети LAN получили бы адреса, заканчивающиеся на .101 и .102, что соответствует нижнему концу диапазона, выбранного в соответствии с проектом.

Подготовка к экзамену

Повторите все ключевые темы

Повторите все ключевые темы данной главы, помеченные пиктограммой “Ключевая тема”. Ключевые темы и соответствующие им страницы перечислены в табл. 12.5.

Таблица 12.5. Ключевые темы главы 12

Элемент	Описание	Страница
Список	Основные факты о подсетях	368
Список	Какие места в сетевой топологии нуждаются в подсети	369
Рис. 12.7	Концепции размера подсети	372
Список	Средства продления существования IPv4	376
Рис. 12.14	Формат адреса разделенной на подсети сети класса А, В и С	380
Рис. 12.15	Общая логика при выборе размера части подсети в адресе	380
Список	Элементы, совместно определяющие подсеть	383

Заполните таблицы и списки по памяти

Распечатайте приложение М (Appendix L) с компакт-диска или его раздел, относящийся к этой главе, и заполните таблицы и списки по памяти. В приложении Н (Appendix M) приведены заполненные таблицы и списки для самоконтроля.

Ключевые термины

Дайте определения перечисленных ниже терминов и проверьте правильность их написания в списке терминов:

подсеть (subnet), сеть (network), классовая сеть (classful network), маска подсети переменной длины (Variable Length Subnet Mask — VLSM), часть сети (network part), часть подсети (subnet part), часть хоста (host part), открытая сеть IP (public IP network), частная сеть IP (private IP network), маска подсети (subnet mask).

В этой главе...

- **Концепции классовых сетей.** Рассматриваются темы, связанные с сетями класса A, B и C (другими словами, классовыми сетями IP).
- **Практические задачи по классовым сетям.** Этот раздел поможет читателям подготовиться к решению практических задач на экзаменах CCENT и CCNA. Здесь приведены советы и рекомендации, как лучше применить логику и математику для анализа классовых сетей.

ГЛАВА 13

Анализ классовых сетей IPv4

При работе с сетью выявление проблем зачастую начинается с выяснения IP-адреса и маски. Только по IP-адресу нужно уметь определить несколько фактов о сети класса А, В или С, в которой он располагается. Эти факты могут быть полезны при диагностике некоторых сетевых проблем.

В этой главе приведен ряд ключевых фактов о классовых сетях IP и объяснено, как выявить эти факты. Затем будут приведены некоторые практические задачи. Прежде чем переходить к следующей главе, следует попрактиковаться, пока не удастся выявлять все эти факты быстро и уверенно на основании IP-адреса.

Контрольные вопросы: знаете ли вы уже темы главы

Этот раздел предназначен для того, чтобы читатель мог предварительно оценить свои знания и решить, нужно ли ему читать главу целиком. Если ответы на девять из десяти вопросов даны правильно, можно сразу же перейти к последнему разделу “Подготовка к экзамену”. Основные темы этой главы и предварительных контрольных вопросов перечислены в табл. 13.1. Отвечая на контрольные вопросы и используя таблицу, читатель сможет достаточно точно определить свои знания в той или иной области. Ответы на вопросы приведены в приложении А.

Таблица 13.1. Темы контрольных вопросов

Основная тема	Номера вопросов
Концепции классовых сетей	1–6

- Что из приведенного ниже не является допустимым идентификатором сети класса А? (Выберите несколько ответов.)
 - 1.0.0.0.
 - 130.0.0.0.
 - 127.0.0.0.
 - 9.0.0.0.
- Что из приведенного ниже не является допустимым идентификатором сети класса В?
 - 130.0.0.0.
 - 191.255.0.0.
 - 128.0.0.0.

- г) 150.255.0.0.
 - д) Все это допустимые идентификаторы сети класса В.
3. Что из следующего является истиной об IP-адресе сети IP 172.16.99.45? (Выберите несколько ответов.)
- а) Идентификатор сети 172.0.0.0.
 - б) Сеть имеет класс В.
 - в) По умолчанию для сети задана маска 255.255.255.0.
 - г) В не разделенной на подсети сети для хостов предназначено 16 битов.
4. Что из следующего является истиной об IP-адресе сети IP 192.168.6.7? (Выберите несколько ответов.)
- а) Идентификатор сети 192.168.6.0.
 - б) Сеть имеет класс В.
 - в) По умолчанию для сети задана маска 255.255.255.0.
 - г) В не разделенной на подсети сети для хостов предназначено 16 битов.
5. Что из следующего является широковещательным адресом сети?
- а) 10.1.255.255.
 - б) 192.168.255.1.
 - в) 24.1.1.255.
 - г) 172.30.255.255.
6. Что из следующего является идентификатором сети класса А, В или С?
- а) 10.1.0.0.
 - б) 192.168.1.0.
 - в) 127.0.0.0.
 - г) 72.20.0.1.

Основные темы

Концепции классовых сетей

Предположим, вы на собеседовании при приеме на первую работу в отрасли ИТ. В ходе собеседования вам предложен IPv4-адрес и маска: 10.4.5.99, 255.255.255.0. Что вы можете сказать о классовой сети (в данном случае сети класса А), в которой располагается этот IP-адрес?

Данный раздел — первый из двух основных разделов главы, в котором приведен обзор концепций *классовых сетей IP* (classful IP network), другими словами, сетей класса А, В и С. В частности, в текущей главе объясняется, как, начиная только с одного IP-адреса, выявить факты, приведенные ниже.

- Класс (А, В или С).
- Заданная по умолчанию маска.
- Количество октетов (битов) сети.
- Количество октетов (битов) хоста.
- Количество адресов хостов в сети.
- Идентификатор сети.
- Широковещательный адрес сети.
- Первый и последний адрес, допустимые для использования в сети.

Классовая сеть IPv4 и связанные с ней факты

Протокол IP версии 4 (IPv4) определяет пять классов адресов. Три класса, А, В и С, используют одноадресатные IP-адреса. *Одноадресатные адреса* (unicast address) идентифицируют один хост или интерфейс, таким образом, он однозначно идентифицирует устройство. Адреса класса D служат многоадресатными адресами; так, пакет, посланный на один многоадресатный IPv4-адрес класса D, фактически будет доставлен нескольким хостам. И наконец, адреса класса Е являются экспериментальными.

Класс может быть идентифицирован на основании значения первого октета адреса, как показано в табл. 13.2.

Таблица 13.2. Классы IPv4-адресов на основании значения первого октета



Значения первого октета	Класс	Назначение
1–126	A	Одноадресатный (большие сети)
128–191	B	Одноадресатный (сети среднего размера)
192–223	C	Одноадресатный (маленькие сети)
224–239	D	Многоадресатный
240–255	E	Экспериментальный

Вопросы экзаменов CCENT и CCNA сосредоточены главным образом на одноадресатных классах (А, В и С), а не на классах D и E. После идентификации класса

сети как А, В или С, множество других связанных с ними фактов можно воспроизвести по памяти. В табл. 13.3 приведена информация для справки и последующего изучения; каждая из этих концепций описана в данной главе.



Таблица 13.3. Основные факты о классах А, В и С

Частные сети IP	Класс А	Класс В	Класс С
Диапазон первого октета	1 – 126	128 – 191	192 – 223
Допустимые адреса сети	1.0.0.0 – 126.0.0.0	128.0.0.0 – 191.255.0.0	192.0.0.0 – 223.255.255.0
Всего сетей	$2^7 - 2 = 126$	$2^{14} = 16\ 384$	$2^{21} = 2\ 097\ 152$
Хостов на сеть	$2^{24} - 2$	$2^{16} - 2$	$2^8 - 2$
Октеты (биты) в части сети	1 (8)	2 (16)	3 (24)
Октеты (биты) в части хоста	3 (24)	2 (16)	1 (8)
Маска по умолчанию	255.0.0.0	255.255.0.0	255.255.255.0

Реальные сети класса А, В и С

В табл. 13.3 приведен список диапазонов адресов сетей класса А, В и С. Однако некоторые ключевые моменты могут отсутствовать в справочной таблице. В данном разделе исследуются адреса сетей классов А, В и С, сосредоточиваясь на важных темах, исключениях и необычных случаях.

В первую очередь, количество сетей в каждом классе значительно отличается. В классе А существуют лишь 126 сетей: 1.0.0.0, 2.0.0.0, 3.0.0.0 и так далее до 126.0.0.0. В классе В — 16 384 сети, а в классе С — более 2 миллионов.

Далее, размер сети каждого класса также значительно отличается. Каждая сеть класса А относительно велика (более 16 миллионов IP-адресов хостов на сеть), поскольку первоначально они были предназначены для использования большими компаниями и организациями. Сети класса В меньше (более 65 тысяч хостов на сеть). И наконец, у сетей класса С, предназначенных для малых организаций, есть по 254 адреса хоста в каждой сети (рис. 13.1).

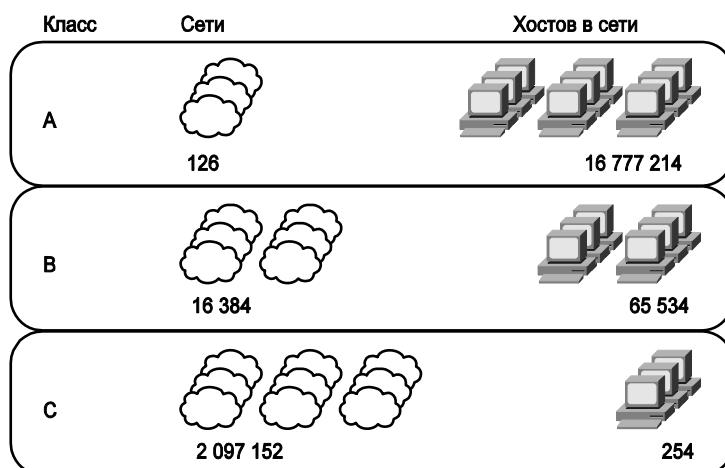


Рис. 13.1. Количество и размеры сетей класса А, В и С

Форматы адресов

Иногда сети класса А, В или С можно считать сетями, не разделенными на подсети. В таком случае у адресов классовой сети есть структура из двух частей: *часть сети* (network part), иногда называемая *префиксом* (prefix), и *часть хоста* (host part). Далее, сравнив два любых IP-адреса в одной сети, можно заметить следующее.

Сравнение частей сети и хоста адресов в той же классовой сети



- У адресов в той же сети одинаковые значения в части сети.
- У адресов в той же сети разные значения в части хоста.

Например, в сети класса А 10.0.0.0 по определению часть сети состоит из первого октета. В результате у всех адресов в части сети одинаковое значение, а именно 10 в первом октете. Если сравнить какие-нибудь два адреса в сети, у них будут разные значения в последних трех октетах (октетах хоста). Например, у IP-адресов 10.1.1.1 и 10.1.1.2 одинаковое значение (10) в части сети, но разные значения в части хоста.

На рис. 13.2 приведены формат и размеры (в битах) частей сети и хоста IP-адресов в сети класса А, В и С до того, как они будут разделены на подсети.

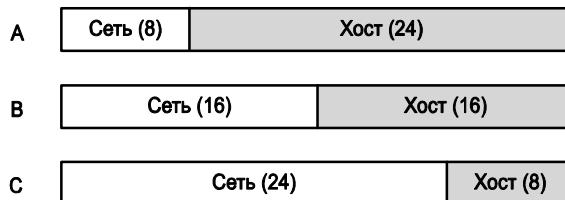


Рис. 13.2. Размеры (в битах) частей сети и хоста не разделенных на подсети классовых сетей

Маски по умолчанию

Хотя людям легко понять концепции, представленные на рис. 13.2, компьютеры предпочитают числа. Чтобы выразить эти же идеи для компьютера, с каждым классом сети связана *маска по умолчанию* (default mask), которая определяет размеры частей сети и хоста не разделенной на подсети сети класса А, В и С. Для этого маска содержит набор двоичных единиц для битов, которые принадлежат части сети, и двоичных нулей для битов, которые принадлежат части хоста.

Например, у сети класса А 10.0.0.0 есть часть сети в первом октете (8 битов) и часть хоста в последних трех октетах (24 бита). В результате маска по умолчанию (255.0.0.0) этого класса в двоичном виде выглядит так:

11111111 00000000 00000000 00000000

На рис. 13.3 представлены маски, заданные по умолчанию, для каждого класса сети в двоичном и десятичном форматах.

ВНИМАНИЕ!

Десятичное число 255 преобразуется в двоичное число 11111111. Десятичное число 0 преобразуется в 8-битовое двоичное число 00000000. Вся таблица числовых преобразований приведена в приложении Б.



A	<table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 15%;">Десятичный</td><td style="width: 15%;">255</td><td>.</td><td style="width: 15%;">0</td><td>.</td><td style="width: 15%;">0</td><td>.</td><td style="width: 15%;">0</td></tr> <tr> <td>Двоичный</td><td>11111111</td><td></td><td>00000000</td><td></td><td>00000000</td><td></td><td>00000000</td></tr> <tr> <td>Концепция</td><td colspan="4">Сеть (8)</td><td colspan="3">Хост (24)</td></tr> </table>	Десятичный	255	.	0	.	0	.	0	Двоичный	11111111		00000000		00000000		00000000	Концепция	Сеть (8)				Хост (24)		
Десятичный	255	.	0	.	0	.	0																		
Двоичный	11111111		00000000		00000000		00000000																		
Концепция	Сеть (8)				Хост (24)																				
B	<table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 15%;">Десятичный</td><td style="width: 15%;">255</td><td>.</td><td style="width: 15%;">255</td><td>.</td><td style="width: 15%;">0</td><td>.</td><td style="width: 15%;">0</td></tr> <tr> <td>Двоичный</td><td>11111111</td><td></td><td>11111111</td><td></td><td>00000000</td><td></td><td>00000000</td></tr> <tr> <td>Концепция</td><td colspan="4">Сеть (16)</td><td colspan="3">Хост (16)</td></tr> </table>	Десятичный	255	.	255	.	0	.	0	Двоичный	11111111		11111111		00000000		00000000	Концепция	Сеть (16)				Хост (16)		
Десятичный	255	.	255	.	0	.	0																		
Двоичный	11111111		11111111		00000000		00000000																		
Концепция	Сеть (16)				Хост (16)																				
C	<table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 15%;">Десятичный</td><td style="width: 15%;">255</td><td>.</td><td style="width: 15%;">255</td><td>.</td><td style="width: 15%;">255</td><td>.</td><td style="width: 15%;">0</td></tr> <tr> <td>Двоичный</td><td>11111111</td><td></td><td>11111111</td><td></td><td>11111111</td><td></td><td>00000000</td></tr> <tr> <td>Концепция</td><td colspan="4">Сеть (24)</td><td colspan="3">Хост (8)</td></tr> </table>	Десятичный	255	.	255	.	255	.	0	Двоичный	11111111		11111111		11111111		00000000	Концепция	Сеть (24)				Хост (8)		
Десятичный	255	.	255	.	255	.	0																		
Двоичный	11111111		11111111		11111111		00000000																		
Концепция	Сеть (24)				Хост (8)																				

Рис. 13.3. Заданные по умолчанию маски для классов A, B и C

Количество хостов на сеть

Вычисление количества хостов в сети требует некоторой простой двоичной математики. Сначала рассмотрим случай, когда есть один двоичный знак. Сколько индивидуальных значений он обеспечит? Конечно, это два значения: 0 и 1. С двумя битами можно получить четыре комбинации: 00, 01, 10 и 11. Таким образом, имея N битов, можно получить 2^N уникальных комбинаций.

Адреса хостов (IP-адреса, называемые хостам) должны быть уникальными. Биты хоста предназначены для предоставления каждому хосту уникального IP-адреса на основании разных значений в части хоста. Таким образом, имея H битов хоста, можно получить 2^H уникальных комбинаций.

Однако количество хостов в сети не 2^H , а $2^H - 2$. Каждая сеть резервирует два числа: одно для идентификатора сети и одно для широковещательного адреса сети. В результате формула вычисления количества хостов в сети класса A, B или C выглядит как $2^H - 2$, где H — количество битов хоста.

Определение идентификатора сети и связанных значений

У каждой классовой сети есть четыре ключевых числа, которые описывают сеть. Эти четыре числа можно получить, исходя только из одного IP-адреса в сети. Это следующие значения:

- номер сети;
- первый (в цифровой форме самый низкий) пригодный для использования адрес;
- последний (в цифровой форме самый высокий) пригодный для использования адрес;
- широковещательный адрес сети.

Сначала рассмотрим номер сети и первый пригодный для использования IP-адрес. *Номер сети* (network number), называемый также *идентификатором сети* (network ID) или *адресом сети* (network address), идентифицирует сеть. По определению номер сети (в цифровой форме) — это самый малый номер. Однако для предотвращения любой двусмысленности разработчики IP-адресации добавили ограничение: номер сети не может быть назначен как IP-адрес. Таким образом, самый младший номер в сети — это ее идентификатор, а первый пригодный для использования в качестве IP-адреса — *на единицу больше, чем номер сети*.

Затем рассмотрим широковещательный адрес сети наряду с последним (в цифровой форме самым старшим) пригодным для использования IP-адресом. Документ RFC по протоколу TCP/IP определяет широковещательный адрес сети как специальный адрес в каждой сети. Этот широковещательный адрес применим как адрес получателя пакета, и маршрутизаторы отправляют копию пакета с таким адресом всем хостам в данной классовой сети. В цифровой форме широковещательный адрес сети — это всегда самый старший (последний) номер в сети. В результате самый старший (последний) номер, пригодный для использования в качестве IP-адреса, является адресом, который *на единицу меньше, чем широковещательный адрес сети*.

Проще говоря, если можно определить номер и широковещательный адрес сети, вычисление первого и последнего пригодных для использования IP-адресов в сети элементарно. На экзамене нужно уметь легко определить все четыре значения следующим образом.

Этапы определения информации о классовой сети



- Этап 1** На основании первого октета определите класс сети (A, B или C).
- Этап 2** На основании класса мысленно разделите октеты на части сети и хоста.
- Этап 3** Для выяснения номера сети замените октеты хоста IP-адреса на 0.
- Этап 4** Для выяснения первого адреса добавьте 1 к четвертому октету идентификатора сети.
- Этап 5** Для выяснения широковещательного адреса замените октеты хоста идентификатора сети на 255.
- Этап 6** Для выяснения последнего адреса вычтите 1 из четвертого октета широковещательного адреса сети.

Описанный процесс выглядит сложней, чем он есть на самом деле. На рис. 13.4 приведен пример этого процесса для IP-адреса 10.1.2.3 сети класса A с соответствующими номерами этапов в кружочках.

На рис. 13.4 показана идентификация класса A сети (этап 1), а также количества октетов сети и хоста (1 и 3 соответственно). Чтобы выяснить идентификатор сети на этапе 3, скопирован только первый октет, последние три октета (хоста) заменены нулями. На этапе 4 скопирован только идентификатор сети и добавлена единица к четвертому октету. Аналогично для выяснения широковещательного адреса на этапе 5 скопированы октеты сети, а октеты хоста заменены на 255. Затем, на этапе 6, из четвертого октета вычтите 1, чтобы выяснить последний пригодный для использования IP-адрес.

Чтобы продемонстрировать альтернативный пример, рассмотрим IP-адрес 172.16.8.9. На рис. 13.5 приведен процесс применительно к этому IP-адресу.

Класс ① A B C
Разделение ② ↓

Сеть	Хост		
10	17	.	18 . 21
Часть хоста = 0 ③	10	0 . 0 . 0	+1
Добавить 1 ④	10	0 . 0 . 1	
Часть хоста = 255 ⑤	10	255 . 255 . 255	-1
Вычесть 1 ⑥	10	255 . 255 . 254	

Рис. 13.4. Пример определения идентификатора сети и других значений для адреса 10.17.18.21

Класс ① A B C
Разделение ② ↓

Сеть	Хост		
172 . 16 .	8 . 9		
Часть хоста = 0 ③	172 . 16 . 0 . 0		+1
Добавить 1 ④	172 . 16 . 0 . 1		
Часть хоста = 255 ⑤	172 . 16 . 255 . 255		-1
Вычесть 1 ⑥	172 . 16 . 255 . 254		

Рис. 13.5. Пример определения идентификатора сети и других значений для адреса 172.16.8.9

На рис. 13.5 показана идентификация класса В сети (этап 1), а также количества октетов сети и хоста (2 и 2 соответственно). Поскольку для выяснения идентификатора сети на этапе 3 скопированы только два первых октета, нулями заменены последние два октета (хоста). Аналогично этап 5 демонстрирует то же действие, но с установкой в 255 последних двух октетов (хоста).

Необычные идентификаторы сети и широковещательные адреса

Необычные номера из диапазона адресов сетей класса А, В и С, а также производные от них могут вызвать некоторое замешательство. В этом разделе приведены примеры некоторых необычно выглядящих, но вполне допустимых номеров, а также номеров, выглядящих вполне normally.

Для класса А первый странный факт — это то, что в диапазоне значений первого октета отсутствуют числа 0 и 127. Кроме того, то, что могло бы быть сетью класса А 0.0.0.0, первоначально резервировалось для некоторых широковещательных целей, таким образом, все адреса, которые начинаются с 0 в первом октете, зарезервированы

ны. То, что могло бы быть сетью класса А 127.0.0.0, все еще зарезервировано как специальный адрес, используемый при программной проверке, и называется *локальным диагностическим адресом* (loopback address) (127.0.0.1).

Для класса В (и С) некоторые из номеров сети могут выглядеть странно, особенно для тех, кто привык считать, что нули в конце означают идентификатор сети, а 255 в конце — широковещательный адрес сети. Во-первых, номера сети класса В располагаются в диапазоне от 128.0.0.0 до 191.255.0.0, в общей сложности 2^{14} сетей. Однако самый первый (младший) номер сети класса В (128.0.0.0) немного похож на номер сети класса А, поскольку он завершается тремя нулями. Но первый октет, 128, свидетельствует о том, что это сеть класса В с двумя октетами части сети (128.0).

Пример адреса 191.255.0.0 из верхней части диапазона сети класса В также может выглядеть странно на первый взгляд, но в действительности это самый верхний из допустимых адресов сети класса В. Широковещательный адрес такой сети (199.255.255.255) может немного походить на широковещательный адрес сети класса А из-за трех чисел 255 в конце, но в действительности это широковещательный адрес сети класса В.

Другие допустимые идентификаторы сети класса В, которые выглядят необычно, — это 130.0.0.0, 150.0.0.0, 155.255.0.0 и 190.0.0.0. Все они следуют соглашению о наличии значений от 128 до 191 в первом октете, значений от 0 до 255 во втором октете и двух или более нулей, поэтому они вполне допустимые идентификаторы сети класса В.

Сети класса С следуют тем же общим правилам, что и сети класса В, но с первыми тремя октетами, определяющими сеть. Номера сети находятся в диапазоне 192.0.0.0–223.255.255.0, с совпадающими значениями первых трех октетов для всех адресов в одной сети. Подобно сетям класса В, часть допустимых номеров сети класса С действительно выглядит странно. Например, сеть класса С 192.0.0.0 немного похожа на сеть класса А из-за последних трех октетов (0), но, поскольку это сеть класса С, она состоит из всех адресов, которые начинаются с трех октетов 192.0.0. Аналогично сеть класса С 223.255.255.0 — тоже вполне допустимая сеть класса С, состоящая из всех адресов, которые начинаются с 223.255.255.

Вот другие допустимые идентификаторы сети класса С, которые выглядят необычно: 200.0.0.0, 220.0.0.0, 205.255.255.0 и 199.255.255.0. Все они следуют соглашению о значении 192–223 в первом октете и значениях 0–255 во втором и третьем октетах, а также нулем в четвертом октете.

Практические задачи по классовым сетям

Подобно всем темам по IP-адресации и подсетям, на экзамене CCENT и CCNA необходимо быть готовым к практическим задачам. Перед экзаменом следует овладеть концепциями и процессами, описанными в данной главе, а также быть в состоянии отвечать быстро и правильно. Не буду слишком подчеркивать важность владения IP-адресацией и подсетями для экзаменов, просто знайте эти темы, и знайте их хорошо.

Однако не стоит учить все в этой главе прямо сейчас. Необходимо немного попрактиковаться, чтобы удостовериться в понимании процессов. Можно пока использовать свои записи, эту книгу или все, что угодно. Достаточно попрактиковавшись, чтобы подтвердить способность получить правильные ответы, используя лю-

бую доступную помощь, темы этой главы станут понятны достаточно хорошо, чтобы можно было переходить к следующей главе.

Перед экзаменом попрактикуйтесь, чтобы овладеть темой данной главы полностью и отвечать достаточно быстро. Ключевые концепции и рекомендации такого двухэтапного подхода приведены в табл. 13.4.

Таблица 13.4. Продолжайте читать с учетом целей экзамена по темам данной главы

Период	Перед переходом к следующей главе	Перед сдачей экзамена
Сосредоточиться на ...	теме изучения	Быть быстрым и правильным
Разрешенные средства	Все	Ваш мозг и блокнот
Цель: точность	90% правильных ответов	100% правильных ответов
Цель: скорость	Любая скорость	10 секунд

Практические задания, следующие из ключевых фактов об IP-адресе

Примеры практических заданий по поиску различных фактов, следующие из ключевых фактов об IP-адресе, обсуждавшихся в этой главе, приведены в табл. 13.5. Попробуйте заполнить эту таблицу.

Таблица 13.5. Практическое задание: поиск идентификатора и широковещательного адреса сети

	IP-адрес	Класс	Количество октетов сети	Количество октетов хоста	Идентификатор сети	Широковещательный адрес сети
1	1.1.1.1					
2	128.1.6.5					
3	200.1.2.3					
4	192.192.1.1					
5	126.5.4.3					
6	200.1.9.8					
7	192.0.0.1					
8	191.255.1.47					
9	223.223.0.1					

Ответы приведены ниже, в разделе “Ответы на приведенные ранее практические задания”.

Практическое задание на запоминание подробностей о классах адресов

В табл. 13.2 и 13.3, приведенных ранее в этой главе, содержалась некая ключевая информация о классах IPv4-адресов. Табл. 13.6 и 13.7 представляют собой не заполненные версии тех же таблиц. Попробуйте вспомнить эти ключевые факты, особенно диапазон значений в первом октете, который идентифицирует класс адресов, и заполнить эти таблицы. Затем вернитесь к табл. 13.2 и 13.3 и проверьте свои ответы. Повторяйте этот процесс до тех пор, пока не сможете запомнить всю информацию в таблицах.

Таблица 13.6. Не заполненная версия табл. 13.2

Значения первого октета	Класс	Назначение
	A	
	B	
	C	
	D	
	E	

Таблица 13.7. Не заполненная версия табл. 13.3

Частные сети IP	Класс А	Класс В	Класс С
Диапазон первого октета			
Допустимые адреса сети			
Всего сетей			
Хостов на сеть			
Октеты (биты) в части сети			
Октеты (биты) в части хоста			
Маска по умолчанию			

Дополнительные практические задания

Для дополнительной практики по классовым сетям можно использовать следующее.

- Приложение Г, в котором содержатся дополнительные практические задачи. Оно содержит также объяснения по поиску ответа каждого задания. Приложение в формате PDF находится на прилагаемом к книге компакт-диске.
- Создайте собственные задания. Можно случайно выбрать любой IP-адрес и попытаться выяснить ту же информацию, что и в практических заданиях этого раздела. Затем, чтобы проверить ответ, воспользуйтесь любым калькулятором подсетей. Большинство калькуляторов подсетей вычисляют класс и идентификатор сети. (Несколько калькуляторов предложено на веб-странице автора этой книги, указанной во введении.)
- Приложение Analyze Networks для iPhone на Subnet Prep (www.subnetprep.com) предоставляет обзорное видео и практически безграничное количество практических заданий; это отличный способ улучшить скорость решения задач, когда предоставляется свободная минута.

Подготовка к экзамену

Повторите все ключевые темы

Повторите все ключевые темы данной главы, помеченные пиктограммой “Ключевая тема”. Ключевые темы и соответствующие им страницы перечислены в табл. 13.8.

Таблица 13.8. Ключевые темы главы 13

Элемент	Описание	Страница
Табл. 13.2	Классы IPv4-адресов на основании значения первого октета	391
Табл. 13.3	Основные факты о классах А, В и С	392
Список	Сравнение частей сети и хоста адресов в той же классовой сети	393
Рис. 13.3	Заданные по умолчанию маски для классов А, В и С	394
Список	Этапы определения информации о классовой сети	395

Заполните таблицы и списки по памяти

Распечатайте приложение М (Appendix L) с компакт-диска или его раздел, относящийся к этой главе, и заполните таблицы и списки по памяти. В приложении Н (Appendix M) приведены заполненные таблицы и списки для самоконтроля.

Ключевые термины

Дайте определения перечисленных ниже терминов и проверьте правильность их написания в списке терминов:

сеть (network), классовая сеть (classful network), номер сети (network number), идентификатор сети (network ID), адрес сети (network address), широковещательный адрес сети (network broadcast address), первый адрес (first address), последний адрес (last address), часть сети (network part), часть хоста (host part), заданная по умолчанию маска (default mask)

Практика

Если это еще не сделано, попрактикуйтесь в вопросах выявления деталей классовой сети, описанных в данной главе. Рекомендации приведены в разделе “Практические задачи по классовым сетям”.

Ответы на приведенные ранее практические задания

Набор практических заданий см. в табл. 13.5, а ответы приведены в табл. 13.9.

Таблица 13.9. Практическое задание: поиск идентификатора и широковещательного адреса сети

IP-адрес	Класс	Количество октетов сети	Количество октетов хоста	Идентификатор сети	Широковещательный адрес сети
1 1.1.1.1	A	1	3	1.0.0.0	1.255.255.255
2 128.1.6.5	B	2	2	128.1.0.0	128.1.255.255

Окончание табл. 13.9

IP-адрес	Класс	Количество октетов сети	Количество октетов хоста	Идентификатор сети	Широковещательный адрес сети
3 200.1.2.3	C	3	1	200.1.2.0	200.1.2.255
4 192.192.1.1	C	3	1	192.192.1.0	192.192.1.255
5 126.5.4.3	A	1	3	126.0.0.0	126.255.255.255
6 200.1.9.8	C	3	1	200.1.9.0	200.1.9.255
7 192.0.0.1	C	3	1	192.0.0.0	192.0.0.255
8 191.255.1.47	B	2	2	191.255.0.0	191.255.255.255
9 223.223.0.1	C	3	1	223.223.0.0	223.223.0.255

Чтобы определить класс, количество октетов сети и хоста, необходимо обратить внимание на первый октет IP-адреса. Если значение находится в диапазоне от 1 до 126 включительно, значит, адрес принадлежит сети класса А, с одним октетом сети и тремя октетами хоста. Если значение находится между 128 и 191 включительно, то адрес принадлежит сети класса В, с двумя октетами сети и двумя хоста. Если значение находится между 192 и 223 включительно — это адрес класса С, с тремя октетами сети и одним октетом хоста.

Значения последних двух столбцов находят на основании табл. 13.3, а именно количества октетов сети и хоста наряду с IP-адресом. Для поиска идентификатора сети скопируйте IP-адрес, но измените октеты хоста на 0. Аналогично для поиска широковещательного адреса сети скопируйте IP-адрес, но измените октеты хоста на 255.

Последние три задания могут вызвать сомнение, они были включены нарочно, чтобы продемонстрировать пример таких необычных случаев.

Ответ на практическое задание 7

Рассмотрим IP-адрес 192.0.0.1. Первый октет, 192, находится ближе к нижней границе диапазона класса С; таким образом, у этого адреса есть три октета сети и один октет хоста. Для поиска идентификатора сети скопируйте адрес, но измените один октет хоста (четвертый) на 0. В результате получится 192.0.0.0. Выглядит странно, но это действительно идентификатор сети.

Нахождение широковещательного адреса сети для задания 7 также может выглядеть странно. Для этого скопируйте IP-адрес (192.0.0.1), но измените последний октет (единственный октет хоста) на 255. Получится широковещательный адрес 192.0.0.255. В частности, если покажется, что широковещательным адресом должен быть 192.255.255.255, значит, вы попали в ловушку. Сработала логика: “Замените все нули в идентификаторе сети на 255”, что не является правильным. Вместо этого на 255 нужно изменить все октеты хоста в IP-адресе (или идентификаторе сети).

Ответ на практическое задание 8

Первый октет в задании 8 (191.255.1.47) находится в верхней части диапазона адресов сети класса В (128–191). Таким образом, для поиска идентификатора сети измените последние два октета (октеты хоста) на 0, получится 191.255.0.0. Это значение иногда создает проблемы, поскольку люди привыкли думать, что 255 означает широковещательный адрес.

Широковещательный адрес находится при замене двух октетов хоста на 255 и составляет 191.255.255.255. Выглядит скорее как широковещательный адрес сети класса А, но на самом деле это широковещательный адрес сети класса В 191.255.0.0.

Ответ на практическое задание 9

Последняя проблема с IP-адресом 223.223.0.1 заключается в том, что он ближе к верхней части диапазона адресов класса С. В результате, чтобы сформировать идентификатор сети 223.223.0.0, изменить на нуль нужно только последний октет (хоста). Выглядит похоже на номер сети класса В, поскольку заканчивается нулями в двух октетах, но это в действительности идентификатор сети класса С (на основании значения в первом октете).

В этой главе...

- **Преобразование масок подсети.** Описано преобразование между тремя форматами маски подсети: двоичного, десятичного и префиксного.
- **Практические задания по преобразованию масок подсети.** Предоставлены практические задачи и советы по преобразованию между тремя форматами маски подсети.

ГЛАВА 14

Преобразование маски подсети

Маски подсети служат многим важным целям в мире IPv4-адресации и создания подсетей. Но данная глава игнорирует эти цели. Вместо них она сосредоточена на числах, используемых как маски подсети, точнее, на трех разных форматах их представления:

- двоичное представление;
- десятичное представление с разделительными точками (Dotted Decimal Notation — DDN);
- префиксное представление (называемое также CIDR).

В текущей главе описываются числа и преобразования между тремя их различными форматами, чтобы в последующих главах можно было работать с масками без применения математики.

Контрольные вопросы: знаете ли вы уже темы главы

Этот раздел предназначен для того, чтобы читатель мог предварительно оценить свои знания и решить, нужно ли ему читать главу целиком. Если ответы на девять из десяти вопросов даны правильно, можно сразу же перейти к последнему разделу “Подготовка к экзамену”. Основные темы этой главы и предварительных контрольных вопросов перечислены в табл. 14.1. Отвечая на контрольные вопросы и используя таблицу, читатель сможет достаточно точно определить свои знания в той или иной области. Ответы на вопросы приведены в приложении А.

Таблица 14.1. Темы контрольных вопросов

Основная тема	Номера вопросов
Преобразование масок подсети	1–6

1. Какие из следующих ответов представляют префиксный (CIDR) эквивалент маски 255.255.254.0?
 - а) /19
 - б) /20
 - в) /23
 - г) /24
 - д) /25
2. Какие из следующих ответов представляют префиксный (CIDR) эквивалент маски 255.255.255.240?

- а) /26
- б) /28
- в) /27
- г) /30
- д) /29

3. Какие из следующих ответов представляют префиксный (CIDR) эквивалент маски 255.255.192.0?

- а) /18
- б) /19
- в) /20
- г) /21
- д) /22

4. Какие из следующих ответов представляют десятичный (DDN) эквивалент маски /24?

- а) 255.255.240.0
- б) 255.255.252.0
- в) 255.255.255.0
- г) 255.255.255.192
- д) 255.255.255.240

5. Какие из следующих ответов представляют десятичный (DDN) эквивалент маски /30?

- а) 255.255.255.192
- б) 255.255.255.252
- в) 255.255.255.240
- г) 255.255.254.0
- д) 255.255.255.0

6. Какие из следующих ответов представляют десятичный (DDN) эквивалент маски /21?

- а) 255.255.240.0
- б) 255.255.248.0
- в) 255.255.252.0
- г) 255.255.254.0
- д) 255.255.255.0

Основные темы

Преобразование масок подсети

В этом разделе описано преобразование между различными форматами маски подсети. Впоследствии эти процессы можно использовать при решении практических задач. Если преобразования из одного формата в другой уже знакомы, переходите сразу к разделу “Практические задания по преобразованию масок подсети”.

Три формата масок

Маски подсети могут быть записаны как 32-разрядные двоичные числа, но не любые. В частности, двоичная маска подсети должна следовать таким правилам:

Правила для двоичных значений маски подсети



- Значение не должно чередовать единицы и нули.
- Если есть единицы, они располагаются слева.
- Если есть нули, они располагаются справа.

Например, следующие значения недопустимы. Первое недопустимо потому, что чередуются значения 0 и 1, а второе потому, что 0 находится слева, а 1 справа:

10101010 01010101 11110000 00001111
00000000 00000000 00000000 11111111

Следующие два двоичных значения отвечают требованиям, согласно которым все 1 слева, а затем все 0 справа, без чередования 1 и 0:

11111111 00000000 00000000 00000000
11111111 11111111 11111111 00000000

Существуют еще два дополнительных формата маски подсети, чтобы людям не приходилось работать непосредственно с 32-битовыми двоичными числами. Один формат, *десятичное представление с разделительными точками* (Dotted-Decimal Notation — DDN), преобразует каждый набор из 8 битов в десятичный эквивалент. Например, две предыдущие двоичные маски можно преобразовать в следующие маски DDN, поскольку двоичные значения 11111111 преобразуются в десятичные 255, а двоичные 00000000 — в десятичное число 0.

255.0.0.0
255.255.255.0

Хотя формат DDN существовал с момента появления IPv4-адресации, третий, *префиксный* (prefix), формат маски был добавлен позже, в начале 1990-х годов. Этот формат использует правило, согласно которому маска подсети начинается с некоторого количества единиц, а остальные цифры являются нулями. Префиксный формат включает наклонную черту (/), сопровождающую количеством двоичных единиц в двоичной маске. Используя те же два примера, что и ранее, получим следующие эквиваленты масок в префиксном формате:

/8
/24

Обратите внимание на то, что могут использоваться термины *префикс* (prefix), или *префиксная маска* (prefix mask), и *маска CIDR* (CIDR mask), или *маска после наклонной черты* (slash mask). Этот более новый стиль префиксной маски появился одновременно со спецификацией *бесклассовой адресации* (Classless Interdomain Routing — CIDR) в начале 1990-х годов, и аббревиатуру CIDR ассоциировали со всем, что было связано с адресацией CIDR, включая маски префиксного стиля. Кроме того, термин *маска после наклонной черты* иногда используется потому, что значение маски включает наклонную черту (/).

И в реальной жизни, и на экзаменах Cisco CCENT и CCNA необходимо уметь работать с масками в любых форматах. В оставшейся части этого раздела рассматриваются преобразования между тремя форматами.

Преобразование между двоичным и префиксным форматами

Преобразование между двоичным и префиксным форматами маски должно быть относительно интуитивно понятным, поскольку известно, что префиксное значение — это просто количество двоичных единиц в двоичной маске. Для окончности изложения рассмотрим преобразование в каждом направлении.



Правила преобразования между двоичными и префиксными формами маски

- **Из двоичной в префиксную.** Подсчитайте количество единиц в двоичной маске и запишите его в десятичной форме после /.
- **Из префиксной в двоичную.** Напишите количество единиц, соответствующее префиксному значению, и дополните их нулями до размера 32-разрядного двоичного числа.

В табл. 14.2 и 14.3 приведено несколько примеров.

Таблица 14.2. Пример преобразования: двоичная — в префиксную

Двоичная маска	Логика	Предфиксная маска
11111111 11111111 11000000 00000000	Подсчитать $8 + 8 + 2 = 18$ единиц	/18
11111111 11111111 11111111 11110000	Подсчитать $8 + 8 + 8 + 4 = 28$ единиц	/28
11111111 11111000 00000000 00000000	Подсчитать $8 + 5 = 13$ единиц	/13

Таблица 14.3. Пример преобразования: префиксная — в двоичную

Предфиксная маска	Логика	Двоичная маска
/18	Написать 18 единиц, затем 14 нулей (всего 32)	11111111 11111111 11000000 00000000
/28	Написать 28 единиц, затем 4 нуля (всего 32)	11111111 11111111 11111111 11110000
/13	Написать 13 единиц, затем 19 нулей (всего 32)	11111111 11111000 00000000 00000000

Преобразование между двоичным форматом и DDN

По определению *десятичное число с разделительными точками* (DDN), используемое в IPv4-адресации, содержит четыре десятичных числа, отделенных точками. Каждое десятичное число представляет 8 битов. Так, одно число DDN представляется

четыре десятичных числа, которые вместе представляют некое 32-разрядное двоичное число.

Преобразование маски из формата DDN в двоичный эквивалент относительно просто, но может оказаться трудоемко. Процесс преобразования описан ниже.

Для каждого октета осуществить преобразование из десятичной формы в двоичную.

Однако в зависимости от умения выполнять преобразование чисел из десятичной системы в двоичную этот процесс может быть трудоемким или длительным. Чтобы справиться с преобразованием масок на экзамене, выберите один из следующих методов преобразования и добейтесь его осуществления очень быстро и точно.

- Осуществляйте десятично-двоичные преобразования, но попрактикуйтесь, чтобы делать их быстро. Если решите выбрать этот путь, попробуйте игру Binary Game от Cisco, которую можно найти в учебной сети Cisco Learning Network (CLN) (learningnetwork.cisco.com).
- Используйте таблицу десятично-двоичных преобразований из приложения Б. Это позволит находить ответы быстрее сейчас, но на экзамене ею воспользоваться не удастся.
- Запомните девять десятичных значений, которые могут быть в десятичной маске, и попрактикуйтесь в использовании справочной таблицы с этими значениями.

Третий метод является рекомендуемым методом в этой книге, он основан на том факте, что любой и каждый десятичный октет маски может иметь только одно из девяти значений. Почему? Помните, что двоичная маска не может чередовать 1 и 0, а 0 расположены справа? Этим правилам соответствуют только девять 8-битовых двоичных чисел. В табл. 14.4 приведен список этих значений, а также другая полезная информация.

Таблица 14.4. Девять значений, возможных в одном октете маски подсети

Двоичный октет	Десятичный эквивалент	Количество двоичных единиц
00000000	0	0
10000000	128	1
11000000	192	2
11100000	224	3
11110000	240	4
11111000	248	5
11111100	252	6
11111110	254	7
11111111	255	8

Множество процессов создания подсетей, полагающихся на использование двоичной математики, может быть также осуществлено и без двоичной математики. Некоторые из них (включая преобразования маски) подразумевают использование информации из табл. 14.4. Необходимо запомнить информацию этой таблицы. Рекомендуется сделать копию таблицы для удобства на время тренировки. (Вы, вероятно, запомните содержимое этой таблицы в процессе практики преобразований, причем вполне достаточно, чтобы осуществлять их быстро и правильно.)

С использованием таблицы процессы преобразования в каждом направлении с двоичными и десятичными масками осуществляются так:

Ключевая тема

Правила преобразования между двоичной и DDN формами маски

- **Из двоичной в десятичную.** Для каждого октета найдите в таблице двоичное значение и запишите соответствующее десятичное значение.
- **Из десятичной в двоичную.** Для каждого октета найдите в таблице десятичное значение и запишите соответствующее двоичное значение.

В табл. 14.5 и 14.6 приведено несколько примеров.

Таблица 14.5. Пример преобразования: двоичная — в десятичную

Двоичная маска	Логика	Десятичная маска
11111111 11111111 11000000 00000000	11111111 в 255 11000000 в 192 00000000 в 0	255.255.192.0
11111111 11111111 11111111 11110000	11111111 в 255 11110000 в 240	255.255.255.240
11111111 11111000 00000000 00000000	11111111 в 255 11111000 в 248 00000000 в 0	255.248.0.0

Таблица 14.6. Пример преобразования: десятичная — в двоичную

Десятичная маска	Логика	Двоичная маска
255.255.192.0	255 в 11111111 192 в 11000000 0 в 00000000	11111111 11111111 11000000 00000000
255.255.255.240	255 в 11111111 240 в 11110000	11111111 11111111 11111111 11110000
255.248.0.0	255 в 11111111 248 в 11111000 0 в 00000000	11111111 11111000 00000000 00000000

Преобразование между префиксным форматом и DDN

При обучении наилучший способ преобразования между префиксным и десятичным форматами подразумевает предварительное преобразование в двоичный формат. Например, чтобы перейти от десятичного числа к префиксному, сначала преобразуйте его в двоичное, а затем двоичное в префиксное.

При подготовке к экзамену добейтесь способности вычислять эти преобразования в уме. При обучении вы, вероятно, захотите использовать бумагу. Для тренировки попробуйте записывать не все в каждом октете двоичного числа, а только количество двоичных единиц.

На рис. 14.1 приведен пример преобразования префикса в десятичное число. Слева показан промежуточный этап преобразования в двоичный формат. Для сравнения справа приведен промежуточный этап преобразования в двоичный формат сокращено, где следует указать только количество двоичных единиц в каждом октете двоичной маски.



Рис. 14.1. Преобразование из префиксного формата в десятичный: полная и сокращенная формы

Аналогично при преобразовании десятичного числа в префикс мысленно преобразуйте его в двоичное, а по мере приобретения навыка используйте только количество единиц в каждом октете двоичного числа. На рис. 14.2 приведен пример такого преобразования.

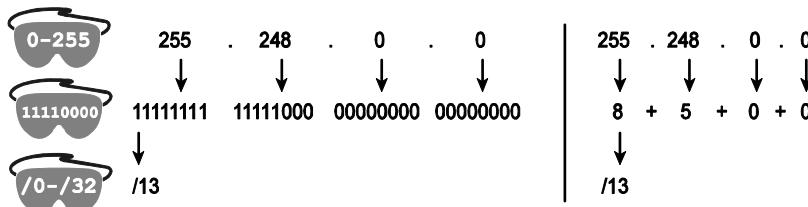


Рис. 14.2. Преобразование из десятичного формата в префиксный: полная и сокращенная формы

Обратите внимание: в приложении Б есть таблица, в которой перечислены все 33 допустимые маски подсети во всех трех форматах.

Практические задания по преобразованию масок подсети

Прежде чем перейти к следующей главе, попрактикуйтесь в процессах, обсуждаемых в данной главе, пока не станете получать правильные ответы почти всегда. Используйте любые средства по своему усмотрению и любое время. Затем можно продолжить чтение. Однако перед сдачей экзамена потренируйтесь, чтобы овладеть темой данной главы полностью и отвечать достаточно быстро. Ключевые концепции и рекомендации такого двухэтапного подхода приведены в табл. 14.7.

Таблица 14.7. Продолжайте читать с учетом целей экзамена по темам данной главы

Период	Перед переходом к следующей главе	Перед сдачей экзамена
Сосредоточиться на ...	теме изучения	Быть быстрым и правильным
Разрешенные средства	Все	Ваш мозг и блокнот
Цель: точность	90% правильных ответов	100% правильных ответов
Цель: скорость	Любая скорость	10 секунд

Практические задания этой главы

В табл. 14.8 содержатся три столбца: префиксная маска, двоичная и десятичная. В каждой строке приведена маска в одном из трех форматов. Задача — найти значение маски в других двух форматах по каждой строке. Ответы приведены в табл. 14.10.

Таблица 14.8. Практическое задание: поиск значения маски в двух других форматах

Префиксная маска	Двоичная	Десятичная
	11111111 11111111 11000000 00000000	255.255.255.252
/25		
/16		255.0.0.0
	11111111 11111111 11111100 00000000	255.254.0.0
/27		

Дополнительные практические задания

Для дополнительной практики по преобразованию масок подсети можно использовать следующее.

- Приложение Д, в котором содержатся дополнительные практические задания. Оно содержит также объяснения по поиску ответа каждого задания.
- Создайте собственные задания. Поскольку существует только 33 корректных маски подсети, выберите любую и преобразуйте ее в два других формата. Затем проверьте ответ в приложении Б, где перечислены все значения масок во всех трех форматах. (Рекомендация: преобразуйте префикс в двоичный формат, а затем в десятичный. Потом преобразуйте маску DDN в двоичный и префиксный форматы.)
- Приложение Convert Masks для iPhone на Subnet Prep (www.subnetprep.com) предоставляет обзорное видео и практические задания; это отличный способ улучшить скорость решения задач, когда предоставляется свободная минута.

Подготовка к экзамену

Повторите все ключевые темы

Повторите все ключевые темы данной главы, помеченные пиктограммой “Ключевая тема”. Ключевые темы и соответствующие им страницы перечислены в табл. 14.9.

Таблица 14.9. Ключевые темы главы 14

Элемент	Описание	Страница
Список	Правила для двоичных значений маски подсети	407
Список	Правила преобразования между двоичными и префиксными формами маски	408
Список	Правила преобразования между двоичной и DDN формами маски	410

Ключевые термины

Дайте определения перечисленных ниже терминов и проверьте правильность их написания в списке терминов:

двоичная маска (binary mask), десятичное представление с разделительными точками (Dotted-Decimal Notation — DDN), десятичная маска (decimal mask), префиксная маска (prefix mask), маска после наклонной черты (slash mask), маска CIDR (CIDR mask)

Практика

Если это еще не сделано, попрактикуйтесь в вопросах преобразования маски подсети, описанных в данной главе. Рекомендации приведены в разделе “Практические задания по преобразованию масок подсети”.

Ответы на приведенные ранее практические задания

Набор практических задач представлен ранее в табл. 14.8, а ответы приведены в табл. 14.10.

Таблица 14.10. Ответы на практические задания табл. 14.8

Префиксная	Двоичная маска	Десятичная
/18	11111111 11111111 11000000 00000000	255.255.192.0
/30	11111111 11111111 11111111 11111100	255.255.255.252
/25	11111111 11111111 11111111 10000000	255.255.255.128
/16	11111111 11111111 00000000 00000000	255.255.0.0
/8	11111111 00000000 00000000 00000000	255.0.0.0
/22	11111111 11111111 11111100 00000000	255.255.252.0
/15	11111111 11111110 00000000 00000000	255.254.0.0
/27	11111111 11111111 11111111 11100000	255.255.255.224

В этой главе...

- **Определение формата IPv4-адресов.** Описано, как маска подсети и класс адресов разделяют IP-адрес на части сети, подсети и хоста.
- **Практические задания по анализу масок подсети.** Содержатся рекомендации по применению на практике математического механизма, связанного с данной главой.

ГЛАВА 15

Анализ существующих масок подсети

Исследуя существующий проект подсети, при анализе маски можно узнать довольно много о проекте. Сначала маска делит адрес на две части: *префикс* и *хост*. Затем класс сети разделяет префиксную часть адреса на части *сети* и *подсети*.

Как только размер трех частей IP-адреса будет известен, можно сделать некоторые обобщения о подсети и всей классовой сети. Данная глава поможет перепроектировать некоторые из уже сделанных выборов в проекте, когда некто уже выбрал определенную маску. Для этого в главе исследуется процесс разделения IP-адресов на три части (сеть, подсеть и хост) на основании класса и маски подсети наряду с дополнительными факторами, которые впоследствии могут быть вычислены на основании этой информации.

Контрольные вопросы: знаете ли вы уже темы главы

Этот раздел предназначен для того, чтобы читатель мог предварительно оценить свои знания и решить, нужно ли ему читать главу целиком. Если ответы на девять из десяти вопросов даны правильно, можно сразу же перейти к последнему разделу “Подготовка к экзамену”. Основные темы этой главы и предварительных контрольных вопросов перечислены в табл. 15.1. Отвечая на контрольные вопросы и используя таблицу, читатель сможет достаточно точно определить свои знания в той или иной области. Ответы на вопросы приведены в приложении А.

Таблица 15.1. Темы контрольных вопросов

Основная тема	Номера вопросов
Определение формата IPv4-адресов	1–6

1. Работая в службе технической поддержки, вы, получив звонок, изучаете IP-адрес (10.55.66.77) и маску (255.255.255.0) компьютера пользователя. Размышляя с точки зрения классовой логики, вы определяете количество битов сети (N), подсети (S) и хоста (H). Что из приведенного ниже истинно в данном случае?

- а) N=12
- б) S=12
- в) H=8
- г) S=8
- д) N=24

2. Работая в службе технической поддержки, вы, получив звонок, изучаете IP-адрес и маску (192.168.9.0/27) компьютера пользователя. Размышляя с точки зрения классовой логики, вы определяете количество битов сети (N), подсети (S) и хоста (H). Что из приведенного ниже истинно в данном случае?
- а) N=24
 - б) S=24
 - в) H=8
 - г) H=7
3. Работая в службе технической поддержки, вы, получив звонок, изучаете IP-адрес (172.28.99.101) и маску (255.255.255.128) компьютера пользователя. Размышляя с точки зрения классовой логики, вы определяете количество битов сети (N), подсети (S) и хоста (H). Что из приведенного ниже истинно в данном случае?
- а) N=12
 - б) S=12
 - в) H=8
 - г) S=8
 - д) N=16
4. Инженер обдумывает с точки зрения логики бесклассовой IP-адресации следующий IP-адрес и маску: 10.55.66.77, 255.255.255.0. Какие из следующих утверждений истинны? (Выберите несколько ответов.)
- а) Размер части сети составляет 8 битов.
 - б) Длина префикса составляет 24 бита.
 - в) Длина префикса составляет 16 битов.
 - г) Размер части хоста составляет 8 битов.
5. Какое из следующих утверждений истинно с точки зрения бесклассовых концепций IP-адресации?
- а) Используется 128-битовый IP-адрес.
 - б) Применимы только для сетей класса А и В.
 - в) Разделяет IP-адреса на части сети, подсети и хоста.
 - г) Игнорирует правила сетей класса А, В и С.
6. Какая из следующих масок при использовании в качестве единой маски в пределах сети класса В предоставила бы достаточно битов подсети для поддержки 100 подсетей? (Выберите несколько ответов.)
- а)/24
 - б) 255.255.255.252
 - в)/20
 - г) 255.255.252.0

Основные темы

Определение формата IPv4-адресов

У масок подсети много задач. Например, маска определяет префиксную часть IPv4-адресов в подсети, которая должна иметь одинаковое значение для всех адресов в подсети.

На рис. 15.1 представлены две подсети: все адреса одной из них начинаются с 172.16.2, а другой — с 172.16.3. В этом примере у адресов подсети одинаковое значение в первых трех октетах. Но как компьютеры и другие сетевые устройства узнают этот факт? Зная маску подсети, в данном случае /24, можно определить префиксную часть как первые три октета адресов.

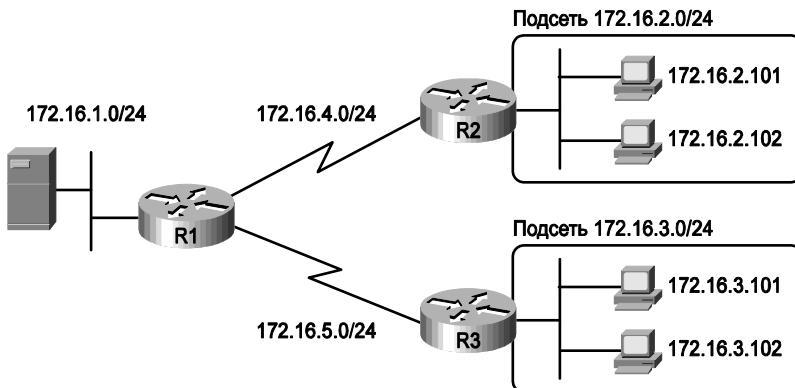


Рис. 15.1. Пример проекта подсети с маской /24

Маски подсети определяют некоторые фундаментальные концепции подсети, а также применяются в различных математических операциях, связанных с адресацией и созданием подсетей. Фактически маска подсети используется в данной подсети для следующих целей.

Некоторые из функций маски подсети



- Определяет размер префиксной части (сети и подсети) адресов подсети.
- Определяет размер части хоста адресов подсети.
- Применяется при вычислении количества хостов в подсети.
- Предоставляет сетевому инженеру средство выяснения подробностей о проекте подсети (количество битов подсети и хоста).
- Согласно определению используется при вычислении количества подсетей во всей классовой сети.
- Применяется в двоичных вычислениях идентификатора и широковещательного адреса подсети.

В этой главе рассматриваются четыре первых элемента списка, а остальные роли маски подсети обсуждаются в главах 16 и 17.

Маски делят адреса подсети на две части

Маска подсети разделяет IP-адреса подсети на две части: *префикса* (или *подсети*) и *хоста*.

Часть префикса идентифицирует адреса, которые располагаются в той же подсети, поскольку у всех IP-адресов в той же подсети одинаковое значение в префиксной части их адресов. Идея очень похожа на почтовый индекс в адресах обычной почты. У всех почтовых адресов в одном городе одинаковый почтовый индекс. Аналогично у всех IP-адресов в одной подсети идентичные значения в префиксной части адресов.

Часть хоста в адресе уникально идентифицирует хост в подсети. Если сравнить какие-нибудь два IP-адреса в той же подсети, то их части хоста будут отличаться, даже при том, что в префиксных частях их адресов то же значение. Подведем итог сравнения.



Сравнение IP-адресов в одной подсети

- **Часть префикса (подсети).** Однаковы во всех адресах той же подсети.
- **Часть хоста.** Различны во всех адресах той же подсети.

Предположим, например, что есть подсеть, которая концептуально включает все адреса, тремя первыми октетами которой являются 10.1.1. Несколько адресов этой подсети приведено ниже.

10.1.1.1
10.1.1.2
10.1.1.3

В этом списке части префикса или подсети (первые три октета 10.1.1) одинаковы, а части хоста (последний октет, выделенный полужирным шрифтом) разные. Таким образом, часть префикса или подсети адреса идентифицирует группу, а часть хоста — определенный элемент группы.

Маска подсети определяет разделительную линию между частями префикса и хоста. Для этого маска создает концептуальную линию между двоичными единицами и нулями. Короче говоря, если маска имеет Р двоичных единиц, то префиксная часть имеет длину в Р бит, а остальная часть битов является битами хоста. Общая концепция представлена на рис. 15.2.



Рис. 15.2. Части префикса (подсети) и хоста, разделенные единицами и нулями маски

На рис. 15.2 представлена общая концепция, а на рис. 15.3 — та же концепция, но с конкретной маской 255.255.255.0. Как показано на рис. 15.3, маска 255.255.255.0 (/24) имеет 24 единицы, а следовательно, у первых трех октетов каждого IP-адреса должно быть одинаковое значение, точно как в примере, приведенном ниже.



Рис. 15.3. Маска 255.255.255.0: P=24, H=8

Маски и классы делят адреса на три части

Кроме представления с двумя частями IPv4-адресов, возможно наличие трех частей. Для этого достаточно применить к формату адреса правила класса А, В и С, чтобы выявить часть сети в начале адреса. Эта дополнительная логика делит префикс на две части: часть *сети* и часть *подсети*. Класс определяет длину части сети, а часть подсети является остальной частью префикса. Концепция представлена на рис. 15.4.



Рис. 15.4. Применение концепции класса для создания трех частей адреса

Совместно части сети и подсети составляют префикс, поскольку у всех адресов в той же подсети должны быть идентичные значения в частях подсети и сети. При рассмотрении адреса с точки зрения наличия двух или трех частей часть хоста остается неизменной.

Для полноты картины на рис. 15.5 демонстрируется тот же пример, что и в предыдущем разделе, с подсетью “все адреса, которые начинаются с 10.1.1”. В этом примере подсеть использует маску 255.255.255.0, и все адреса принадлежат сети класса А 10.0.0.0. Класс определяет 8 битов сети, а маска — 24 бита префикса, значит, в подсети существует $24 - 8 = 16$ битов. Часть хоста остается равной 8 битам, согласно маске.

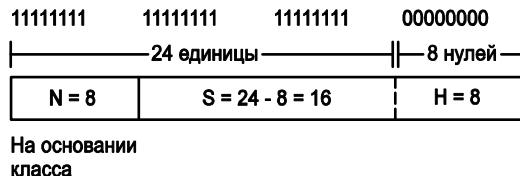


Рис. 15.5. Подсеть 10.1.1.0, маска 255.255.255.0: N=8, S=16, H=8

Бесклассовая и классовая адресация

Термины *бесклассовая адресация* (classless addressing) и *классовая адресация* (classful addressing) относятся к двум разным способам восприятия IPv4-адресов, как было описано в этой главе. Классовая адресация предполагает, что применяются правила классов А, В и С, таким образом, префикс разделяется на части сети и подсети, как на рис. 15.4 и 15.5. Бесклассовая адресация означает, что правила классов А, В и С игнорируются, т.е. префиксная часть считается единой частью, как показано на рис. 15.2 и 15.3. Следующие более формальные определения приведены для справки и изучения.



Определения классовой и бесклассовой адресации

- **Бесклассовая адресация.** Концепция наличия у IPv4-адреса двух частей (префиксной и хоста), определенных только маской, *без учета класса* (A, B или C).
- **Классовая адресация.** Концепция наличия у IPv4-адреса трех частей (сети, подсети и хоста), определенных маской *и классом A, B или C*.

ВНИМАНИЕ!

Контекст сертификации CCNA включает два других раздела, которые (к сожалению) также носят название *бесклассовый* и *классовый*. Кроме бесклассовой и классовой адресации, описанной здесь, существуют термины *бесклассовая маршрутизация* (classless routing) и *классовая маршрутизация* (classful routing), относящиеся к некоторым подробностям перенаправления маршрутизаторами Cisco пакетов с использованием стандартного маршрута. Кроме того, каждый протокол маршрутизации может быть отнесен к *бесклассовым протоколам маршрутизации* (classless routing protocol) или к *классовым протоколам маршрутизации* (classful routing protocol). В результате эти термины можно легко перепутать и неправильно использовать. Поэтому, когда видите слова, *бесклассовые* и *классовые*, обратите внимание на контекст их использования: адресация, маршрутизация или протоколы маршрутизации.

Выводы на основании формата IPv4-адреса

Зная, как разделить адрес, используя бесклассовые и классовые правила адресации, с помощью нескольких простых математических формул можно легко установить некоторые важные факты.

Сначала, зная количество битов хоста, для любой подсети можно вычислить количество IP-адресов хоста в подсети. Затем, если известно количество битов подсети (используется концепция классовой адресации) и известно, что все подсети сети используют только одну маску, можно также вычислить количество подсетей в сети. Формулы требуют знания степеней числа 2.

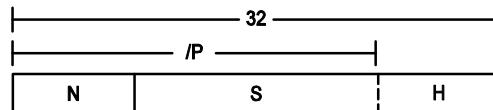
- **Хостов в подсети.** $2^H - 2$, где H — количество битов хоста.
- **Подсетей в сети.** 2^S , где S — количество битов подсети. Используйте эту формулу, только если во всей сети применяется одна маска.

ВНИМАНИЕ!

В главе 12 приведено много подробностей о концепциях, связанных с масками, включая комментарии об одной маске для всей сети класса А, В или С.

Размеры частей IPv4-адресов также могут быть вычислены. Математика проста, но важны концепции. Имея в виду, что IPv4-адреса имеют длину 32 бита, обе части в бесклассовой адресации должны составить в целом 32 ($P + H = 32$), и в классовой адресации эти три части должны составить в целом 32 ($N + S + H = 32$). Эти отношения представлены на рис. 15.6.

При ответе на вопросы экзаменов CCENT и CCNA, а также при исследовании проблем в реальных сетях зачастую начинают с IP-адреса и маски. На основании информации этой главы и предыдущих глав вполне можно найти всю информацию на рис. 15.6, а затем вычислить количество хостов на подсеть и количество подсетей в сети. Для справки этот процесс изложен поэтапно.



Класс:
A: $N = 8$
B: $N = 16$
C: $N = 24$

Рис. 15.6. Отношения между /P, N, S и H



Формальные этапы анализа и вычисления значений, обсуждаемых в данной главе

- Этап 1** Преобразуйте маску в префиксный формат (/P), если нужно. (См. подробней в главе 14.)
- Этап 2** На основании класса определите N. (См. подробней в главе 13.)
- Этап 3** Вычислите $S = P - N$.
- Этап 4** Вычислите $H = 32 - P$.
- Этап 5** Вычислите количество хостов на подсеть: $2^H - 2$.
- Этап 6** Вычислите количество подсетей: 2^S .

Рассмотрим, например, случай IP-адреса 8.1.4.5 с маской 255.255.0.0. Результат приведен ниже.

- Этап 1** $255.255.0.0 = /16$, таким образом $P=16$.
- Этап 2** 8.1.4.5 находится в диапазоне 1–126 первого октета, таким образом, это класс А, значит, $N=8$.
- Этап 3** $S = P - N = 16 - 8 = 8$.
- Этап 4** $H = 32 - P = 32 - 16 = 16$.
- Этап 5** $2^{16} - 2 = 65\,534$ хоста на подсеть.
- Этап 6** $2^8 = 256$ подсетей.

Для другого примера рассмотрим адрес 200.1.1.1 и маску 255.255.255.252. Результат приведен ниже.

- Этап 1** $255.255.255.252 = /30$, таким образом, $P=30$.
- Этап 2** 200.1.1.1 находится в диапазоне 192–223 первого октета, таким образом, это класс С, значит, $N=24$.
- Этап 3** $S = P - N = 30 - 24 = 6$.
- Этап 4** $H = 32 - P = 32 - 30 = 2$.
- Этап 5** $2^2 - 2 = 2$ хоста на подсеть.
- Этап 6** $2^6 = 64$ подсети.

Этот пример использует популярную маску для последовательных каналов, поскольку последовательные каналы требуют только два адреса хоста и маску, поддерживающую только два адреса хоста.

Практические задания по анализу масок подсети

Прежде чем перейти к следующей главе, попрактикуйтесь в процессах, обсуждаемых в данной главе, пока не станете получать правильные ответы почти всегда. Используйте любые средства по своему усмотрению и любое время. Затем можно продолжить чтение.

Перед сдачей экзамена потренируйтесь, чтобы овладеть темой данной главы полностью и отвечать достаточно быстро. Что касается времени, ответ (размер трех час-

тей плюс формулы для вычисления количества подсетей и хостов) нужно давать приблизительно через 15 секунд. Ключевые концепции и рекомендации такого двухэтапного подхода приведены в табл. 15.2.

Таблица 15.2. Продолжайте читать с учетом целей экзамена по темам данной главы

Период	Перед переходом к следующей главе	Перед сдачей экзамена
Сосредоточиться на ...	теме изучения	Быть быстрым и правильным
Разрешенные средства	Все	Ваш мозг и блокнот
Цель: точность	90% правильных ответов	100% правильных ответов
Цель: скорость	Любая скорость	15 секунд

Практические задания этой главы

На листе бумаги ответьте на следующие вопросы. В каждом случае:

- определите структуру адресов в каждой подсети на основании класса и маски, используя классовые концепции IP-адресации. Другими словами, найдите размер частей сети, подсети и хоста адресов;
- вычислите количество хостов в подсети;
- вычислите количество подсетей в сети с учетом того, что повсюду используется та же маска.

Ответы приведены в разделе “Ответы на приведенные ранее практические задания”.

1. 8.1.4.5, 255.255.254.0
2. 130.4.102.1, 255.255.255.0
3. 199.1.1.100, 255.255.255.0
4. 130.4.102.1, 255.255.252.0
5. 199.1.1.100, 255.255.255.224

Дополнительные практические задания

Для дополнительной практики по анализу масок подсети можно использовать следующее.

- Приложение Е, в котором содержатся дополнительные практические задания. Оно содержит также объяснения по поиску ответа каждого задания.
- Приложение З, которое содержит еще 25 практических заданий, связанных с этой главой. Хотя Приложение Е сосредоточено на темах данной главы, задачи в приложениях Е и З начинаются с IP-адреса и маски. Так, приложение З включает также комментарий и ответы на вопросы по количеству битов сети, подсети и хоста, а также другие темы, связанные с данной главой.
- Создайте собственные задания. Большинство калькуляторов подсети вычисляют количество битов сети, подсети и хоста, когда вводится IP-адрес и маска. Поэтому запишите IP-адрес и маску на бумаге, а затем найдите N, S и H. Затем, чтобы проверить ответ, используйте любой калькулятор подсети. Большинство калькуляторов подсети вычисляют класс и идентификатор сети. (Несколько калькуляторов предложено на веб-странице автора этой книги, указанной во введении).

Подготовка к экзамену

Повторите все ключевые темы

Повторите все ключевые темы данной главы, помеченные пиктограммой “Ключевая тема”. Ключевые темы и соответствующие им страницы перечислены в табл. 15.3.

Таблица 15.3. Ключевые темы главы 15

Элемент	Описание	Страница
Список	Некоторые из функций маски подсети	417
Список	Сравнение IP-адресов в одной подсети	418
Рис. 15.2	Части префикса (подсети) и хоста, разделенные единицами и нулями маски	418
Рис. 15.4	Применение концепции класса для создания трех частей адреса	419
Список	Определения классовой и бесклассовой адресации	420
Список	Формальные этапы анализа и вычисления значений, обсуждаемых в данной главе	421

Ключевые термины

Дайте определения перечисленных ниже терминов и проверьте правильность их написания в списке терминов:

классовая адресация (classful addressing), бесклассовая адресация (classless addressing)

Практика

Если это еще не сделано, попрактикуйтесь в вопросах анализа маски подсети, описанных в данной главе. Рекомендации приведены в разделе “Практические задания по анализу масок подсети”.

Ответы на приведенные ранее практические задания

В разделе “Практические задания этой главы” приведено несколько практических задач. Ответы, приведенные в табл. 15.4.

Таблица 15.4. Ответы на практические задания этой главы

Задача	/P	Класс	N	S	H	2^S	$2^H - 2$
1	8.1.4.5 255.255.254.0	23	A	8	15	9	32 768
2	130.4.102.1 255.255.255.0	24	B	16	8	8	256
3	199.1.1.100 255.255.255.0	24	C	24	0	8	Нет
4	130.4.102.1 255.255.252.0	22	B	16	6	10	64
5	199.1.1.100 255.255.255.224	27	C	24	3	5	8

Ниже приведено описание заданий.

1. 8.1.4.5, первый октет (8) находится в диапазоне 1–126, следовательно, это адрес класса А с 8 битами сети. Маска 255.255.254.0 преобразуется в /23, следователь-

но, $P - N = 15$ для 15 битов подсети. Н находим при вычитании $/P$ (23) из 32, т.е. 9 битов хоста.

2. 130.4.102.1, первый октет находится в диапазоне 128–191, следовательно, это адрес класса В с $N = 16$ битов. 255.255.255.0 преобразуется в /24, следовательно, количество битов подсети $24 - 16 = 8$. При 24 битах префикса количество битов хоста составляет $32 - 24 = 8$.
3. Третье задание преднамеренно демонстрирует случай, когда маска не создает часть подсети адреса. Первый октет адреса 199.1.1.100 находится между 192 и 223, следовательно, это адрес класса С с 24 битами сети. Префиксная версия маски /24, следовательно, количество битов подсети $24 - 24 = 0$. Количество битов хоста 32 минус длина префикса (24) дает в общей сложности 8 битов хоста. Таким образом, в данном случае используется маска по умолчанию, которая не создает ни битов подсети, ни самих подсетей.
4. Адрес тот же, что и во втором задании, 130.4.102.1, принадлежит сети класса В с $N = 16$ битам. Но это задание использует другую маску, 255.255.252.0, которая преобразуется в /22. Это дает количество битов подсети $22 - 16 = 6$. При 22 битах префикса количество битов хоста составляет $32 - 22 = 10$.
5. Адрес тот же, что и в третьем задании, 199.1.1.100, принадлежит сети класса С с $N = 24$ битам. Но это задание использует другую маску, 255.255.255.224, которая преобразуется в /27. Это дает количество битов подсети $27 - 24 = 3$. При 27 битах префикса количество битов хоста составляет $32 - 27 = 5$.

В этой главе...

- **Выбор маски, удовлетворяющей требованиям.** Обсуждаются концепции выбора маски подсети, удовлетворяющей заданным требованиям.
- **Практические задания по выбору масок подсети.** Содержатся рекомендации по применению на практике математического механизма, связанного с данной главой.

ГЛАВА 16

Разработка маски подсети

В главе 12 дано общее представление о проекте подсети и процессе его реализации. Сначала инженер анализирует потребности в создании подсети, а также количество необходимых хостов на подсеть. На втором основном этапе он выбирает конкретную классовую сеть, а затем единую маску подсети для использования: маску, которая отвечает требованиям, выявленным на первом этапе. Основные этапы приведены на рис. 16.1.

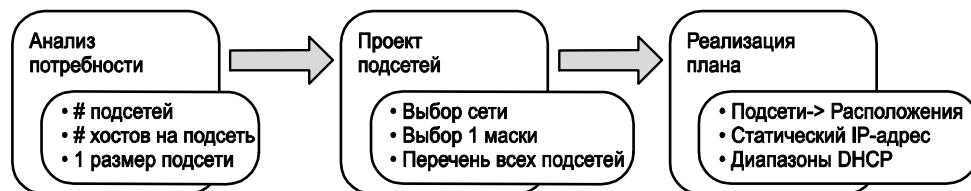


Рис. 16.1. Проект подсети и процесс его реализации из главы 12

В этой главе выбор маски подсети рассматривается подробнее. В частности, описано, как определить минимум необходимых битов подсети и хоста, чтобы удовлетворять требованиям. Сначала исследуются случаи, в которых никакая маска не отвечает требованиям. Затем исследуются случаи, для которых только одна маска отвечает требованиям, и другие случаи, для которых требованиям отвечает несколько масок подсети. И наконец, рассматривается выбор маски в случае, когда существует несколько возможностей.

Контрольные вопросы: знаете ли вы уже темы главы

Этот раздел предназначен для того, чтобы читатель мог предварительно оценить свои знания и решить, нужно ли ему читать главу целиком. Если ответы на девять из десяти вопросов даны правильно, можно сразу же перейти к последнему разделу “Подготовка к экзамену”. Основные темы этой главы и предварительных контрольных вопросов перечислены в табл. 16.1. Отвечая на контрольные вопросы и используя таблицу, читатель сможет достаточно точно определить свои знания в той или иной области. Ответы на вопросы приведены в приложении А.

Таблица 16.1. Темы контрольных вопросов

Основная тема	Номера вопросов
Выбор маски, удовлетворяющей требованиям	1–7

1. Проект создания подсетей IP компании находится на стадии реализации. На настоящий момент главный инженер решил использовать сеть класса В 172.23.0.0. Проект требует 100 подсетей с наибольшей подсетью, нуждающейся в 500 хостах. Руководство требует, чтобы проект предусматривал 50-процентный рост количества подсетей и размера наибольшей подсети. Требуется также использовать единую маску по всей сети класса В. Сколько масок отвечает этим требованиям?
 - а) 0
 - б) 1
 - в) 2
 - г) 3+
2. Проект создания подсетей IP компании находится на стадии реализации. На настоящий момент главный инженер решил использовать сеть класса С 192.168.8.0. Проект требует 12 подсетей с наибольшей подсетью, нуждающейся в 8 хостах. Требуется также использовать единую маску по всей сети класса С. Сколько масок отвечает этим требованиям?
 - а) 0
 - б) 1
 - в) 2
 - г) 3+
3. Проект подсетей IP требует 200 подсетей, 120 хостов на подсеть в наибольшей подсети и использования единой маски в одной частной сети IP. Проект требует также запланировать 20-процентный рост количества подсетей и хостов в наибольшей подсети. Какие из следующих ответов определяют частную сеть IP и маску, отвечающую этим требованиям?
 - а) 10.0.0.0/25
 - б) 10.0.0.0/22
 - в) 172.16.0.0/23
 - г) 192.168.7.0/24
4. Проект подсети использует сеть класса А 10.0.0.0. Инженер должен выбрать единственную маску для всей сети. Проект требует 1200 подсетей с наибольшей подсетью в 300 хостов. Какая из следующих масок отвечает требованиям и резервирует дополнительное количество хостов на подсеть?
 - а) /16
 - б) /19
 - в) /21
 - г) /23

5. Инженер планирует использовать сеть класса В 172.19.0.0 и единую маску подсети по всей сети. В ответах перечислены маски, которые рассматривает инженер. Выберите из них маску, которая обеспечит наибольшее количество хостов на подсеть при достаточном количестве битов для поддержки 1000 подсетей.
- а) 255.255.255.0
 - б) /26
 - в) 255.255.252.0
 - г) /28
6. Инженер планирует использовать сеть класса С 192.168.2.0 и единую маску подсети по всей сети. В ответах перечислены маски, которые рассматривает инженер. Выберите из них маску, которая обеспечит наибольшее количество хостов на подсеть при количестве битов подсети, достаточном для поддержки десяти подсетей.
- а) 255.255.255.0
 - б) /25
 - в) 255.255.255.192
 - г) /27
 - д) 255.255.255.248
7. Проект подсети использует сеть класса А 10.0.0.0, и инженер должен выбрать единую маску для всей сети. Проект требует 1000 подсетей с наибольшей подсетью в 200 хостов. Какая из следующих масок отвечает требованиям при максимальном количестве подсетей?
- а) /18
 - б) /20
 - в) /22
 - г) /24

Основные темы

Выбор маски, удовлетворяющей требованиям

В данной главе рассматривается поиск всех масок, которые отвечают заданным требованиям по количеству подсетей и хостов на подсеть. В главе подразумевается, что инженер уже определил эти требования и выбрал номер сети, которая будет разделена на подсети. Инженер также решил использовать одно значение маски во всей классовой сети.

Вооружившись информацией, изложенной в этой главе, можно отвечать на такие вопросы, как следующий, который имеет значение как для реальных технических задач, так и для экзаменов Cisco.

Вы используете сеть класса B 172.16.0.0. Необходимо 200 подсетей и 200 хостов на подсеть. Какие из следующих масок подсети отвечают требованиям? (Затем следует несколько возможных ответов с различными масками подсети.)

В начале текущего раздела приведен обзор концепций главы 12. В этом разделе представлены основные концепции того, как инженер при разработке соглашений подсети должен выбрать маску на основании требований.

Здесь, после общих концепций, связанных с темами главы 12, они рассматриваются глубже. В частности, рассматриваются три общих случая.

- Ни одна маска не отвечают требованиям.
- Одна и только одна маска отвечает требованиям.
- Требованиям отвечает несколько масок.

Для последнего случая рассматривается, как определить все маски, которые отвечают требованиям, и как выбрать из них наиболее подходящую.

Обзор: выбор минимального количества битов подсети и хоста

Сетевой инженер должен исследовать требования к количеству подсетей и хостов на подсеть, а затем выбрать маску. Как обсуждалось подробно в главе 15, классовое представление IP-адресов определяет структуру IP-адреса из трех частей: сети, подсети и хоста. Сетевой инженер должен выбрать маску так, чтобы количество битов подсети и хоста (S и H соответственно на рис. 16.2) отвечало требованиям.

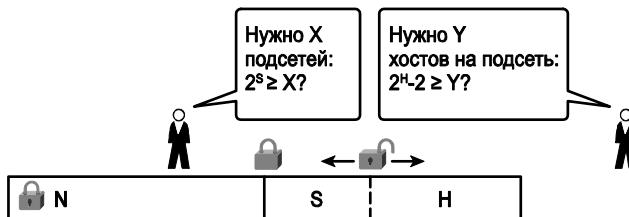


Рис. 16.2. Выбор количества битов подсети и хоста

В основном инженер должен выбрать биты подсети S так, чтобы количество подсетей, которое может быть уникально пронумеровано S битами (2^s), по крайней мере

соответствовало количеству необходимых подсетей. Инженер применяет подобную логику к количеству битов хоста H , которое можно вычислить по формуле $2^H - 2$, поскольку два адреса в каждой подсети зарезервировано. Для удобства в табл. 16.2 приведены степени числа 2, она также будет полезна при решении этих задач.

Таблица 16.2. Степени числа 2. Справочник для разработки маски

Количество бит	2^x
1	2
2	4
3	8
4	16
5	32
6	64
7	128
8	256
9	512
10	1024
11	2048
12	4096
13	8192
14	16 384
15	32 768
16	65 536

Более формально процесс подразумевает определение минимальных значений S и H , которые отвечают требованиям. Ниже приведены начальные этапы выбора маски.

- Этап 1** Определить количество битов сети (N) на основании ее класса.
- Этап 2** Определить наименьшее значение S по формуле $2^S \Rightarrow X$, где X — необходимое количество подсетей.
- Этап 3** Определить наименьшее значение H по формуле $2^H - 2 \Rightarrow Y$, где Y — необходимое количество хостов на подсеть.

В следующих трех разделах исследуются эти начальные этапы выбора маски подсети.

Ни одна маска не отвечает требованиям

После определения необходимого количества битов подсети и хоста может оказаться, что они не вписываются в 32-разрядную маску подсети IPv4. Помните: маска всегда содержит в общей сложности 32 бита с двоичными единицами в части сети и подсети, а также двоичными нулями в части хоста. Условия экзаменационного вопроса могут содержать такие требования, для удовлетворения которых 32 битов не хватит.

Рассмотрим, например, следующий типичный экзаменационный вопрос.

Сетевой инженер создает проект подсети. Он планирует использовать сеть класса В 172.16.0.0. Есть потребность в 300 подсетях и 280 хостах на подсеть. Какую из следующих масок он мог бы выбрать?

Трехэтапный процесс, приведенный в предыдущем разделе, свидетельствует о том, что для удовлетворения этим требованиям понадобится в общей сложности 34 бита, поэтому не подойдет никакая маска. Поскольку используется сеть класса В, в адресе будет 16 битов сети и 16 битов хоста, — этого достаточно, чтобы создать части подсети и оставить биты хоста для каждой подсети. Количество битов подсети $S=8$ недостаточно, поскольку $2^8 = 256 < 300$, а $S=9$ достаточно, поскольку $2^9 = 512 \Rightarrow 300$. Аналогично, поскольку $2^8 - 2 = 254 < 280$, 8 битов хоста недостаточно, а 9 битов хоста ($2^9 - 2 = 510 \Rightarrow 280$) — вполне.

Эти требования не оставляют достаточно места для количества всех хостов и подсетей, так как части сети, подсети и хоста составляют в целом больше 32 битов.

- N=16. Поскольку сеть класса В, существует 16 битов сети.
- S=9 как минимум, поскольку 8 битов недостаточно для 300 подсетей ($2^8 = 256 < 300$), а 9 битов вполне достаточно $2^9 = 512$.
- H=9 как минимум, поскольку 8 битов недостаточно для 280 хостов на подсеть ($2^8 - 2 = 254 < 280$), но битов 9 вполне достаточно $2^9 - 2 = 510$.

На рис. 16.3 представлен полученный формат IP-адресов в этой подсести, после того, как инженер расписал 9 битов подсети на бумаге. Остается только 7 битов хоста, но инженер нуждается в 9.

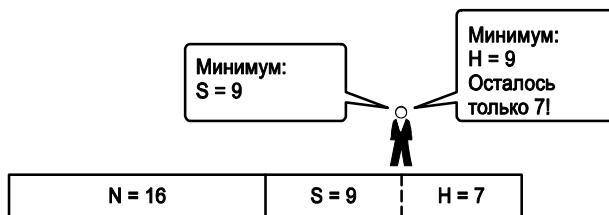


Рис. 16.3. Слишком мало битов для части хоста при данных требованиях

Требованиям отвечает только одна маска

Процесс, обсуждаемый в этой главе, частично сосредоточивается на поиске наименьшего количества битов подсети и хоста, удовлетворяющих требованиям. Если инженер попытается использовать эти минимальные значения и совместно биты частей сети, подсети и хоста составят в целом точно 32 бита, то требованиям отвечает только одна маска.

Рассмотрим, например, переделанную версию примера из предыдущего раздела с меньшими количествами подсетей и хостов следующим образом.

Сетевой инженер создает проект подсети. Он планирует использовать сеть класса В 172.16.0.0. Есть потребность в 200 подсетях и 180 хостах на подсеть. Какую из следующих масок он мог бы выбрать?

Трехэтапный процесс определения минимального количества битов сети и хоста приводит к потребности в 16, 8 и 8 битах соответственно. Как и прежде, в сети класса В 16 битов сети. При потребности только в 200 хостах $S=8$ достаточно, поскольку

$2^8 = 256 \Rightarrow 200$; 7 битов подсети не достаточно для 200 подсетей ($2^7 = 128$). Аналогично, поскольку $2^8 - 2 = 254 \Rightarrow 180$, 8 битов хоста отвечают требованиям; 7 битов хоста (для 126 хостов на подсеть) было бы недостаточно.

На рис. 16.4 приведен полученный формат IP-адресов в этой подсете.

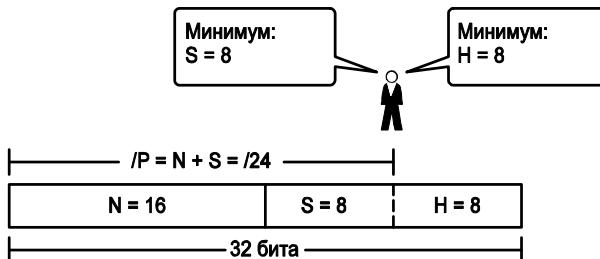


Рис. 16.4. Одна маска, отвечающая требованиям

На рис. 16.4 маска представлена концептуально. Для поиска фактического значения маски запишите ее в префиксном формате (/P), где $P = N+S$ или, в данном случае, /24.

Требованиям отвечает несколько масок

В зависимости от требований к количеству подсетей и хостов на подсеть, а также выбранной сети, требованиям могут отвечать несколько масок. В этих случаях необходимо найти все применимые маски. Затем появляется выбор, но что следует учитывать при выборе одной маски среди всех, которые отвечают требованиям? Этот раздел демонстрирует поиск всех масок, а также фактов, учитываемых при выборе одной маски из списка.

Поиск всех масок: концепции

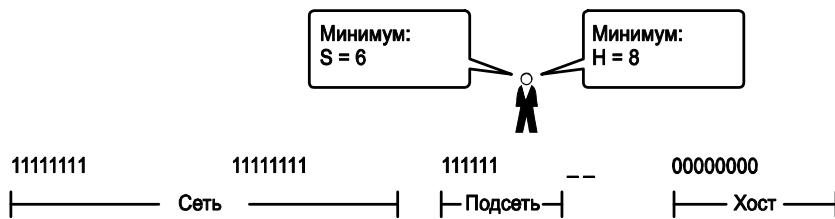
Чтобы лучше разъяснить, как осуществляется поиск всех масок подсети в двоичном формате, в этом разделе описаны два главных этапа. На первом из них 32-разрядная двоичная маска подсети создается на бумаге. Записываются двоичные единицы для битов сети, двоичные единицы для битов подсети и двоичные нули для битов хоста, как всегда. Однако для S и H следует использовать минимальные значения. Когда все биты будут записаны, их может оказаться меньше 32!

Рассмотрим, например, следующую задачу, подобную приведенной ранее, но с некоторыми изменениями в требованиях.

Сетевой инженер создает проект подсети. Он планирует использовать сеть класса В 172.16.0.0. Есть потребность в 50 подсетях и 180 хостах на подсеть. Какую из следующих масок он мог бы выбрать?

Этот пример подобен прежнему, за исключением того, что в данном случае необходимо только 50 подсетей. Инженер снова использует частную сеть IP 172.16.0.0 с 16 битами сети. Проект в данном случае требует только 6 битов подсети, поскольку $2^6 = 64 \Rightarrow 50$, а также минимум 8 битов хоста.

Один из способов рассмотрения концепции поиска всех масок, которые отвечают этим требованиям, заключается в записи битов маски подсети: двоичные единицы для частей сети и подсети, а также двоичных нулей для части хоста. Однако считайте 32-разрядную маску 32-мя разрядными позициями, а двоичные нули пишите только с правого края. Общее представление приведено на рис. 16.5.

Рис. 16.5. Неполная маска $N=16$, $S=6$ и $H=8$

На рис. 16.5 приведено 30 битов, но у маски должно быть 32 бита. Два оставшихся бита могли бы стать битами подсети, будучи установленными в двоичные единицы. Эти же два бита могли бы быть битами хоста, будучи установленными в двоичные нули. Инженер просто должен решить, хочет ли он иметь больше битов подсети и больше подсетей или больше битов хоста для большего количества хостов на подсеть.

Но инженер не может выбрать любые значения для этих двух битов. Маска должна все еще выполнять следующее правило.

Ключевая тема Факты о двоичных значениях в масках подсети

Маска подсети начинается со всех двоичных единиц и сопровождается всеми двоичными нулями без их чередования.

В примере с двумя не заполненными битами, представленном на рис. 16.5, одно значение (двоичное 01) нарушит это правило, а три другие комбинации двух битов (00, 10 и 11) — нет. В результате в этом примере требованиям отвечают три маски, как показано на рис. 16.6.

			S = 6	H = 8	
	11111111	11111111	111111	__	00000000
/22	11111111	11111111	11111100	__	00000000
/23	11111111	11111111	11111110	__	00000000
/24	11111111	11111111	11111111	__	00000000
			S=6	H=10	
			S=7	H=9	
			S=8	H=8	

Легенда: минимальное значение

Рис. 16.6. Три маски, отвечающие требованиям

В трех масках первая имеет наименьшее количество битов подсети, а потому — больше битов хоста. Так, первая маска максимизирует количество хостов на подсеть. Последняя маска использует минимальное значение для количества битов хоста, позволяя использовать больше битов для подсети, продолжая все еще удовлетворять требования. В результате последняя маска максимизирует количество возможных подсетей.

Поиск всех масок: математика

Хотя концепции, связанные с примером, представленным на рис. 16.5 и 16.6, важны, диапазон отвечающих требованиям масок можно найти существенно легче, используя только простую математику. Как только стало известно значение N и минимальные значения S и H , процесс поиска маски требует лишь нескольких этапов. Поиск значения $/P$ при наименьших количествах битов подсети и хоста происходит следующим образом.

Более краткий процесс поиска всех префиксных масок, которые отвечают определенным требованиям



Этап 1 Вычислите самую короткую префиксную маску ($/P$) на основании *минимального значения S*, где $P = N + S$.

Этап 2 Вычислите самую длинную префиксную маску ($/P$) на основании *минимального значения H*, где $P = 32 - H$.

Этап 3 Диапазон допустимых масок включает все значения $/P$ между двумя значениями, вычисленными на предыдущих этапах.

В примере, представленном на рис. 16.6, $N = 16$, минимум $S = 6$ и минимум $H=8$. На первом этапе выявляют самую короткую префиксную маску ($/P$ с наименьшим значением) $/22$, при сложении N и S ($16 + 6 = 22$). Второй этап выявляет самую длинную отвечающую требованиям префиксную маску при вычитании наименьшего возможного значения для H (в данном случае 8) из числа 32. В результате получится маска $/24$. Третий этап напоминает, что диапазон от $/22$ до $/24$ включает $/23$, что также является возможным выбором.

Выбор лучшей маски

Если установленным требованиям отвечает несколько возможных масок, у инженера есть выбор. При этом, конечно, возникает вопрос: какую маску выбрать? Почему одна маска может быть лучше другой? Причины в итоге можно свести к трем основным пунктам.

Причины выбора одной маски подсети, а не другой



- **Максимизировать количество хостов в подсети.** Чтобы сделать этот выбор, используйте самую короткую префиксную маску (т.е. маску с наименьшим значением $/P$), поскольку у нее наибольшая часть хоста.
- **Максимизировать количество подсетей.** Чтобы сделать этот выбор, используйте самую длинную префиксную маску (т.е. маску с наибольшим значением $/P$), поскольку у нее наибольшая часть подсетей.
- **Увеличить количество и подсетей, и хостов.** Чтобы сделать этот выбор, используйте маску в середине диапазона, это позволит предоставить больше битов и подсети, и хоста.

Например, на рис. 16.6 приведен диапазон масок $/22-24$, отвечающих требованиям. У самой короткой маски, $/22$, наименьшее количество битов подсети и наибольшее количество битов хоста (10) из трех вариантов. Это максимизирует количество хостов в подсети. Самая длинная маска, $/24$, максимизирует количество битов

подсети (8), увеличивая количество подсетей, по крайней мере в рамках соответствия исходным требованиям. Маска в середине, /23, предусматривает некий рост количества и подсетей, и хостов в подсети.

Формальный процесс

До сих пор в этой главе объяснялись различные этапы поиска масок подсети, удовлетворяющих требованиям проекта. Теперь они объединяются в общий список всего процесса, приведенный ниже. Обратите внимание на то, что в списке нет никаких новых концепций, которые не обсуждались бы ранее.



Полный процесс поиска и выбора масок, удовлетворяющих определенным требованиям

- Этап 1** Найдите количество битов сети (N) согласно правилам класса.
- Этап 2** Вычислите минимальное количество битов подсети (S), чтобы 2^S было больше или равно количеству необходимых подсетей.
- Этап 3** Вычислите минимальное количество битов хоста (H), чтобы $2^H - 2$ было больше или равно количеству необходимых хостов в подсети.
- Этап 4** Если $N+S+H > 32$, то ни одна маска не удовлетворяет требованиям.
- Этап 5** Если $N+S+H = 32$, то требованиям удовлетворяет только одна маска. Вычислите маску как $/P$, где $P = N+S$.
- Этап 6** Если $N+S+H < 32$, то требованиям удовлетворяет несколько масок.
 - а) Вычислите маску $(/P)$ на основании минимального значения S , где $P = N+S$. Эта маска максимизирует количество хостов в подсети.
 - б) Вычислите маску $(/P)$ на основании минимального значения H , где $P = 32 - H$. Эта маска максимизирует количество возможных подсетей.
 - в) Получите полный диапазон масок, включив все префиксные длины между двумя значениями, вычисленными на этапах а) и б).

Практические задания по выбору масок подсети

Прежде чем перейти к следующей главе, попрактикуйтесь в процессах, обсуждаемых в данной главе, пока не станете почти всегда получать правильные ответы. Используйте любые средства по своему усмотрению и любое время. Затем можно продолжить чтение.

Перед сдачей экзамена потренируйтесь, чтобы овладеть темой данной главы полностью и отвечать достаточно быстро. Что касается времени, ответ (все маски, отвечающие требованиям, которые максимизируют количество подсетей или хостов) нужно давать приблизительно через 15 секунд. Ключевые концепции и рекомендации такого двухэтапного подхода приведены в табл. 16.3.

Таблица 16.3. Продолжайте читать с учетом целей экзамена по темам данной главы

Период	Перед переходом к следующей главе	Перед сдачей экзамена
Сосредоточиться на ...	теме изучения	Быть быстрым и правильным
Разрешенные средства	Все	Ваш мозг и блокнот
Цель: точность	90% правильных ответов	100% правильных ответов
Цель: скорость	Любая скорость	15 секунд

Практические задания этой главы

Ниже приведены три отдельных задания с адресом классовой сети, а также необходимым количеством подсетей и хостов на подсеть. Для каждого задания определите минимальное количество битов подсети и хоста, которые отвечают требованиям. Если возможно несколько масок, обратите внимание на то, какая маска максимизирует количество хостов в подсетеи, а какая количество подсетей. Если требованиям отвечает только одна маска, укажите ее. Приведите маски в префиксном формате.

- Сети 10.0.0.0 требуется 1500 подсетей и 300 хостов на подсеть.
- Сети 172.25.0.0 требуется 130 подсетей и 127 хостов на подсеть.
- Сети 192.168.83.0 требуется 8 подсетей и 8 хостов на подсеть.

Ответы приведены в табл. 16.5.

Дополнительные практические задания

Ниже перечислены некоторые возможности для дополнительной практики.

- Приложение Ж, содержащее дополнительные практические задания. Оно содержит также объяснения по поиску ответа к каждому заданию.
- Создайте собственные задания. Большинство калькуляторов подсети позволяют ввести класс А, В или С сети и выбрать маску, затем калькулятор перечислит количество подсетей и хостов в подсетеи, созданных этой сетью и маской. Выберите номер сети и необходимые количества подсетей и хостов, получите ответы и проверьте результат с калькулятором.

Подготовка к экзамену

Повторите все ключевые темы

Повторите все ключевые темы данной главы, помеченные пиктограммой “Ключевая тема”. Ключевые темы и соответствующие им страницы перечислены в табл. 16.4.

Таблица 16.4. Ключевые темы главы 16

Элемент	Описание	Страница
Определение	Факты о двоичных значениях в масках подсети	434
Список	Более краткий процесс поиска всех префиксных масок, которые отвечают определенным требованиям	435
Список	Причины выбора одной маски подсети, а не другой	435
Список	Полный процесс поиска и выбора масок, удовлетворяющих определенным требованиям	436

Ключевые термины

В этой главе нет новых терминов.

Практика

Если это еще не сделано, попрактикуйтесь в вопросах поиска всех масок подсети на основании требований, описанных в данной главе. Рекомендации приведены в разделе “Практические задания по выбору масок подсети”.

Ответы на приведенные ранее практические задания

В разделе “Практические задания этой главы” приведены три практических задания. Ответы, приведены в табл. 16.5. После таблицы следуют примечания к каждому заданию.

Таблица 16.5. Практическое задание: поиск масок, которые отвечают требованиям

Задание	Класс	Минимум битов подсети	Минимум битов хоста	Префиксный диапазон	Префикс для максимизации подсетей	Префикс для максимизации хостов
1	A	11	9	/19 – /23	/23	/19
2	B	8	8	/16	Нет	Нет
3	C	3	4	/27 – /28	/28	/27

1. N=8, поскольку в задаче упоминается сеть класса А 10.0.0.0. С потребностью в 1500 подсетях 10 битов подсети обеспечивают только 1024 подсети (согласно табл. 16.2), а 11 битов подсети (S) предусмотрели бы 2048 подсетей, что больше необходимых 1500. Аналогично наименьшим количеством битов хоста будет 9, поскольку $2^8 - 2 = 254$, а проект требует 300 хостов на подсеть. Самая короткая префиксная маска была бы /19, вычисляемая при добавлении N (8) к наименьшему допустимому для использования количеству битов подсети S (11). Анало-

гично с минимальным значением Н (9) самая длинная префиксная маска максимизирует количество подсетей, $32 - H = /23$.

2. N=16, поскольку в задаче упоминается сеть класса В 172.25.0.0. С потребностью в 130 подсетях 7 битов подсети обеспечивают только 128 подсетей (согласно табл. 16.2), а 8 битов подсети (S) предусмотрели бы 256 подсетей, что больше необходимых 130. Аналогично наименьшим количеством битов хоста будет 8, поскольку $2^7 - 2 = 126$ близко к необходимым 127, но не совсем достаточно, что делает Н = 8 наименьшим количеством битов хоста, которое отвечает требованиям. Обратите внимание: в сумме количество битов сети, минимальное количество битов подсети и хоста составит 32, таким образом, только одна маска отвечает требованиям, а именно /24, вычисляемая при суммировании количества битов сети (16) и подсети (8).
3. N=24, поскольку в задаче упоминается сеть класса С 192.168.83.0. С потребностью в 8 подсетях 3 бита подсети обеспечивают их недостаточно. Наименьшее количество битов хоста будет 4, поскольку $2^3 - 2 = 6$, а проект требует 8 хостов на подсеть. Самая короткая префиксная маска была бы /27, она вычисляется при добавлении N (24) к наименьшему пригодному для использования количеству битов подсети S (3). Аналогично при минимальном значении Н (4) самая длинная префиксная маска максимизирует количество подсетей, $32 - H = /28$.

В этой главе...

- **Определение подсети.** Обсуждается концепция подсети и ключевых чисел, которые определяют подсеть: идентификатор подсети, широковещательный адрес подсети, а также диапазон пригодных для использования IP-адресов в подсети.
- **Анализ существующих подсетей: двоичный.** Исследуются ключевые числа, которые определяют подсеть при анализе двоичных значений.
- **Анализ существующих подсетей: десятичный.** Исследуются ключевые числа, которые определяют подсеть при анализе десятичных значений.
- **Практические задания по анализу существующих подсетей.** Приведены советы и рекомендации, а также указано, где найти больше задач по темам этой главы.

ГЛАВА 17

Анализ существующих подсетей

Большинство сетевых работ требует действий с оперативной точки зрения, начиная процесс с существующих IP-адресов, масок и подсетей. Нередко задача начинается с поиска IP-адреса и маски, используемой неким хостом. Затем, чтобы понять, как объединенная сеть направляет пакеты на этот хост, следует найти основные элементы информации о подсети, а именно:

- идентификатор подсети;
- широковещательный адрес подсети;
- диапазон пригодных для использования одноадресатных IP-адресов подсети.

В этой главе обсуждаются концепции и математический механизм, позволяющие взять известный IP-адрес и маску, а затем полностью описать подсеть, находя значения из этого списка. Такие задачи, вероятно, обеспечат наиболее важные навыки в области IP-адресации и создания подсетей в данной книге, поскольку они чаще всего встречаются при работе и диагностике реальных сетей.

Контрольные вопросы: знаете ли вы уже темы главы

Этот раздел предназначен для того, чтобы читатель мог предварительно оценить свои знания и решить, нужно ли ему читать главу целиком. Если ответы на девять из десяти вопросов даны правильно, можно сразу же перейти к последнему разделу “Подготовка к экзамену”. Основные темы этой главы и предварительных контрольных вопросов перечислены в табл. 17.1. Отвечая на контрольные вопросы и используя таблицу, читатель сможет достаточно точно определить свои знания в той или иной области. Ответы на вопросы приведены в приложении А.

Таблица 17.1. Темы контрольных вопросов

Основная тема	Номера вопросов
Определение подсети	1
Анализ существующих подсетей: двоичный	2
Анализ существующих подсетей: десятичный	3–7

1. С точки зрения правил классовой адресации у IP-адреса может быть три части: сети, подсети и хоста. Если исследовать все адреса в одной подсети в двоичном формате, какое из следующих утверждений правильно описывает совпадение частей всех адресов? Выберите лучший ответ.

- а) Только части сети.
 - б) Только части подсети.
 - в) Только части хоста.
 - г) Части сети и подсети.
 - д) Части подсети и хоста.
2. Какое из следующих утверждений истинно исходя из двоичных значений идентификатора подсети, широковещательного адреса подсети и IP-адреса хоста в какой-нибудь одной подсети? (Выберите несколько ответов.)
- а) Вся часть хоста широковещательного адреса состоит из двоичных нулей.
 - б) Вся часть хоста идентификатора подсети состоит из двоичных нулей.
 - в) Вся часть хоста пригодного для использования IP-адреса может состоять из двоичных единиц.
 - г) Часть хоста любого пригодного для использования IP-адреса не должна состоять исключительно из двоичных нулей.
3. Что из следующего является резидентским идентификатором подсети для IP-адреса 10.7.99.133/24?
- а) 10.0.0.0
 - б) 10.7.0.0
 - в) 10.7.99.0
 - г) 10.7.99.128
4. Что из следующего является резидентской подсетью для IP-адреса 192.168.44.97/30?
- а) 192.168.44.0
 - б) 192.168.44.64
 - в) 192.168.44.96
 - г) 192.168.44.128
5. Что из следующего является широковещательным адресом подсети, в которой располагается IP-адрес 172.31.77.201/27?
- а) 172.31.201.255
 - б) 172.31.255.255
 - в) 172.31.77.223
 - г) 172.31.77.207
6. Некий инженер просит вас настроить сервер DHCP так, чтобы зарезервировать 100 последних пригодных для использования IP-адресов в подсети 10.1.4.0/23. Какой из следующих IP-адресов мог бы оказаться зарезервированным в результате новой конфигурации?
- а) 10.1.4.156
 - б) 10.1.4.254
 - в) 10.1.5.200

- г) 10.1.7.200
- д) 10.1.255.200

7. Некий инженер просит вас настроить сервер DHCP так, чтобы зарезервировать 20 первых пригодных для использования IP-адресов в подсети 192.168.9.96/27. Какой из следующих IP-адресов мог бы оказаться зарезервированным в результате новой конфигурации?

- а) 192.168.9.126
- б) 192.168.9.110
- в) 192.168.9.1
- г) 192.168.9.119

Основные темы

Определение подсети

Подсеть IP — это подмножество классовой сети, созданное по выбору сетевого инженера. Но этот инженер не может выбрать произвольное подмножество адресов; он должен следовать определенным правилам, которые приведены ниже.

- Подсеть содержит набор последовательных чисел.
- Подсеть содержит 2^H номеров, где H — количество битов хоста, определенных маской подсети.
- Два специальных номера в диапазоне не могут использоваться как IP-адреса.
 - Первый номер (самый младший) — это *идентификатор подсети* (subnet ID).
 - Последний номер (самый верхний) — это *широковещательный адрес подсети* (subnet broadcast address).
- Остальные адреса, значения которых находятся между идентификатором и широковещательным адресом подсети, используются как *одноадресатные IP-адреса* (unicast IP address).

В этом разделе приведен обзор и подробно описаны концепции идентификатора подсети, широковещательного адреса подсети и диапазона адресов подсети.

Пример с сетью 172.16.0.0 и четырьмя подсетями

Предположим, вы работаете в центре поддержки и получаете звонки от пользователей, у которых проблемы с компьютером. Пользователь сообщает свой IP-адрес и маску: 172.16.150.41, 255.255.192.0. Одна из первых и наиболее распространенных задач, которые приходится решать на основании данной информации, — это поиск идентификатора подсети, в которой располагается указанный адрес. (Фактически идентификатор подсети иногда называется резидентской подсетью, поскольку IP-адрес существует или располагается в этой подсети.)

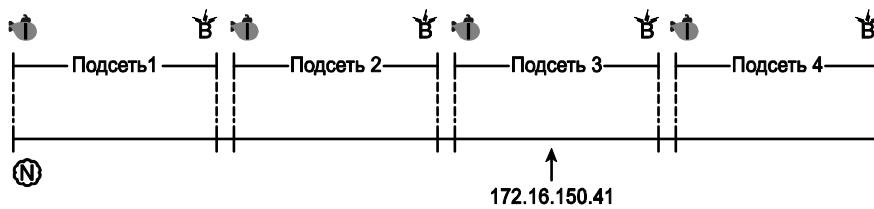
Прежде чем обратиться к математике, исследуйте маску (255.255.192.0) и классовую сеть (172.16.0.0). Из маски, на основании изложенного в главе 15, можно вывести структуру адресов в подсети, включая количество битов подсети и хоста. Такой анализ свидетельствует, что адрес содержит два бита подсети, а значит, возможны четыре (2^2) подсети. (Если эти концепции еще не до конца очевидны, обратитесь к главе 15.). Структура адреса приведена на рис. 17.1.

172.16.150.41, 255.255.192.0 (/18)		
N = 16	S = 2	H = 14
$/P = N + S = /18$		
$\text{Подсети} = 2^S$ $\text{Хосты} = 2^H - 2$		

Рис. 17.1. Структура адреса: сеть класса B, маска /18

До сих пор в этой книге подразумевалось, что в сети класса А, В или С используется единая маска. Продолжим это положение: все подсети здесь имеют одинаковый размер, поскольку у всех подсетей та же структура. Например, адрес на рис. 17.1 имеет структуру с четырьмя подсетями, поэтому все четыре подсети будут иметь по $2^{14} - 2$ адреса хоста.

Далее сосредоточимся на двух концепциях, связанных с этим примером: что в данной сети существуют четыре подсети и у них одинаковый размер. Концептуально, если представить всю сеть класса В как числовую ось с четырьмя подсетями равного размера, каждая подсеть содержит, по существу, четверть сети, и каждая подсеть использует четверть номеров, как показано на рис. 17.2.



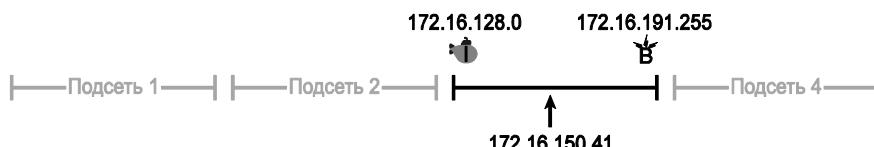
Легенда:

- Идентификатор сети
- Идентификатор подсети
- Широковещательный адрес подсети

Рис. 17.2. Сеть 172.16.0.0, разделенная на четыре равных подсети

На рис. 17.2 приведена также концепция этих четырех подсетей на числовой оси вверху рисунка, а вся сеть класса В 172.16.0.0 — на числовой оси внизу. У каждой подсети есть идентификатор слева (наименьшее число в подсети) и широковещательный адрес подсети справа (наибольшее число в подсети).

Как уже упоминалось, зачастую решение задачи приходится начинать с IP-адреса и маски, а затем находить подсеть, в которой располагается адрес. И снова, используя IP-адрес 172.16.150.41 как пример, на рис. 17.3 показана резидентская подсеть наряду с идентификатором и широковещательным адресом подсети в выделенной подсети.



Легенда:

- Идентификатор подсети
- Широковещательный адрес подсети

Рис. 17.3. Резидентская подсеть для 172.16.150.41, 255.255.192.0

Концепции идентификатора подсети

Идентификатор подсети — это число, используемое для ее краткого представления. Будучи указанным вместе с маской подсети, идентификатор подсети идентифицирует подсеть и применяется при получении широковещательного адреса, а также диапазона адресов подсети. Чтобы не записывать все эти подробности о подсете, достаточно записать идентификатор подсети и маску (их вполне достаточно для полного описания подсети).

Идентификатор подсети присутствует во многих местах, но чаще всего он используется в таблицах маршрутизации. Например, когда инженер задает маршрутизатору IP-адрес и маску, он вычисляет идентификатор подсети и помещает маршрут в свою таблицу маршрутизации для данной подсети. Затем, как правило, маршрутизатор анонсирует комбинацию идентификатор/маска подсети соседним маршрутизаторам с помощью некоторого протокола маршрутизации. В конечном счете все маршрутизаторы предприятия узнают о подсете (снова используя комбинацию идентификатора подсети и маски) и отображают ее в своих таблицах маршрутизации. (Содержимое таблицы маршрутизации маршрутизатора можно отобразить с помощью команды `show ip route`.)

К сожалению, терминология подсетей может иногда вызывать проблемы. Для начала скажем, что термины *идентификатор подсети* (subnet ID), *номер подсети* (subnet number) и *адрес подсети* (subnet address) — синонимы. Кроме того, люди иногда говорят просто *подсеть*, имея в виду и концепцию подсети, и число, которое используется как идентификатор подсети. В разговоре о маршрутизации иногда используют термин *префикс* вместо термина *подсеть*. Термин *префикс* означает ту же идею, что и термин *подсеть*, но только используется в терминологии бесклассовой адресации как способ описания IP-адреса (см. главу 15).

Самый большой беспорядок в терминологии вызывают термины *сеть* (network) и *подсеть* (subnet). В реальном мире люди часто используют эти термины как синонимы, что в некоторых случаях совершенно резонно. В других случаях значения этих терминов специфичны, и различие между ними — вопрос обсуждаемой темы.

Например, зачастую спрашивают: “Каков идентификатор сети?”, когда на самом деле хотят узнать идентификатор подсети. В другом случае речь могла бы идти об идентификаторе сети класса А, В или С. Поэтому когда инженер задает вопрос “Каков идентификатор сети 172.16.150.41/18?”, используйте контекст, чтобы выяснить, нужен ли литерал идентификатора классовой сети (в данном случае 172.16.0.0) или литерал идентификатора подсети (в данном случае 172.16.128.0).

На экзамене следует быть готовым к этому и обращать внимание на контекст, когда используются термины *подсеть* и *сеть*, чтобы выяснить конкретное значение термина в данном случае.

Ключевые факты об идентификаторе подсети наряду с возможными синонимами приведены в табл. 17.2.



Таблица 17.2. Основные факты об идентификаторах подсетей

Определение	Число, представляющее подсеть
Числовое значение	Первое (наименьшее) число в подсети
Литеральные синонимы	Номер подсети, адрес подсети, префикс, резидентская подсеть
Обычное использование синонима	Сеть, идентификатор сети, номер сети, адрес сети
Обычно встречается в...	таблице маршрутизации, документации

Широковещательный адрес подсети

У широковещательного адреса подсети две основные роли: он используется как IP-адрес получателя при передаче пакетов всем хостам в подсети, а также при поиске старшего адреса в диапазоне допустимых адресов подсети.

Первоначально задача широковещательного адреса подсети состояла в том, чтобы предоставить хостам эффективный способ передачи одного пакета всем хостам в подсети. Например, хост в подсети А может послать пакет с адресом получателя, соответствующим широковещательному адресу подсети В. Маршрутизаторы перенаправляют этот пакет точно так же, как пакет, посланный хосту в подсети В. Как только пакет достигнет последнего маршрутизатора, подключенного к подсети В, он перенаправит его всем хостам в подсети В, как правило, инкапсулируя пакет в широковещательный фрейм уровня управления передачей данных. В результате все хосты подсети В получат копию пакета.

Хотя ныне у широковещательного адреса подсети небольшое практическое применение, на экзамене CCENT и CCNA он используется часто, поскольку широковещательный адрес — это последний (самый старший) адрес в диапазоне адресов подсети. Для поиска младшего конца диапазона вычислите идентификатор подсети, а для поиска старшего — широковещательный адрес подсети.

Ключевые факты о широковещательном адресе подсети наряду с возможными синонимами приведены в табл. 17.3.

Таблица 17.3. Основные факты о широковещательных адресах подсетей



Частные сети IP	Класс сети
Определение	Зарезервированный адрес в каждой подсети, используемый как адрес получателя пакета, который заставляет маршрутизатор перенаправить пакет всем хостам в этой подсети
Числовое значение	Последнее (наибольшее) число в подсети
Литеральные синонимы	Направленный широковещательный адрес
Обычное использование синонима	Сетевое широковещание
Обычно встречается в...	вычислениях диапазона адресов подсети

Диапазон пригодных для использования адресов

Инженер, реализующий объединенную сеть IP, должен знать диапазон одноадресатных IP-адресов в каждой подсети. Прежде чем можно будет запланировать, какие адреса использовать как статически назначаемые IP-адреса при настройке сервера DHCP и какие зарезервировать для дальнейшего использования, необходимо знать диапазон пригодных для использования адресов.

Для поиска диапазона пригодных для использования IP-адресов в подсети найдите сначала идентификатор и широковещательный адрес подсети. Затем добавьте 1 к четвертому октету идентификатора подсети, чтобы получить первый (младший) пригодный для использования адрес, и вычтите 1 из четвертого октета широковещательного адреса подсети, чтобы получить последний (старший) пригодный для использования адрес в подсети.

Например, на рис. 17.3 представлены идентификатор подсети 172.16.128.0 и маска /18. Первый пригодный для использования адрес на единицу больше идентифи-

катора подсети (в данном случае 172.16.128.1). На том же рисунке широковещательный адрес подсети — 172.16.191.255, таким образом, последний пригодный для использования адрес на единицу меньше — 172.16.191.254.

Теперь, рассмотрев концепции чисел, которые совместно определяют подсеть, в остальной части этой главы сосредоточимся на математическом механизме, используемом для поиска этих значений.

Анализ существующих подсетей: двоичный

Что означает “проанализировать подсеть”? В данной книге это означает, что исходя из IP-адреса и маски нужно определить ключевые факты о подсети, в которой располагается этот адрес, а именно: выяснить идентификатор подсети, широковещательный адрес подсети и диапазон адресов. Анализ может также включать вычисление количества адресов в подсети, как обсуждалось в главе 15, но в данной главе нет обзора этих концепций.

Есть много методов вычисления подробностей подсети на основании адреса и маски. Данный раздел начинается с обсуждения некоторых вычислений, в которых используется двоичная математика, а следующий раздел демонстрирует альтернативу — использование десятичной математики. Хотя для быстроты на экзаменах большинство людей предпочитают использовать десятичный метод, двоичные вычисления в конечном счете дают лучшее представление об IPv4-адресации. В частности, если планируется получить сертификат Cisco степени выше CCNA, следует уделить время изучению двоичных методов, обсуждаемых в этом разделе, даже если для экзаменов используются десятичные методы.

Поиск идентификатора подсети: двоичный метод

В начале этого раздела, где используется двоичная математика, рассмотрим сначала простую десятичную математическую задачу: найти наименьшее десятичное трехзначное число, которое начинается с 4. Ответ, конечно, 400. Большинству людей, конечно, многоэтапная логика для этого не нужна, все знают, что 0 — самое малое значение, которое можно использовать для любой цифры в десятичном числе. Известно также, что первой цифрой должна быть 4, а количество знаков в числе — три, таким образом, используя самое низкое значение (0) для последних двух цифр, находят ответ: 400.

Эта же концепция применима для двоичных IP-адресов при вычислении идентификатора подсети. Подобные концепции уже были изложены в других главах, поэтому поиск идентификатора подсети в двоичном формате может быть интуитивно понятен! В противном случае следующие ключевые факты помогут понять логику.

- У всех адресов подсети (идентификатор подсети, широковещательный адрес подсети и все пригодные для использования IP-адреса) одинаковое значение в префиксной части.
- Идентификатор подсети — самое низкое числовое значение в подсети, поэтому его часть хоста заполнена двоичными нулями.

Для поиска идентификатора подсети в двоичном формате возьмите IP-адрес в двоичном виде и замените все биты хоста на двоичные нули. Для этого необходимо преобразовать IP-адрес в двоичный формат. Необходимо также выявить биты префикса и хоста, которые можно легко получить, преобразовав маску (по мере необхо-

димости) в префиксный формат. (В приложении Б содержится таблица десятично-двоичных преобразований.) На рис. 17.4 приведена концепция с использованием тех же адреса и маски, что и в прежних примерах этой главы: 172.16.150.41, маска /18.

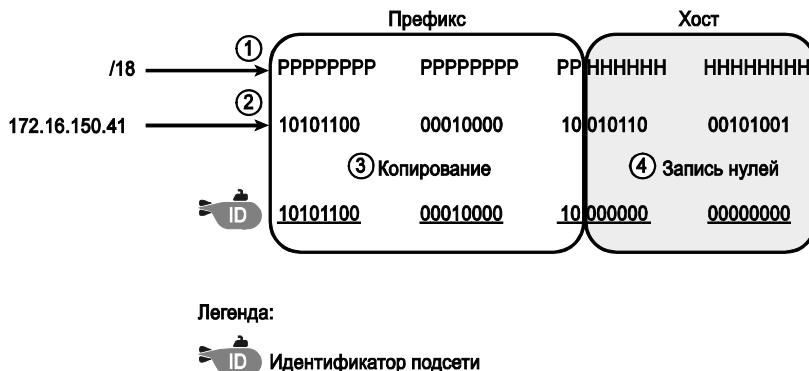


Рис. 17.4. Двоичная концепция: преобразование IP-адреса в идентификатор подсети

Начнем сверху рис. 17.4: формат IP-адреса представлен в виде 18 битов префикса (Р) и 14 битов хоста (Н) маски (этап 1). Вторая строка (этап 2) демонстрирует двоичную версию IP-адреса, преобразованного из десятичного представления с разделительными точками (DDN) 172.16.150.41. (Если таблица преобразования из приложения Б еще не использовалась, то самое время перепроверить преобразование всех четырех октетов на ее основании.)

Следующие два этапа демонстрируют действие: копирование битов префикса IP-адреса (этап 3) и присвоение битам хоста двоичных значений 0 (этап 4). В результате получается значение идентификатора подсети (в двоичном формате).

Последний этап, не представленный на рис. 17.4, подразумевает преобразование идентификатора подсети из двоичной системы счисления в десятичную. Здесь это преобразование представлено как отдельный этап на рис. 17.5 главным образом потому, что на данном этапе процесса многие делают ошибку. При преобразовании 32-разрядного числа (такого, как IP-адрес или идентификатор подсети) в формат DDN IPv4 необходимо придерживаться следующего правила:

преобразуйте из двоичной системы счисления в десятичную по 8 битов за раз, независимо от разделительной линии между частями префикса и хоста.

Этот последний этап представлен на рис. 17.5. Обратите внимание на то, что у третьего октета (третий набор из 8 битов) два бита находятся в префиксе и шесть битов в части хоста, но преобразование происходит для всех восьми битов.

ВНИМАНИЕ!

Числовые преобразования на рис. 17.4 и 17.5 можно осуществить с использованием таблицы преобразований из приложения Б. При преобразовании из формата DDN в двоичный для каждого октета находят десятичное значение в таблице, а затем записывают 8-битовый двоичный эквивалент. При преобразовании двоичного формата в DDN для каждого октета в таблице находят соответствующее двоичное значение и записывают соответствующее десятичное значение. Например, число 172 преобразуется в двоичное значение 10101100, а двоичное значение 00010000 преобразуется в десятичное 16.

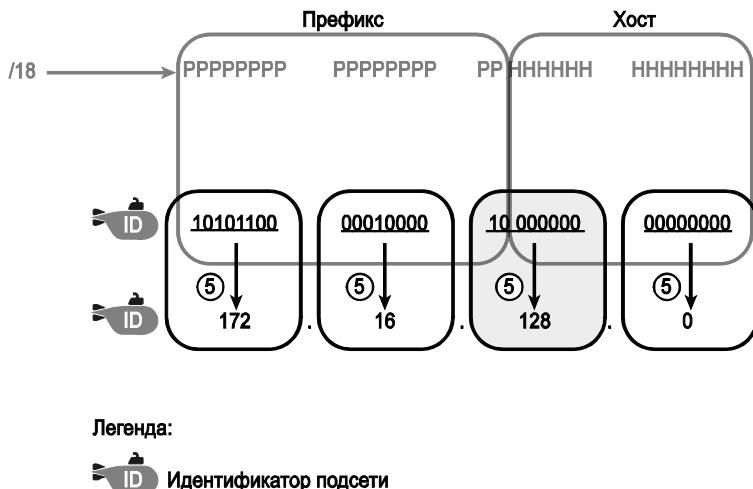


Рис. 17.5. Преобразование идентификатора подсети из двоичного формата в DDD

Поиск широковещательного адреса подсети: двоичный метод

При поиске широковещательного адреса подсети используется подобный процесс, но вместо записи всех битов части хоста наименьшим значением (бинарными нулями) они заполняются наибольшим значением (двоичными единицами). Данная концепция представлена на рис. 17.6.

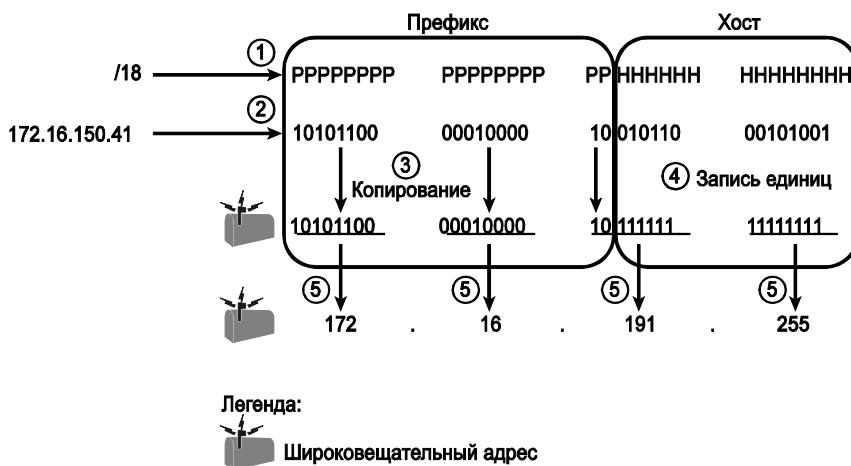


Рис. 17.6. Поиск широковещательного адреса подсети: двоичный метод

Первые три этапа процесса, приведенного на рис. 17.6, те же, что и на рис. 17.4. Это выявление битов префикса и хоста (этап 1), результат преобразования IP-адреса 172.16.150.41 в двоичный формат (этап 2) и копирование битов префикса (в данном случае первых 18 битов). Различие начинается в битах хоста справа — все они (в данном случае последние 14 битов) заменяются наибольшим возможным значением (двоичными единицами). На последнем этапе 32-разрядный широковещатель-

ный адрес подсети преобразуется в формат DDN. Кроме того, не забывайте, что при любом преобразовании из формата DDN в двоичный формат, и наоборот, используется по 8 битов за раз. В данном случае третий октет двоичных 10111111 преобразуется в десятичное значение 191.

Практические двоичные задачи

На рис. 17.4–17.6 приведен процесс поиска идентификатора подсети с использованием двоичной математики. Далее тот же процесс резюмирован в письменной форме для простоты изучения и применения.

Этапы применения двоичной математики для поиска идентификатора подсети



- Этап 1** Для нахождения длины префикса (/P) и длины части хоста (32 - P) преобразуйте маску в префиксный формат.
- Этап 2** Преобразуйте IP-адрес в его 32-разрядный двоичный эквивалент.
- Этап 3** Скопируйте префиксные биты IP-адреса.
- Этап 4** Запишите нули для битов хоста.
- Этап 5** Преобразуйте полученное 32-разрядное число, по 8 битов за раз, в десятичное число.

Процесс поиска широковещательного адреса подсети совершенно такой же, кроме этапа 4, где биты записываются единицами, а не нулями.

Уделите некоторое время решению следующих пяти практических задач на бумаге. В каждом случае найдите и идентификатор, и широковещательный адрес подсети. Кроме того, запишите маску в префиксном стиле.

1. 8.1.4.5, 255.255.0.0
2. 130.4.102.1, 255.255.255.0
3. 199.1.1.100, 255.255.255.0
4. 130.4.102.1, 255.255.252.0
5. 199.1.1.100, 255.255.255.224

В табл. 17.4–17.8 представлены результаты пяти задач. Здесь биты хоста выделены полужирным шрифтом в двоичной версии адреса и маски, а также в двоичной версии идентификатора и широковещательного адреса подсети.

Таблица 17.4. Анализ подсети для адреса 8.1.4.5 и маски 255.255.0.0

Длина префикса	/16	11111111 11111111 00000000 00000000
Адрес	8.1.4.5	00001000 00000001 00000100 00000101
Идентификатор подсети	8.1.0.0	00001000 00000001 00000000 00000000
Широковещательный адрес	8.1.255.255	00001000 00000001 11111111 11111111

Таблица 17.5. Анализ подсети для адреса 130.4.102.1 и маски 255.255.255.0

Длина префикса	/24	11111111 11111111 11111111 00000000
Адрес	130.4.102.1	10000010 00000100 01100110 00000001
Идентификатор подсети	130.4.102.0	10000010 00000100 01100110 00000000
Широковещательный адрес	130.4.102.255	10000010 00000100 01100110 11111111

Таблица 17.6. Анализ подсети для адреса 199.1.1.100 и маски 255.255.255.0

Длина префикса	/24	11111111 11111111 11111111 00000000
Адрес	199.1.1.100	11000111 00000001 00000001 01100100
Идентификатор подсети	199.1.1.0	11000111 00000001 00000001 00000000
Широковещательный адрес	199.1.1.255	11000111 00000001 00000001 11111111

Таблица 17.7. Анализ подсети для адреса 130.4.102.1 и маски 255.255.252.0

Длина префикса	/22	11111111 11111111 11111100 00000000
Адрес	130.4.102.1	10000010 00000100 011001 10 00000001
Идентификатор подсети	130.4.100.0	10000010 00000100 011001 00 00000000
Широковещательный адрес	130.4.103.255	10000010 00000100 011001 11 11111111

Таблица 17.8. Анализ подсети для адреса 199.1.1.100 и маски 255.255.255.224

Длина префикса	/27	11111111 11111111 11111111 11 100000
Адрес	199.1.1.100	11000111 00000001 00000001 011 00100
Идентификатор подсети	199.1.1.96	11000111 00000001 00000001 011 00000
Широковещательный адрес	199.1.1.127	11000111 00000001 00000001 011 11111

Сокращенный двоичный процесс

Описанный ранее в этом разделе двоичный процесс требует, чтобы все четыре октета были преобразованы в двоичные числа, а затем обратно в десятичные. Однако на основании маски DDN очень легко предсказать результаты по крайней мере трех из четырех октетов. Избежание двоичной математики во всех октетах, кроме одного, сокращает количество необходимых преобразований.

Сначала рассмотрим октет, значение маски DDN которого составляет 255. Десятичное значение 255 преобразуется в двоичное 11111111, значит, все 8 битов префиксные. Теперь рассмотрим приведенный в этой главе процесс из пяти этапов, но только для этого одного октета. В двоичном процессе поиска идентификатора подсети немало времени тратится на преобразование соответствующего октета IP-адреса в двоичный формат (этап 2). Но что происходит на этапе 3? Копирование! Затем, на этапе 4, то же 8-битовое значение преобразуется обратно в десятичное число, получается то же десятичное значение, с которого все началось! Так есть ли смысл во всех преобразованиях этого октета?

Рассмотрим знакомый случай 172.16.150.41 с маской 255.255.192.0, приведенный на рис. 17.4–17.6. В этом примере первые два октета маски — 255. Если вернуться к приведенным ранее рисункам, то можно увидеть: они демонстрируют, что первые два октета идентификатора и широковещательного адреса подсети составляют 172.16. Короче говоря, поскольку маска в каждом из первых двух октетов содержит значение 255, все, что достаточно сделать, — это скопировать десятичные значения IP-адреса данных октетов.

Для октетов, значение маски DDN которых составляет десятичный 0, существует другое сокращение. Десятичный 0 преобразуется в 8-битовое двоичное значение 00000000. Октет маски с 8 двоичными нулями означает, что все 8 битов в этом октете — биты хоста. И снова рассмотрим процесс из пяти этапов: на этапе 2 значение

IP-адреса преобразуется в двоичное значение, но на этапе 4 все 8 этих битов преобразуются в 00000000, независимо от того, чем они были ранее. На этапе 5 этот двоичный октет 00000000 преобразуется назад в десятичное число, т.е. в десятичный 0. Таким образом, если некий октет маски DDN содержит десятичный 0, идентификатор подсети будет иметь десятичный 0 в том же октете и математических преобразований в этом октете можно избежать.

Следующие пересмотренные этапы процесса учитывают эти два сокращения. Однако, когда значение октета маски не равно ни 0, ни 255, процесс требует тех же преобразований, но максимум для одного октета. При поиске идентификатора подсети следующая логика применима для каждого из четырех октетов.

Общие этапы использования двоичной и десятичной математики для поиска идентификатора подсети



Этап 1 Если октет маски равен 255, копируйте десятичный октет IP-адреса.

Этап 2 Если октет маски равен 0, запишите для него десятичный 0.

Этап 3 Если октет маски не равен 0 и 255, используйте в этом октете ту же двоичную логику, что и в разделе “Поиск идентификатора подсети: двоичный метод”.

Пример этого процесса приведен на рис. 17.7, опять же на примере 172.16.150.41, 255.255.192.0.

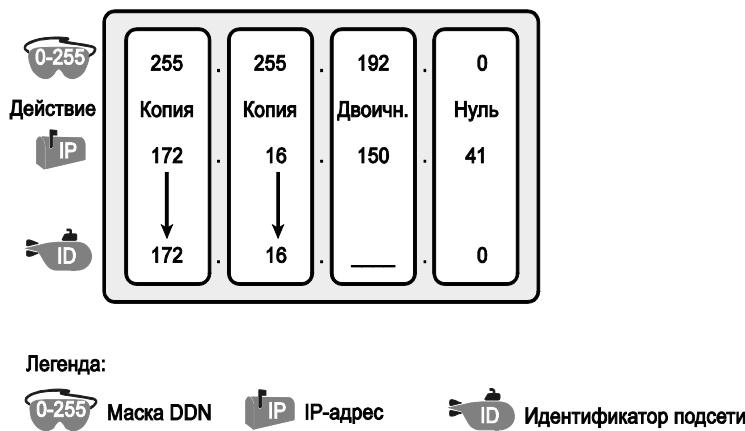


Рис. 17.7. Пример сокращения двоичного процесса

Подобное сокращение существует и при поиске широковещательного адреса подсети. Для октетов маски DDN, равных десятичному 0, значение широковещательного адреса подсети устанавливается равным 255, а не 0, как указано в следующем списке:

Этапы использования двоичной и десятичной математики для поиска широковещательного адреса подсети



Этап 1 Если октет маски равен 255, копируйте десятичный октет IP-адреса.

Этап 2 Если октет маски равен 0, запишите для него десятичное 255.

Этап 3 Если октет маски не равен 0 и 255, используйте в этом октете ту же двоичную логику, что и в разделе “Поиск широковещательного адреса подсети: двоичный метод”.

Краткое замечание о логической математике

В этой главе было описано, как люди могут использовать двоичную математику для поиска идентификатора и широковещательного адреса подсети. Однако компьютеры используют совершенно иной двоичный процесс для поиска тех же значений, использующий раздел математики, называемый *Булевой алгеброй*. Компьютеры уже хранят IP-адрес и маску в двоичном формате, поэтому они не должны делать никаких преобразований ни из десятичных чисел, ни в десятичные числа. Далее, операции Булевой алгебры позволяют компьютерам вычислять идентификатор и широковещательный адрес подсети всего за несколько действий процессора.

Не обязательно хорошо знать Булеву математику, чтобы иметь понятие о создании подсетей IP. Но если интересно, то вот как компьютеры используют Булеву логику для поиска идентификатора и широковещательного адреса подсети соответственно:

- выполнение булева И для IP-адреса и маски. Это преобразует все биты хоста в двоичные 0;
- инверсия маски и последующее булево ИЛИ для IP-адреса и инвертированной маски подсети. Это преобразует все биты хоста в двоичные 1.

Поиск диапазона адресов

Поиск диапазона пригодных для использования адресов подсети, как только стали известны идентификатор и широковещательный адрес подсети, требует только простого сложения и вычитания. Для поиска первого (самого низкого) пригодного для использования IP-адреса в подсети просто добавьте 1 к четвертому октету идентификатора подсети. Для поиска последнего (самого высокого) пригодного для использования IP-адреса вычтите 1 из четвертого октета широковещательного адреса подсети.

Анализ существующих подсетей: десятичный

Анализ существующих подсетей с использованием двоичного процесса работает хорошо. Однако занимает у большинства людей много времени, особенно на десятично-двоичные преобразования, а на экзаменах Cisco CCENT и CCNA решать задачи следует быстро. На экзамене нужно быть в состоянии вычислить идентификатор подсети и диапазон пригодных для использования адресов по IP-адресу и маске в течение приблизительно 15 секунд. При использовании двоичных методов большинству людей требуется большой практический навык, чтобы даже с помощью сокращенного двоичного процесса суметь найти эти ответы вовремя.

В данном разделе обсуждается, как находить идентификатор и широковещательный адрес подсети, используя только десятичную математику. Используя этот процесс, большинству людей проще и быстрее найти ответы, по крайней мере, после небольшой тренировки, по сравнению с двоичным процессом. Однако десятичный процесс ничего не скажет о смысле происходящего. Если вы не прочитали предыдущий раздел, “Анализ существующих подсетей: двоичный”, имеет смысл прочитать его ради понимания процесса создания подсетей. Этот раздел сосредоточивается на том, чтобы получать правильный ответ быстрее, используя подходящий метод.

Анализ с простыми масками

При трех простых масках поиск идентификатора и широковещательного адреса подсети требует лишь элементарной логики и почти никакой математики. Существуют три простых маски:

255.0.0.0
255.255.0.0
255.255.255.0

У этих масок есть только числа 255 и 0 в десятичном формате. По сравнению с ними у трудных масок есть один октет, значение которого ни 255, ни 0, что делает логику более сложной.

ВНИМАНИЕ!

Термины *простая маска* (easy mask) и *трудная маска* (difficult mask) придуманы в этой книге для описания маски и уровня трудности при работе с ней.

Когда в задаче используется простая маска, можете быстро найти идентификатор подсети на основании IP-адреса и маски в формате DDN. Просто используйте при поиске идентификатора подсети следующий процесс для каждого из этих четырех октетов.

Этап 1 Если октет маски равен 255, скопируйте его десятичное значение из IP-адреса.

Этап 2 Если октет маски равен 0, запишите десятичный 0.

Для поиска широковещательного адреса подсети используйте подобный простой процесс следующим образом.

Этап 1 Если октет маски равен 255, скопируйте его десятичное значение из IP-адреса.

Этап 2 Если октет маски равен 0, запишите десятичное 255.

Прежде чем перейти к следующему разделу, уделите время заполнению пробелов в табл. 17.9. Проверьте свои ответы по табл. 17.14 в разделе “Ответы на приведенные ранее практические задания”. Укажите в таблице идентификатор подсети и широковещательный адрес подсети.

Таблица 17.9. Практическое задание: найдите идентификатор и широковещательный адрес подсети по простым маскам

IP-адрес	Маска	Идентификатор подсети	Широковещательный адрес
1 10.77.55.3	255.255.255.0		
2 172.30.99.4	255.255.255.0		
3 192.168.6.54	255.255.255.0		
4 10.77.3.14	255.255.0.0		
5 172.22.55.77	255.255.0.0		
6 1.99.53.76	255.0.0.0		

Предсказуемость в интересующем октете

Хотя с тремя масками (255.0.0.0, 255.255.0.0 и 255.255.255.0) работать проще, остальные делают десятичную математику немного трудной, поэтому назовем эти маски трудными. У трудных масок значение одного октета отлично от 0 или 255. Математика в других трех октетах проста, а октет с более трудной математикой в книге называется *интересующим октетом*.

Если уделить время обдумыванию различных проблем и сосредоточиться на интересующем октете, то можно заметить определенный шаблон. Этот раздел демонстрирует, как использовать шаблон в десятичном числе и найти идентификатор подсети.

Значение идентификатора подсети имеет предсказуемое десятичное значение, если для всех подсетей одной классовой сети используется единая маска. Помните, в этой книге подразумевается, что для данной классовой сети разработчик решил использовать единую маску во всех подсетях. (Более подробную информацию по этой теме см. в главе 12.)

Для демонстрации предсказуемости рассмотрим рис. 17.8, на котором приведены некоторое идеи, учитываемые разработчиком при разделении на подсети сети класса В 172.16.0.0. Рисунок демонстрирует также некоторые сравнения использования масок 255.255.128.0, 255.255.192.0, 255.255.224.0 и 255.255.240.0. Каждая из масок является трудной благодаря наличию в третьем октете числа, отличного от 255 или 0, что делает третий октет интересующим. На рис. 17.8 показаны десятичные значения в третьем октете всех идентификаторов подсети данной сети и номера подсетей на основании каждого возможного выбора для маски.

Подсети сети 172.16.0.0: 172.16.___.0

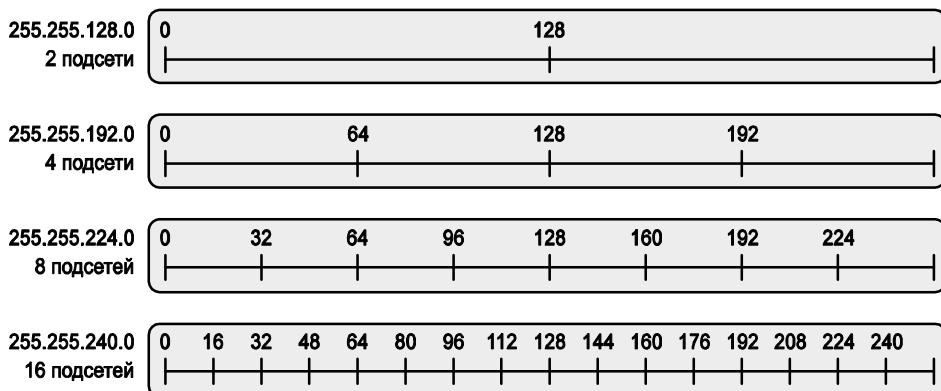


Рис. 17.8. Числовые шаблоны в интересующем октете

В первую очередь обратите внимание на верхнюю часть рисунка, где приведен результат использования маски 255.255.128.0. Визуально первоначальная сеть класса В представляет всю ширину линии, а маска 255.255.128.0 делит ее на две равных половины. Почему две? Поскольку существует только один бит подсети, получается 2^1 (или 2) подсети. На рис. 17.8 представлены значения только в интересующем октете, чтобы подчеркнуть шаблоны, но полными идентификаторами подсети будут 172.16.0.0 и 172.16.128.0.

Затем перейдем к примеру применения маски 255.255.192.0. Используя эту, и только эту маску, сеть класса В разделяется на четыре равных по размеру подсети; поскольку здесь существуют два бита подсети, получается 2^2 , или четыре подсети. Идентификаторы подсети: 172.16.0.0, 172.16.64.0, 172.16.128.0 и 172.16.192.0.

И наконец, в последних двух примерах: с маской 255.255.224.0 есть 8 подсетей, делящих сеть на восемь равных частей, и с маской 255.255.240.0, делящих сеть на 16 равных частей. На рис. 17.8 показаны значения интересующего октета (третий октет в данном случае) со всеми подсетями в формате 172.16._____.0 для данного примера.

Шаблоны на рис. 17.8 очевидны. Независимо от выбранной разработчиком маски подсети значения идентификатора подсети следуют шаблону. Для поиска идентификатора подсети необходим только способ выяснить, каков шаблон. Если начинать приходится только с IP-адреса, найдите идентификатор подсети как число кратное магическому числу, ближайшее к IP-адресу без перекрытия (подробнее об этом — в следующем разделе).

Поиск идентификатора подсети: трудные маски

Ниже описаны все этапы процесса нахождения идентификатора подсети с использованием только десятичной математики. Этот процесс дополняет прежний процесс с использованием простых масок.



Этапы использования только десятичной математики для поиска идентификатора подсети

Этап 1 Если октет маски равен 255, скопируйте его десятичное значение из IP-адреса.

Этап 2 Если октет маски равен 0, запишите десятичный 0.

Этап 3 Если значение другое, считайте октет *интересующим*:

а) вычислите *магическое число* как 256 – маска;

б) установите значение идентификатора подсети как кратное магическому числу, ближайшее к IP-адресу без перекрытия.

Процесс использует два новых термина, введенные в этой книге: *магическое число* (magic number) и *интересующий октет* (interesting octet). Термин *интересующий октет* описывает октет, выявленный на третьем этапе процесса; другими словами, октет маски, значением которого не является ни 255, ни 0. Этап 3 а) использует термин *магическое число*, происходящее от маски DDN. Концептуально магическое число — это число, которое, будучи добавлено к одному идентификатору подсети, даст следующий идентификатор подсети по порядку (см. рис. 17.8). В цифровой форме оно находится при вычитании значения маски DDN, в интересующем октете, из числа 256, как упомянуто на этапе 3 а).

Наилучший способ изучения этого процесса — посмотреть, что происходит. Если можете, отложите пока книгу, достаньте компакт-диск, прилагаемый к ней, и просмотрите видеофильмы о поиске идентификатора подсети с трудной маской. Можно также использовать примеры, приведенные на следующих страницах, чтобы попрактиковаться на бумаге. Затем можно заняться заданиями из раздела “Практические задания по анализу существующих подсетей”.

Резидентская подсеть (пример 1)

Рассмотрим, например, задание найти резидентскую подсеть для IP-адреса 130.4.102.1 и маски 255.255.240.0. Процесс не требует заботиться о битах префикса и хоста, преобразовании маски, рассмотрении маски в двоичном формате или преобразовании IP-адреса в двоичный формат и из него. Вместо этого для каждого из четырех октетов выберите действие на основании значения маски. На рис. 17.9 приведены результаты; номера в кружках соответствуют номерам этапов процесса поиска идентификатора подсети, приведенного выше в главе.

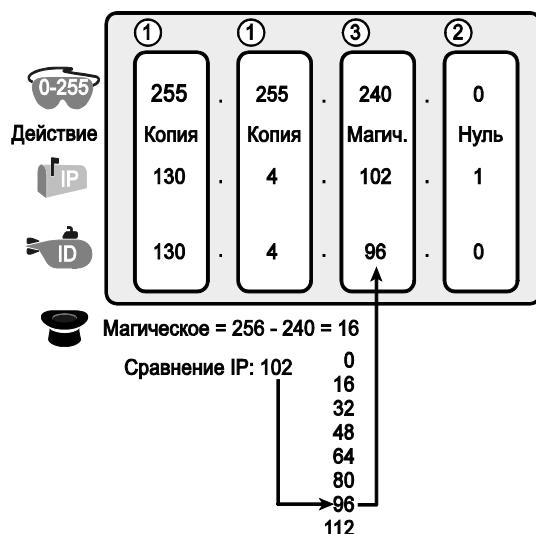


Рис. 17.9. Поиск идентификатора подсети: 130.4.102.1, 255.255.240.0

Сначала исследуйте три не интересующих октета (1, 2 и 4). Процесс основан на маске. У первых двух октетов маски есть значение 255, поэтому просто копируем октеты IP-адреса в октеты идентификатора подсети. У четвертого октета маски значение равно 0, поэтому для четвертого октета идентификатора подсети запишем 0.

Наиболее сложная логика находится в интересующем октете (третьем в данном случае) со значением маски 240. Для этого октета этап 3 а) подразумевает вычисление магического числа, как $256 - \text{маска}$. Это значит, что следует взять значение маски в интересующем октете (в данном случае 240) и вычесть его из 256: $256 - 240 = 16$. Значения идентификатора подсети в этом октете должно быть кратно десятичному числу 16 в данном случае.

Далее, этап 3 б) подразумевает поиск значений, кратных магическому числу (в данном случае 16), и выбор самого близкого из них к IP-адресу без перекрытия. В частности, это означает, что необходимо мысленно вычислить значения, кратные магическому числу, начиная с 0. (Не забывайте 0!) Получаем набор чисел: 0, 16, 32, 48, 64, 80, 96, 112 и т.д. Затем найдите кратное значение, ближайшее к значению IP-адреса в этом октете (в данном случае 102), но не превышающее его. Как видно на рис. 17.9, это значение 96. Именно оно и выбирается для третьего октета идентификатора подсети 130.4.96.0.

Резидентская подсеть (пример 2)

Рассмотрим другой пример: 192.168.5.77 с маской 255.255.255.224. Результаты приведены на рис. 17.10.

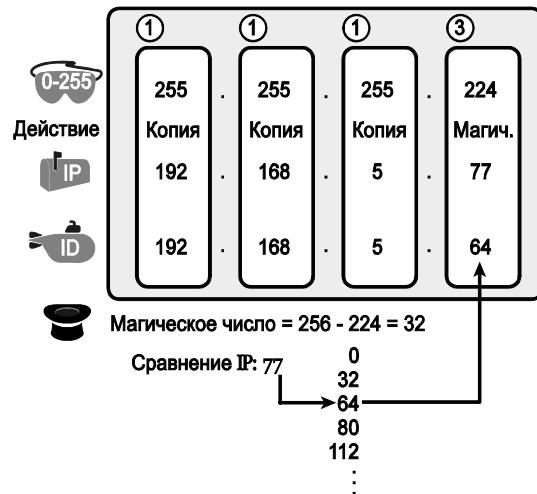


Рис. 17.10. Резидентская подсеть 192.168.5.73, 255.255.255.224

Три не интересующих октета (1, 2 и 3 в данном случае) требуют небольшого напряжения мысли. Для каждого октета со значением маски 255 достаточно скопировать значение из IP-адреса.

Для интересующего октета на этапе 3 а) магическое число составит $256 - 224 = 32$. Кратные магическому числу числа: 0, 32, 64, 96 и т.д. Поскольку значением IP-адреса в четвертом октете является 77, кратное число должно быть ближайшим к нему, но без перекрытия; поэтому идентификатор подсети закончится на 64 (192.168.5.64).

Практические задания по резидентским подсетям

Прежде чем переходить к следующему разделу, уделите время заполнению пробелов в табл. 17.10. Проверьте свои ответы по табл. 17.15. Заполните в таблице столбец идентификатора подсети по каждому случаю. Объяснения выполнения каждого задания приведено после табл. 17.15.

Таблица 17.10. Практическое задание: поиск идентификатора подсети: трудные маски

Задание	IP-адрес	Маска	Идентификатор подсети
1	10.77.55.3	255.248.0.0	
2	172.30.99.4	255.255.192.0	
3	192.168.6.54	255.255.255.252	
4	10.77.3.14	255.255.128.0	
5	172.22.55.77	255.255.254.0	
6	1.99.53.76	255.255.255.248	

Поиск широковещательного адреса подсети: трудные маски

Для поиска широковещательного адреса подсети применяется подобный процесс. Для простоты он начинается с идентификатора подсети, а не IP-адреса. Если вам случится начинать с IP-адреса, используйте описанные в этой главе процессы, чтобы сначала найти идентификатор подсети, а затем используйте следующий процесс для поиска широковещательного адреса подсети для той же подсети. Для каждого октета сделайте следующее.

Ключевая тема Этапы использования только десятичной математики для поиска широковещательного адреса подсети

Этап 1 Если октет маски равен 255, скопируйте значение идентификатора подсети.

Этап 2 Если октет маски равен 0, запишите 255.

Этап 3 Если значение другое, считайте октет *интересующим*:

а) вычислите *магическое число*, как $256 - \text{маска}$;

б) возьмите значение идентификатора подсети, добавьте магическое число и вычтите 1 (*идентификатор + магическое - 1*).

Подобно процессу, использованному при поиске идентификатора подсети, есть несколько возможностей для лучшего изучения и усвоения процесса. Сейчас можно отложить чтение и использовать компакт-диск, прилагаемый к книге, чтобы просмотреть видеофильм о поиске широковещательного адреса подсети с трудной маской. Кроме того, посмотрите примеры в этом разделе, которые демонстрируют этот процесс на бумаге. Затем обратитесь к заданиям из раздела “Практические задания по анализу существующих подсетей” данной главы.

Широковещательный адрес подсети пример 1

Данный пример является продолжением первого примера из раздела “Поиск идентификатора подсети: трудные маски”, представленного на рис. 17.9. Этот пример начинается с IP-адреса и маски (130.4.102.1, 255.255.240.0) и демонстрирует поиск идентификатора подсети 130.4.96.0. Рис. 17.11 начинается теперь с идентификатора подсети и той же маски.



Рис. 17.11. Поиск широковещательного адреса подсети:
130.4.96.0, 255.255.240.0

Сначала исследуйте три не интересующих октета (1, 2 и 4). Первые два октета маски имеют значение 255, поэтому просто копируем октет идентификатора подсети в соответствующий октет широковещательного адреса подсети. В четвертом октете маски значение 0, поэтому для четвертого октета запишите 255.

Интересующим октетом в данном примере является третий, из-за значения 240 маски. Сначала, на этапе 3 а), необходимо вычислить магическое число, как 256 – маска. (Если идентификатор подсети уже вычислен в ходе приведенного ранее процесса, магическое число должно быть известно.) На этапе 3 б) возьмите значение идентификатора подсети (96), добавьте магическое число (16) и вычтите 1, в результате получится 111. Это даст широковещательный адрес подсети 130.4.111.255.

Широковещательный адрес подсети (пример 2)

Этот пример также продолжает предыдущий пример из раздела “Поиск идентификатора подсети: трудные маски”, представленный на рис. 17.10. Пример демонстрировал, как, начиная с IP-адреса 192.168.5.77 и маски 255.255.255.224, найти идентификатор подсети 192.168.5.64. Рис. 17.12 начинается с этого идентификатора подсети и той же маски.

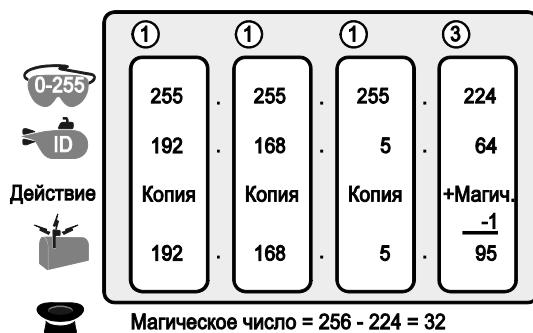


Рис. 17.12. Поиск широковещательного адреса подсети:
192.168.5.64, 255.255.255.224

Сначала исследуйте три не интересующих октета (1, 2 и 3). У первых трех октетов маски значение 255, поэтому просто копируем октет идентификатора подсети в соответствующий октет широковещательного адреса подсети.

Четвертый октет этого примера интересующий, поскольку имеет значение 224 маски. Сначала этап 3 а) требует вычислить магическое число, как 256 – маска. (Если идентификатор подсети уже вычислялся, то это то же магическое число, поскольку используется та же маска.) На этапе 3 б) возьмите значение идентификатора подсети (64), добавьте магическое значение (32) и вычтите 1, в результате получится 95. Это даст широковещательный адрес подсети 192.168.5.95.

Практические задания по широковещательному адресу подсети

Прежде чем переходить к следующему разделу, уделите время выполнению нескольких практических заданий на листе бумаги. Вернитесь к табл. 17.10, где перечислены IP-адреса и маски, чтобы попрактиковаться в поиске широковещательного адреса подсети для всех задач этой таблицы. Затем проверьте свои ответы по табл. 17.16.

Практические задания по анализу существующих подсетей

Перед тем как перейти к следующей главе, попрактикуйтесь в процессах, обсуждаемых в данной главе, пока не станете почти всегда получать правильные ответы. Используйте любые средства по своему усмотрению и любое время. Затем можно продолжить чтение.

Перед сдачей экзамена потренируйтесь, чтобы овладеть темой данной главы полностью и отвечать достаточно быстро. Что касается времени, то идентификатор подсети на основании IP-адреса и маски следует найти приблизительно через 15 секунд. Следует также стремиться, начиная с идентификатора подсети и маски, находить широковещательный адрес и диапазон адресов еще через 10–15 секунд. Ключевые концепции и рекомендации такого двухэтапного подхода приведены в табл. 17.11.

Таблица 17.11. Продолжайте читать с учетом целей экзамена по темам данной главы

Период	Перед переходом к следующей главе	Перед сдачей экзамена
Сосредоточьтесь на ...	теме изучения	быть быстрым и правильным
Разрешенные средства	Все	Ваш мозг и блокнот
Цель: точность	90% правильных ответов	100% правильных ответов
Цель: скорость	Любая скорость	20–30 секунд

Выбор: запомнить или вычислять

Как описано в этой главе, десятичные процессы поиска идентификатора и широковещательного адреса подсети действительно требуют некоторых вычислений, включая вычисление магического числа (256 – маска). Эти же процессы подразумевали, что начинать приходилось с маски в формате DDN. Поэтому уделите время приведенным в книге процессам преобразования маски в формат DDN, прежде чем приступить к экзаменационным вопросам с префиксными масками.

За эти годы многие люди говорили мне, что предпочитают запоминать таблицу для поиска магического числа. В этой таблице перечислены магические числа для разных масок и префиксные маски, таким образом, вы избегаете преобразования из префиксного формата маски в DDN. Табл. 17.12 — пример такой таблицы. Не стесняйтесь игнорировать или использовать данную таблицу, это сугубо ваш собственный выбор.

Таблица 17.12. Справочная таблица: значения маски DDN, двоичный эквивалент, магические числа и префиксы

Префикс, интересующий октет 2	/9	/10	/11	/12	/13	/14	/15	/16
Префикс, интересующий октет 3	/17	/18	/19	/20	/21	/22	/23	/24
Префикс, интересующий октет 4	/25	/26	/27	/28	/29	/30		
Магическое число	128	64	32	16	8	4	2	1
Маска DDN в интересующем октете	128	192	224	240	248	252	254	255

Практические задания этой главы

В отличие от других глав по созданию подсетей, в этой главе практические задания распределены по всей главе, поэтому дополнительных заданий в этом разделе нет. Для справки: практические задачи находятся в следующих разделах.

- Практические двоичные задачи.
- Практические задания по резидентским подсетям.
- Практические задания по широковещательному адресу подсети.

Дополнительные практические задания

В этом разделе перечислены некоторые возможности для дополнительной практики.

- Приложение 3, в котором содержатся дополнительные практические задания. Оно содержит также объяснения по поиску ответа на каждое задание.
- Создайте собственные задания. Большинство калькуляторов подсети позволяют найти биты сети, подсети и хоста, когда вводят IP-адрес и маску, поэтому запишите IP-адрес и маску на бумаге, а затем найдите идентификатор подсети и диапазон адресов. Затем, чтобы проверить результат, используйте любой калькулятор подсети. (Несколько калькуляторов предложено на веб-странице автора этой книги, указанной во введении.)
- Приложения Find a Subnet ID и Find the Address Range для iPhone на Subnet Prep (www.subnetprep.com) предоставляет обзорное видео и практически безграничное количество практических задач, связанных с темами этой главы. Первое приложение посвящено поиску идентификатора подсети, второе — поиску диапазона адресов подсети.

Подготовка к экзамену

Повторите все ключевые темы

Повторите все ключевые темы данной главы, помеченные пиктограммой “Ключевая тема”. Ключевые темы и соответствующие им страницы перечислены в табл. 17.13.

Таблица 17.13. Ключевые темы главы 17

Элемент	Описание	Страница
Табл. 17.2	Основные факты об идентификаторах подсетей	446
Табл. 17.3	Основные факты о широковещательных адресах подсетей	447
Список	Этапы применения двоичной математики для поиска идентификатора подсети	451
Список	Общие этапы использования двоичной и десятичной математики для поиска идентификатора подсети	453
Список	Этапы использования двоичной и десятичной математики для поиска широковещательного адреса подсети	453
Список	Этапы использования только десятичной математики для поиска идентификатора подсети	457
Список	Этапы использования только десятичной математики для поиска широковещательного адреса подсети	460

Заполните таблицы и списки по памяти

Распечатайте приложение М (Appendix L) с компакт-диска или его раздел, относящийся к этой главе, и заполните таблицы и списки по памяти. В приложении Н (Appendix M) приведены заполненные таблицы и списки для самоконтроля.

Ключевые термины

Дайте определения перечисленных ниже терминов и проверьте правильность их написания в списке терминов:

резидентская подсеть (resident subnet), идентификатор подсети (subnet ID), номер подсети (subnet number), адрес подсети (subnet address), широковещательный адрес подсети (subnet broadcast address)

Практика

Если это еще не сделано, попрактикуйтесь в вопросах поиска идентификатора подсети, диапазона адресов и широковещательного адреса подсети, связанных с IP-адресом и маской, описанных в данной главе. Рекомендации приведены в разделе “Практические задания по анализу существующих подсетей”.

Ответы на приведенные ранее практические задания

Эта глава содержит множество заданий, распределенных по всей главе. Ответы находятся в табл. 17.14–17.16.

Таблица 17.14. Ответы на практические задания табл. 17.9

	IP-адрес	Маска	Идентификатор подсети	Широковещательный адрес
1	10.77.55.3	255.255.255.0	10.77.55.0	10.77.55.255
2	172.30.99.4	255.255.255.0	172.30.99.0	172.30.99.255
3	192.168.6.54	255.255.255.0	192.168.6.0	192.168.6.255
4	10.77.3.14	255.255.0.0	10.77.0.0	10.77.255.255
5	172.22.55.77	255.255.0.0	172.22.0.0	172.22.255.255
6	1.99.53.76	255.0.0.0	1.0.0.0	1.255.255.255

Таблица 17.15. Ответы на практические задания табл. 17.10

	IP-адрес	Маска	Идентификатор подсети
1	10.77.55.3	255.248.0.0	10.72.0.0
2	172.30.99.4	255.255.192.0	172.30.64.0
3	192.168.6.54	255.255.255.252	192.168.6.52
4	10.77.3.14	255.255.128.0	10.77.0.0
5	172.22.55.77	255.255.254.0	172.22.54.0
6	1.99.53.76	255.255.255.248	1.99.53.72

Ниже приведены объяснения ответов для табл. 17.15.

1. Интересующий октет второй, с магическим числом $256 - 248 = 8$. К числам, кратным 8, относятся: 0, 8, 16, 24, ..., 64, 72 и 80. Число 72 является самым близким к значению IP-адреса в том же октете (77) без превышения. В результате получаем идентификатор подсети 10.72.0.0.
2. Интересующий октет третий, с магическим числом $256 - 192 = 64$. К числам, кратным 64, относятся: 0, 64, 128 и 192. Число 64 является самым близким к значению IP-адреса в том же октете (99) без превышения. В результате получаем идентификатор подсети 172.30.64.0.
3. Интересующий октет четвертый, с магическим числом $256 - 252 = 4$. К числам, кратным 4, относятся: 0, 4, 8, 12, 16, ..., 48, 52 и 56. Число 52 является самым близким к значению IP-адреса в том же октете (54) без превышения. В результате получаем идентификатор подсети 192.168.6.52.
4. Интересующий октет третий, с магическим числом $256 - 128 = 128$. Для этого случая существуют только два кратных значения: 0 и 128. Число 0 является самым близким к значению IP-адреса в том же октете (3) без превышения. В результате получаем идентификатор подсети 10.77.0.0.
5. Интересующий октет третий, с магическим числом $256 - 254 = 2$. К числам, кратным 2, относятся: 0, 2, 4, 6, 8 и так далее, по существу, все четные числа. Число 54 является самым близким к значению IP-адреса в том же октете (55) без превышения. В результате получаем идентификатор подсети 172.22.54.0.
6. Интересующий октет четвертый, с магическим числом $256 - 248 = 8$. К числам, кратным 8, относятся: 0, 8, 16, 24, ..., 64, 72 и 80. Число 72 является самым близким к значению IP-адреса в том же октете (76) без превышения. В результате получаем идентификатор подсети 1.99.53.72.

Таблица 17.16. Ответы на практические задания раздела “Практические задания по широковещательному адресу подсети”

Идентификатор подсети	Маска	Широковещательный адрес
1 10.72.0.0	255.248.0.0	10.79.255.255
2 172.30.64.0	255.255.192.0	172.30.127.255
3 192.168.6.52	255.255.255.252	192.168.6.55
4 10.77.0.0	255.255.128.0	10.77.127.255
5 172.22.54.0	255.255.254.0	172.22.55.255
6 1.99.53.72	255.255.255.248	1.99.53.79

Ниже приведены объяснения ответов для табл. 17.16.

1. Интересующий октет второй. Обработка трех простых октетов дает широковещательный адрес без интересующего октета 10.____.255.255. С магическим числом $256 - 248 = 8$, второй октет будет 72 (из идентификатора подсети) плюс 8 минус 1, или 79.
2. Интересующий октет третий. Обработка трех простых октетов дает широковещательный адрес без интересующего октета 172.30.____.255. С магическим числом $256 - 192 = 64$, интересующий октет будет 64 (из идентификатора подсети) плюс 64 (магическое число) минус 1, или 127.
3. Интересующий октет четвертый. Обработка трех простых октетов дает широковещательный адрес без интересующего октета 192.168.6.____. С магическим числом $256 - 252 = 4$, интересующий октет будет 52 (значение идентификатора подсети) плюс 4 (магическое число) минус 1, или 55.
4. Интересующий октет третий. Обработка трех простых октетов дает широковещательный адрес без интересующего октета 10.77.____.255. С магическим числом $256 - 128 = 128$, интересующий октет будет 0 (значение идентификатора подсети) плюс 128 (магическое число) минус 1, или 127.
5. Интересующий октет третий. Обработка трех простых октетов дает широковещательный адрес без интересующего октета 172.22.____.255. С магическим числом $256 - 254 = 2$, широковещательный адрес в интересующем октете будет 54 (значение идентификатора подсети) плюс 2 (магическое число) минус 1, или 55.
6. Интересующий октет четвертый. Обработка трех простых октетов дает широковещательный адрес без интересующего октета 1.99.53.____. С магическим числом $256 - 248 = 8$, широковещательный адрес в интересующем октете будет 72 (значение идентификатора подсети) плюс 8 (магическое число) минус 1, или 79.

В этой главе...

- **Поиск всех идентификаторов подсети.** Рассматривается процесс создания списка всех идентификаторов подсетей в сети на основании класса сети IP и единой маски, используемой во всей сети.
- **Практические задания по поиску всех идентификаторов подсети.** Содержатся советы по практическому применению процесса поиска всех подсетей в сети.

ГЛАВА 18

Поиск всех идентификаторов подсети

Как описано в главе 12, процесс проектирования подсетей IP требует выбора нескольких решений. Разработчик должен выбрать определенную частную сеть IP или зарегистрировать открытую сеть IP. Он также должен выбрать, использовать ли одну маску или несколько. (В этой книге подразумевается, что решено использовать одну маску.) И наконец, разработчик должен выбрать, какую именно единую маску использовать.

В этой главе подразумевается наличие результата сделанного выбора (идентификатора сети и одной маски подсети) и демонстрируется, как вычислить все идентификаторы для всех подсетей, которые существуют в данной сети при использовании единой маски.

Контрольные вопросы: знаете ли вы уже темы главы

Этот раздел предназначен для того, чтобы читатель мог предварительно оценить свои знания и решить, нужно ли ему читать главу целиком. Если ответы на девять из десяти вопросов даны правильно, можно сразу же перейти к последнему разделу “Подготовка к экзамену”. Основные темы этой главы и предварительных контрольных вопросов перечислены в табл. 18.1. Отвечая на контрольные вопросы и используя таблицу, читатель сможет достаточно точно определить свои знания в той или иной области. Ответы на вопросы приведены в приложении А.

Таблица 18.1. Темы контрольных вопросов

Основная тема	Номера вопросов
Поиск всех идентификаторов подсети	1–7

1. Какой из приведенных ниже допустимых идентификаторов подсети для сети 10.0.0.0 подразумевает использование маски 255.240.0.0 по всей сети 10.0.0.0? (Выберите несколько ответов.)
 - a) 10.1.16.0
 - б) 10.0.0.0
 - в) 10.240.0.0
 - г) 10.0.0.32
2. Инженер создал последовательный список идентификаторов подсети для сети 172.30.0.0/22. Подразумевается, что маска /22 используется по всей сети. Какое из следующих утверждений истинно? (Выберите несколько ответов.)

- а) Любые два последовательные идентификатора подсети отличаются значением 22 в третьем октете.
- б) Любые два последовательные идентификаторы подсети отличаются значением 16 в четвертом октете.
- в) Список содержит 64 идентификатора подсети.
- г) Последний идентификатор подсети 172.30.252.0.
3. Какой из приведенных ниже идентификаторов подсети допустим для сети 192.168.9.0 при использовании маски /29 с учетом, что она используется по всей сети?
- а) 192.168.9.144
- б) 192.168.9.58
- в) 192.168.9.242
- г) 192.168.9.9
4. Инженер, использующий сеть класса В 172.20.0.0, правильно решил, что следующие идентификаторы подсети допустимы: 172.20.128.0, 172.20.192.0 и 172.20.80.0. С учетом, что во всей сети 172.20.0.0 используется одна маска, какая из следующих масок могла использоваться в компании?
- а) 255.255.252.0
- б) 255.255.192.0
- в) 255.255.224.0
- г) 255.255.0.0
5. Какой из перечисленных ниже идентификаторов подсети не допустим для сети 172.19.0.0 при использовании единой для всей сети маски /24?
- а) 172.19.0.0
- б) 172.19.1.0
- в) 172.19.255.0
- г) 172.19.0.16
6. Какой из перечисленных ниже идентификаторов подсети не допустим для сети 172.19.0.0 при использовании единой для всей сети маски /27?
- а) 172.19.0.0
- б) 172.19.160.16
- в) 172.19.255.64
- г) 172.19.192.192
7. Какой из перечисленных ниже идентификаторов подсети не допустим для сети 10.0.0.0 при использовании единой для всей сети маски /25?
- а) 10.0.0.0
- б) 10.255.255.0
- в) 10.255.127.128
- г) 10.1.1.192

Основные темы

Поиск всех идентификаторов подсети

Эта глава сосредоточена на одном-единственном вопросе:

Дана одна сеть класса A, B или C и одна маска подсети, используемая для всех подсетей, каковы все идентификаторы подсети?

Чтобы узнать ответ на этот вопрос, можно решить проблему двоичным или десятичным способом. В этой главе используется десятичный подход. Хотя сам процесс требует лишь простой математики, большинству людей потребуются практические навыки, чтобы быстро и уверенно отвечать на этот вопрос.

Десятичный процесс начинается с выявления первого, или самого младшего, идентификатора подсети. Затем процесс выявляет шаблон всех идентификаторов подсети для данной маски подсети, чтобы можно было найти каждый последующий идентификатор подсети с помощью простого сложения. Сначала в этом разделе рассматриваются ключевые идеи данного процесса, а затем дано формальное определение процесса.

ВНИМАНИЕ!

В некоторых видеофильмах на прилагаемом компакт-диске продемонстрированы те же фундаментальные процессы поиска всех идентификаторов подсети. Вы можете просмотреть их до или после чтения данного раздела, или даже вместо того, чтобы читать его, пока не узнаете, как независимо найти все идентификаторы подсети. Нумерация этапов процесса на видео может не соответствовать этапам, изложенным в данном издании книги.

Первый идентификатор подсети: нулевая подсеть

Первый этап поиска всех идентификаторов подсети одной сети невероятно прост: скопируйте идентификатор сети. Например, возьмите идентификатор сети класса A, B или C, другими словами, идентификатор классовой сети, и запишите его как первый идентификатор подсети. Независимо от класса (A, B или C) используемой сети и маски подсети, первый идентификатор подсети совпадает с идентификатором сети.

Например, если речь идет о классовой сети 172.20.0.0, то независимо от маски первым идентификатором подсети будет 172.20.0.0.

Этот первый идентификатор подсети в каждой сети имеет два специальных названия: *нулевая подсеть* (zero subnet) или *подсеть нуль* (subnet zero). Первоначально происхождение этих названий связывали с тем фактом, что у нулевой подсети сети в двоичном представлении вся часть подсети занята двоичными нулями. В десятичном представлении нулевая подсеть может быть легко выявлена по тому, что в чистом виде она всегда совпадает с идентификатором самой сети.

ВНИМАНИЕ!

В последнее время в проектах подсетей IP, как правило, не используют нулевую подсеть во избежание недоразумений, которые могут возникнуть из-за совпадения идентификатора сети с идентификатором подсети.

Поиск шаблона с использованием магического числа

Идентификаторы подсети следуют вполне предсказуемому шаблону, по крайней мере, в случае использования единой маски для всех подсетей в сети. Шаблон использует *магическое число*, обсуждавшееся в главе 17. Напомним: магическое число — это 256 минус десятичное значение маски в определенном октете, который в данной книге именуется *интересующим октетом*.

На рис. 18.1 приведены четыре числовых оси, по одной для каждой из масок /17 – /20. Линии с числами представляют шаблон значений в третьем октете идентификаторов подсети при использовании этих масок. Числа слева представляют значение маски в десятичном представлении с разделительными точками (DDN) и вычисляемое магическое число. Справа на рисунке представлены числовые значения в третьем октете для каждой из подсетей любой сети класса В при использовании соответствующей маски.

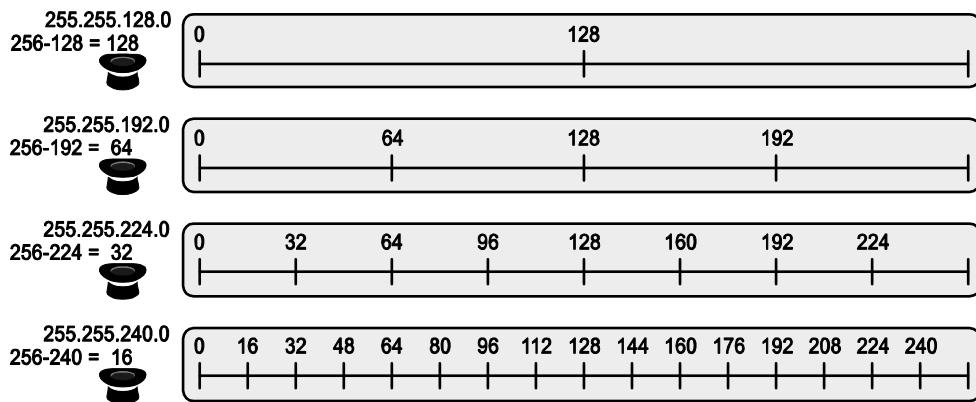


Рис. 18.1. Шаблоны с магическими числами для масок /17 – /20

Например, если сеть класса В 172.16.0.0 разделена на подсети маской /17 (или 255.255.128.0), см. верхнюю часть рисунка, — идентификаторами подсети были бы 172.16.0.0 и 172.16.128.0. Обратите, в частности, внимание на то, что третий октеты каждого идентификатора подсети кратны магическому числу (128), вычисленному как $256 - 128 = 128$. Второй ряд на рис. 18.1 демонстрирует другую маску, 255.255.192.0, с магическим числом 64 ($256 - 192 = 64$). При использовании с сетью 172.16.0.0 идентификаторами подсети были бы 172.16.0.0, 172.16.64.0, 172.16.128.0 и 172.16.192.0, с шаблоном в третьем октете, представляющим значения, кратные 64. То же самое происходит в двух других примерах на рисунке с идентификаторами подсети, кратными 32 (маска /19 или 255.255.224) и 16 (маска /20 или 255.255.240.0) соответственно.

Формальный процесс с менее чем 8 битами подсети

Хотя шаблоны на рис. 18.1 вполне очевидны, может быть не до конца понятно, как применить эти концепции для поиска всех идентификаторов подсети в любом случае. Этот раздел посвящен исключительно процессу поиска всех идентификаторов подсети.

Чтобы упростить объяснения, в этом разделе подразумевается, что битов подсети меньше 8. Далее, в разделе “Поиск всех подсетей с более чем 8 битами подсети”, описан полный процесс, применимый во всех случаях.

Вначале, чтобы упорядочить свои мысли, возможно, имеет смысл свести данные в таблицу, подобную табл. 18.2. В книге такая таблица называется обобщенным перечнем всех подсетей.

Таблица 18.2. Обобщенный перечень всех подсетей

Октет	1	2	3	4
Маска				
Магическое число				
Номер сети/нулевая подсеть				
Первая не нулевая подсеть				
Следующая подсеть				
Последняя подсеть				
Широковещательная подсеть				
Вне диапазона — используется процессом				

Формальный процесс поиска всех идентификаторов подсети, исходя из номера сети и единой маски подсети, имеет следующий вид.



Этапы формального процесса поиска всех идентификаторов подсети, когда битов подсети меньше 8

- Этап 1 В первом пустом ряду таблицы запишите маску подсети в десятичном формате.
- Этап 2 Выявите интересующий октет, который является единственным октетом маски со значением не 255 и не 0. Нарисуйте прямоугольник вокруг столбца интересующего октета.
- Этап 3 Вычислите и запишите магическое число при вычитании значения интересующего октета маски подсети из 256.
- Этап 4 В следующем пустом ряду перечня всех подсетей запишите номер классовый сети, совпадающий с номером нулевой подсети.
- Этап 5 Для поиска каждого последующего номера подсети:
 - а) Для трех не интересующих октетов скопируйте значения предыдущего номера подсети.
 - б) Для интересующего октета добавьте магическое число к интересующему октету предыдущего номера подсети.
- Этап 6 Как только сумма, вычисленная на этапе 5 б, будет равна 256, остановите процесс. Число 256 — вне диапазона, а предыдущий номер подсети — широковещательный адрес подсети.

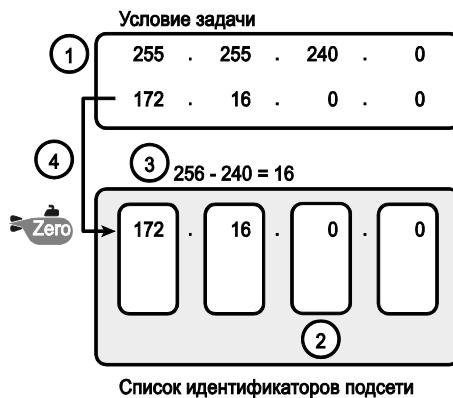
Хотя письменный процесс длинен, обладая практическим навыком, большинство людей смогут найти так ответы намного быстрее, чем при использовании двоичной математики. Как обычно, изучать этот процесс лучше на практике, а не только теоретически. Для этого выполните задания, просмотрите видеофильмы на прилагаемом к книге компакт-диске, а также рассмотрите дополнительные примеры на нем. Для большей практики можно также использовать приложение Find All Subnets с Subnet Prep (www.subnetprep.com).

Пример 1: сеть 172.16.0.0, маска 255.255.240.0

Вначале сосредоточимся на первых четырех из шести этапов, когда сеть 172.16.0.0 разделена на подсети маской 255.255.240.0. Результат этих первых четырех этапов приведен на рис. 18.2.

- Этап 1 Записываем маску 255.255.240.0, которая была дана в условии задачи. (На рис. 18.2, для справки, приведен также идентификатор сети 172.16.0.0.)

- Этап 2** Третий октет маски не 0 и не 255, что делает его интересующим.
- Этап 3** Поскольку значение маски в третьем октете 240, магическое число равно $256 - 240 = 16$.
- Этап 4** Поскольку идентификатор сети 172.16.0.0, первый идентификатор подсети (нулевая подсеть) также 172.16.0.0.



Легенда:

Zero - Нулевая подсеть

Рис. 18.2. Результат выполнения первых четырех этапов: 172.16.0.0, 255.255.240.0

На этих четырех первых этапах выясняется первая подсеть (нулевая), что позволяет осуществить остальные этапы, выявив интересующий октет и магическое число. Пятый этап процесса требует скопировать значения трех не интересующих октетов и добавить магическое число (в данном случае 16) к интересующему октету (в данном случае к октету 3). Повторяйте этот этап, пока значение интересующего октета не станет равно 256 (этап 6). Достигнув числа 256, вы имеете все идентификаторы подсети, а значение 256 вычеркните, так как оно является не корректным идентификатором подсети. Результат выполнения этих этапов приведен на рис. 18.3.

ПРИМЕЧАНИЕ АВТОРА

В любом списке всех идентификаторов подсети самый верхний ее идентификатор называется *широковещательной подсетью* (broadcast subnet). Несколько десятилетий назад инженеры избегали использования широковещательной подсети. Однако ее использование не вызывает проблем. Термин *широковещательная подсеть* возник благодаря тому факту, что широковещательный адрес подсети в широковещательной подсети совпадает с общесетевым широковещательным адресом.

ПРИМЕЧАНИЕ АВТОРА

Термины *широковещательная подсеть* и *широковещательный адрес подсети* иногда путают. *Широковещательная подсеть* (broadcast subnet) — это одна из подсетей, а именно самая старшая подсеть; в сети существует только одна такая подсеть. Термин *широковещательный адрес подсети* описывает один номер в каждой подсети, который в цифровом виде является самым старшим номером в этой подсети.



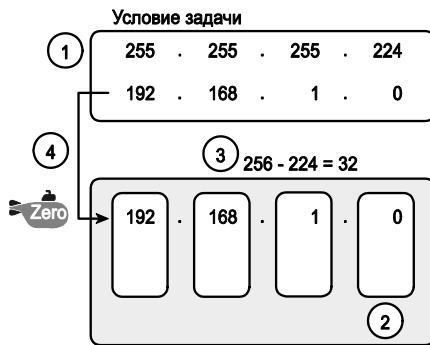
	5A	5A	5Б	5A
	Копия	Копия	Сумма	Копия
Zero	172	16	0	0
ID	172	16	16	0
ID	172	16	32	0
ID	172	16	48	0
ID	172	16	64	0
ID	172	16	240	0
ID	172	16	256	0
		6		

Рис. 18.3. Пример добавления магического числа к интересующему октету при поиске всех идентификаторов подсети

Пример 2: сеть 192.168.1.0, маска 255.255.255.224

В сети класса С с маской 255.255.255.224 интересующим октетом в данном примере является четвертый октет. Однако процесс тот же, с той же логикой, только применяется он к другому октету. Как и в предыдущем примере, следующий список содержит первые четыре этапа, а рис. 18.4 демонстрирует их результаты.

- Этап 1 Записываем маску 255.255.255.224, которая была дана в условии задачи, и дополнительно записываем номер сети (192.168.1.0).
- Этап 2 Четвертый октет маски не 0 и не 255, что делает его интересующим.
- Этап 3 Поскольку значение маски в четвертом октете 224, магическое число равно $256 - 224 = 32$.
- Этап 4 Поскольку идентификатор сети 192.168.1.0, первый идентификатор подсети (нулевая подсеть) также 192.168.1.0.



Список идентификаторов подсети

Легенда:

Zero Нулевая подсеть

Рис. 18.4. Результаты первых четырех этапов:
192.168.1.0, 255.255.255.224

Пятый этап процесса требует скопировать значения первых трех октетов, а затем добавить магическое число (в данном случае 32) к интересующему октету (в данном случае к октету 4). Повторяйте этот этап, пока значение интересующего октета не станет равно 256 (этап 6). Достигнув числа 256, вы имеете все идентификаторы подсети, а значение 256 вычеркните, так как оно является не корректным идентификатором подсети. Результат этих этапов приведен на рис. 18.5.

	5A Копия	5A Копия	5A Копия	5B Сумма
Zero	192	168	1	0
ID	192	168	1	+32 32
ID	192	168	1	+32 64
ID	192	168	1	+32 96
ID	192	168	1	+32 128
ID	192	168	1	+32 224
ID	192	168	1	+32 256
			6	

Рис. 18.5. Идентификаторы подсети:
192.168.1.0, 255.255.255.224

Поиск всех подсетей точно с 8 битами подсети

Формальный процесс в предыдущем разделе определял интересующий октет как октет, значение маски которого не равнялось ни 255, ни 0. Если маска определяет ровно 8 битов подсети, следует использовать совершенно другую логику выявления интересующего октета; в противном случае применяется тот же процесс. Фактически реальные идентификаторы подсети могут быть немного более интуитивно понятными.

Существуют только два случая с точно 8 битами подсети.

- Сеть класса А с маской 255.255.0.0; весь второй октет содержит биты подсети.
- Сеть класса В с маской 255.255.255.0; весь третий октет содержит биты подсети.

В любом случае используйте тот же процесс, что и с менее чем 8 битами подсети, но определите интересующий октет как содержащий биты подсети. Кроме того, поскольку значение маски 255, магическое число будет $256 - 255 = 1$, таким образом, последующий идентификатор подсети будет на единицу больше предыдущего.

Например, для 172.16.0.0 и маски 255.255.255.0 интересующий октет третий, а магическое число $256 - 255 = 1$. Начиная с нулевой подсети, равной по значению номеру сети 172.16.0.0, добавляйте далее 1 в третьем октете. Например, первые четыре подсети следующие:

- 172.16.0.0 (нулевая подсеть);
- 172.16.1.0;

- 172.16.2.0;
- 172.16.3.0.

Поиск всех подсетей с более чем 8 битами подсети

Выше, в разделе “Формальный процесс с менее чем 8 битами подсети”, для упрощения изучения подразумевалось наличие менее 8 битов подсети. В реальной жизни необходимо уметь найти все идентификаторы подсети при любой допустимой маске, поэтому нельзя полагать, что битов подсети окажется меньше 8.

В примерах, где битов подсети по крайней мере 9, есть как минимум 512 идентификаторов подсети, поэтому запись такого списка заняла бы слишком много времени. Для экономии места в примерах будут использоваться сокращения вместо перечисления сотен или тысяч идентификаторов подсети.

Процесс с менее чем 8 идентификаторами подсети подразумевает инкремент магического числа в одном октете. При более чем 8 битов подсети новый дополненный процесс подразумевает приращение в нескольких октетах. Поэтому в данном разделе описаны два общих случая: когда существует 9–16 битов подсети, подразумевающий, что поле подсети составляет только два октета; и случай с 17 или более битами подсети, подразумевающий поле подсети в трех октетах.

Процесс с 9–16 битами подсети

Чтобы понять процесс, необходимо ознакомиться с несколькими используемыми в нем терминами. На рис. 18.6 приведены подробности концепции на примере использования сети класса В 130.4.0.0 и маски 255.255.255.192. В нижней части приведена структура адресов по маске: часть сети из двух октетов, поскольку это адрес класса В, часть подсети на 10 битов по маске (/26) и 6 битов хоста.

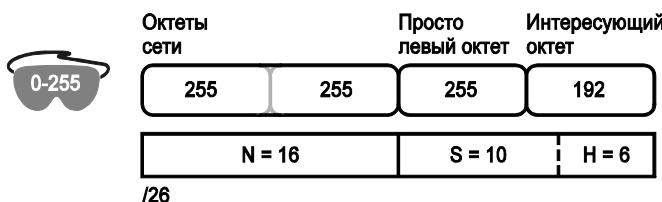


Рис. 18.6. Фундаментальные концепции и термины процесса с более чем 8 битами подсети

В данном случае биты подсети расположены в двух октетах: 3 и 4. Крайний правый из этих октетов — интересующий октет, а октет слева условно именуется *просто левым* (just-left) октетом.

Видоизмененный процесс предполагает приращение магического числа в интересующем октете и приращение на единицу в просто левом октете.

Формальные этапы поиска всех идентификаторов подсети, когда существует больше 8 битов подсети



- Этап 1** Вычислите идентификаторы подсети, используя процесс для 8 битов подсети или меньше. Когда сумма дойдет до значения 256, переходите к следующему этапу; считайте перечисленные идентификаторы подсети *блоком подсетей* (subnet block).

Этап 2 Скопируйте предыдущий блок подсетей, но добавьте 1 к просто левому октету во всех идентификаторах подсети нового блока.

Этап 3 Повторяйте этап 2 до тех пор, пока не создадите блок с просто левым октетом 255, а затем удалите его.

Честно говоря, формальная концепция может вызывать проблемы, если не практиковаться на примерах. Если процесс остается немного неясным, лучше рассмотрите следующие примеры вместо повторного чтения формального процесса.

Сначала рассмотрим пример на основании рис. 18.6, с сетью 130.4.0.0 и маской 255.255.255.192. Структура уже представлена на рис. 18.6, а на рис. 18.7 приведен блок идентификаторов подсети, созданный на этапе 1.

Блок подсети	Просто левый Интересующий			
	130.	4.	0.	0
	130.	4.	0.	64
	130.	4.	0.	128
	130.	4.	0.	192

Рис. 18.7. Этап 1: список первого блока идентификаторов подсети

Логика на этапе 1, подразумевающая создание блока из четырех идентификаторов подсети, следует тому же процессу с магическим числом, что и прежде. Первый идентификатор подсети, 130.4.0.0, является нулевой подсетью. Каждый из следующих трех идентификаторов подсети на 64 больше, поскольку магическое число в данном случае $256 - 192 = 64$.

Этапы 2 и 3 формального процесса демонстрируют, как создать 256 блоков подсетей. Сделав это, можно перечислить все 1024 идентификатора подсети. Для этого создайте 256 полных блоков подсети: один с 0 в просто левом октете, один с 1 в просто левом октете, далее с 2 в просто левом октете и так далее до 255. Процесс продолжается до тех пор, пока не будет создан блок подсетей со значением 255 в просто левом октете (в данном случае в третьем октете). На рис. 18.8 представлена концепция добавления в первых нескольких блоках подсетей.

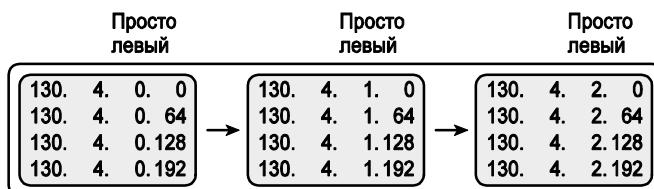


Рис. 18.8. Этап 2: репликация блока подсетей с добавлением единицы в просто левом октете

Этот пример с 10 полными битами подсети создает 256 блоков по 4 подсети в каждом для 1024 подсетей в общей сложности. Эта математика соответствует обычному методу подсчета подсетей, поскольку $2^{10} = 1024$.

Процесс с 17 и более битами подсети

Чтобы создать проект подсети, допускающей 17 и более битов подсети, следует использовать сеть класса А. Кроме того, часть подсети будет состоять из второго и третьего октетов полностью плюс часть четвертого октета. Это означает множество идентификаторов подсети: по крайней мере, 2^{17} (или 131 072) подсети. На рис. 18.9 приведен пример именно такой структуры с сетью класса А и маской /26.



Рис. 18.9. Структура адреса с 18 битами подсети

Для поиска всех идентификаторов подсети в этом примере используйте тот же общий процесс, что и с 9–16 битами подсети, но с большим количеством блоков подсетей. В действительности вы должны создать блоки подсетей для всех комбинаций значений (0–255 включительно) и во втором, и в третьем октете. Общее представление приведено на рис. 18.10. Обратите внимание: только при 2 битах подсети в четвертом октете в этом примере будет по четыре подсети в каждом блоке подсетей.

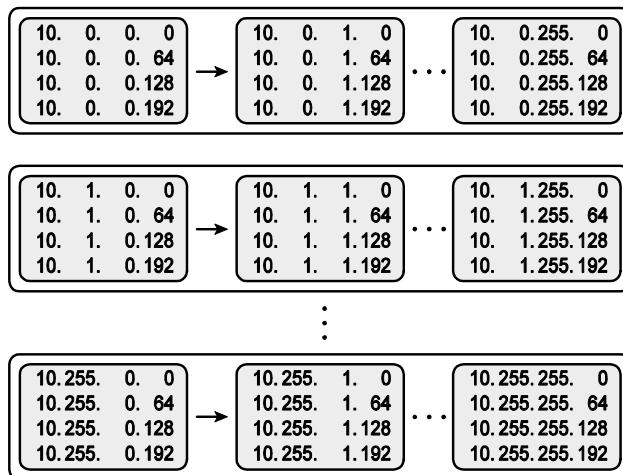


Рис. 18.10. 256 групп по 256 блоков из четырех подсетей

Практические задания по поиску всех идентификаторов подсети

Прежде чем перейти к следующей главе, попрактикуйтесь в процессах, обсуждаемых в данной главе, пока не станете получать правильные ответы почти всегда. Используйте любые средства по своему усмотрению и любое время. Затем можно продолжить чтение.

Перед сдачей экзамена потренируйтесь, чтобы овладеть темой данной главы полностью и отвечать достаточно быстро. Достижение разумной скорости решения задачи довольно трудно, поскольку одни комбинации идентификатора сети и маски могут давать сотни или тысячи подсетей, в то время как другие — значительно меньшие количества. Поэтому перед экзаменом следует быть в состоянии выявить первые четыре подсети, которые включают нулевую подсеть, за 45 секунд. Ключевые концепции и рекомендации такого двухэтапного подхода приведены в табл. 18.3.

Таблица 18.3. Продолжайте читать с учетом целей экзамена по темам данной главы

Период	Перед переходом к следующей главе	Перед сдачей экзамена
Сосредоточьтесь на ...	теме изучения	быть быстрым и правильным
Разрешенные средства	Все	Ваш мозг и блокнот
Цель: точность	90% правильных ответов	100% правильных ответов
Цель: скорость	Любая скорость	45 секунд

Практические задания этой главы

Вот список из трех заданий, где даны номер классовой сети и маска в префиксном стиле. Найдите все идентификаторы подсети для каждой задачи:

1. 192.168.9.0/27
2. 172.30.0.0/20
3. 10.0.0.0/17

Ответы даны ниже, в разделе “Ответы на приведенные ранее практические задания”.

Дополнительные практические задания

В этом разделе перечислены некоторые из возможностей для дополнительной практики.

- Приложение И, в котором содержатся дополнительные практические задания. Там же даны объяснения по поиску ответа к каждому заданию.
- Создайте собственные задания. Большинство калькуляторов подсети позволяют найти все идентификаторы подсети, когда вводят IP-адрес и маску. Поэтому запишите идентификатор сети и маску на бумаге, найдите ответ, а затем введите значения в калькулятор, чтобы проверить результат.
- Приложение Find All Subnets для iPhone на Subnet Prep (www.subnetprep.com) предоставляет обзорное видео, но что важнее всего, практические задания. Как обычно, оно позволяет изучить описанный здесь процесс и попрактиковаться, причем не привязываясь к какому-либо специальному процессу.
- Просмотрите видеофильмы на компакт-диске, демонстрирующие процессы, описанные в этой главе.

Подготовка к экзамену

Повторите все ключевые темы

Повторите все ключевые темы данной главы, помеченные пиктограммой “Ключевая тема”. Ключевые темы и соответствующие им страницы перечислены в табл. 18.4.

Таблица 18.4. Ключевые темы главы 18

Элемент	Описание	Страница
Список этапов	Этапы формального процесса поиска всех идентификаторов подсети, когда битов подсети меньше 8	473
Рис. 18.3	Пример добавления магического числа к интересующему октету при поиске всех идентификаторов подсети	475
Список этапов	Формальные этапы поиска всех идентификаторов подсети, когда существует больше 8 битов подсети	477

Ключевые термины

Дайте определения перечисленных ниже терминов и проверьте правильность их написания в списке терминов:

нулевая подсеть (zero subnet), подсеть нуль (subnet zero), широковещательная подсеть (broadcast subnet)

Ответы на приведенные ранее практические задания

В разделе “Практические задания этой главы” приведены три практических задания. Ответы расположены в таблицах ниже. После таблицы следуют примечания к каждому заданию.

Ответ на практическое задание 1

В первом задании дана сеть 192.168.9.0 и маска /27. Маска преобразуется в маску DDN 255.255.255.224. При использовании сети класса С имеется 24 бита сети и только 3 бита подсети, находящихся в четвертом октете. Таким образом, это случай с менее чем 8 битами подсети и четвертым интересующим октетом.

Для начала запишите нулевую подсеть, а затем начинайте добавлять магическое число в интересующий октет. Нулевая подсеть равна идентификатору сети (в данном случае 192.168.9.0). Магическое число, вычисленное как $256 - 224 = 32$, следует добавить к предыдущему интересующему октету идентификатора подсети. Результаты приведены в табл. 18.5.

Таблица 18.5. Перечень всех подсетей: 192.168.9.0/27

Октет	1	2	3	4
Маска	255	255	255	224
Магическое число				32
Номер сети/нулевая подсеть	192	168	9	0
Первая не нулевая подсеть	192	168	9	32

Окончание табл. 18.5

Октет	1	2	3	4
Следующая подсеть	192	168	9	64
Следующая подсеть	192	168	9	96
Следующая подсеть	192	168	9	128
Следующая подсеть	192	168	9	160
Следующая подсеть	192	168	9	192
Широковещательная подсеть	192	168	9	224
Вне диапазона — используется процессом	192	168	9	256

Ответ на практическое задание 2

Во втором задании дана сеть 172.30.0.0 и маска /20. Маска преобразуется в маску DDN 255.255.240.0. При использовании сети класса В имеется 16 битов сети и только 4 бита подсети, находящихся в третьем октете. Таким образом, это случай с менее чем 8 битами подсети и третьим интересующим октетом.

Для начала запишите нулевую подсеть, а затем начинайте добавлять магическое число в интересующий октет. Нулевая подсеть равна идентификатору сети (в данном случае 172.30.0.0). Магическое число, вычисленное как $256 - 240 = 16$, следует добавить к предыдущему интересующему октету идентификатора подсети. Результаты приведены в табл. 18.6.

Таблица 18.6. Перечень всех подсетей: 172.30.0.0/2

Октет	1	2	3	4
Маска	255	255	240	0
Магическое число			16	
Номер сети/нулевая подсеть	172	30	0	0
Первая не нулевая подсеть	172	30	16	0
Следующая подсеть	172	30	32	0
Следующая подсеть	172	30	48	0
Следующая подсеть	172	30	64	0
Следующая подсеть	172	30	Пропуск	0
			...	
Следующая подсеть	172	30	224	0
Широковещательная подсеть	172	30	240	0
Вне диапазона — используется процессом	172	30	256	0

Ответ на практическое задание 3

В третьем задании дана сеть 10.0.0.0 и маска /17. Маска преобразуется в маску DDN 255.255.128.0. При использовании сети класса А имеется 8 битов сети и 9 битов подсети. Интересующим является октет 3, только с 1 битом подсети в этом октете, а второй октет является просто левым октетом, с 8 битами подсети.

В данном случае начните с поиска первого блока подсетей. Магическое число $256 - 128 = 128$. Первая подсеть (нулевая) равна идентификатору сети. Таким образом, первый блок идентификаторов подсети выглядит так:

10.0.0.0
10.0.128.0

Затем создайте блок подсетей для всех 256 возможных значений в просто левом октете, или октете 2 в данном случае. Следующий список демонстрирует первые три блока идентификаторов подсети плюс последний блок идентификаторов подсети, а не перечень на целую страницу:

10.0.0.0 (нулевая подсеть)
10.0.128.0
10.1.0.0
10.1.128.0
10.2.0.0
10.2.128.0
...
10.255.0.0
10.255.128.0 (широковещательная подсеть)

В этой части рассмотрены следующие темы экзамена Cisco ICND1¹...

Реализация схемы IP-адресации и службы IP в небольшой сети филиала:

- описана работа службы DNS и методы ее проверки;
- рассказано, как с помощью диспетчера SDM включить технологию NAT в небольшой сети с одним провайдером услуг Интернета и проверить конфигурацию в интерфейсе командной строки с помощью команды ping;
- рассказано, как настроить службы DHCP и DNS маршрутизатора, а также проверить их работу и устранить неисправности (с помощью интерфейса CLI и диспетчера SDM);
- описано, как реализовать службы динамической и статической адресации в локальной сети;

Построение небольшой маршрутизируемой сети:

- описаны основные концепции маршрутизации, в том числе пересылка пакетов и процесс обнаружения маршрутов;
- описан принцип работы маршрутизаторов компании Cisco: процесс загрузки, процедура POST и компоненты устройства;
- описан процесс выбора правильной среды передачи данных, кабелей, портов и разъемов для подключения маршрутизаторов к другим сетевым устройствам и хостам;
- рассказало, как настроить протокол RIPv2, проверить и устранить неисправности;
- объяснено, как получить доступ к интерфейсу командной строки маршрутизатора и использовать его для настройки базовых параметров устройства;
- рассказано, как проверить конфигурацию маршрутизатора и работоспособность соединений с помощью команд ping, traceroute, Telnet, SSH и других утилит;
- рассказано, как настроить и проверить работу статических и стандартных маршрутов в устройствах;
- описано, как обращаться с конфигурационными файлами: копировать, редактировать, обновлять, восстанавливать;
- описано, как управлять операционной системой Cisco IOS;
- рассказало, как задать пароли и поддерживать физическую безопасность устройства;
- объяснено, как проверять состояние сети и маршрутизатора с помощью базовых утилит ping, traceroute, Telnet, SSH, ARP, ipconfig и команд групп show и debug.

Поиск угроз безопасности в сети и методы их устранения:

- описано, как находить недочеты системы безопасности, а также приведены рекомендации и методы повышения уровня защиты сетевых устройств.

¹ Текущие темы сертификационного экзамена приведены на сайте <http://www.cisco.com>. — Примеч. авт.

Часть IV. Маршрутизация IPv4

Глава 19. “Работа с маршрутизаторами компании Cisco”

Глава 20. “Концепции и конфигурирование протоколов маршрутизации”

Глава 21. “Поиск и устранение неисправностей маршрутизации”

В этой главе...

- **Установка маршрутизаторов Cisco.** Описаны маршрутизаторы корпоративного уровня и потребительского сегмента, а также рассказано, как такие устройства используются для подключения пользователей к сети.
- **Интерфейс командной строки маршрутизатора.** Описаны схожие элементы и методы интерфейса командной строки маршрутизатора и коммутатора (первая часть описания представлена в главе 8), а также рассмотрены функции, характерные только для маршрутизаторов.
- **Обновление операционной системы Cisco IOS и процесс начальной загрузки устройства.** Описан процесс начального запуска маршрутизатора и рассмотрен алгоритм выбора источника загрузки операционной системы Cisco IOS.

Работа с маршрутизаторами компании Cisco

Маршрутизаторы отличаются от коммутаторов, прежде всего, своими основными функциями. Самая главная задача коммутатора — пересыпать фреймы Ethernet, сравнивая MAC-адрес получателя с таблицей MAC-адресов (т.е. таблицей коммутации) устройства; основная же задача маршрутизатора — пересыпать пакеты, сравнивая IP-адрес получателя со своей таблицей маршрутизации IP. В современных коммутаторах Ethernet есть один или несколько различных типов интерфейсов Ethernet, в маршрутизаторах же есть как интерфейсы Ethernet и WAN, так и многие другие типы портов, позволяющие подключиться к телекоммуникационной инфраструктуре через телевизионный кабель, по цифровой абонентской линии и технологии DSL, а также многие другие, позволяющие получить доступ к Интернету. Итак, маршрутизаторы могут работать с очень большим количеством технологий и различных сред передачи данных, а коммутаторы рассчитаны на передачу фреймов Ethernet между устройствами Ethernet только в локальных сетях. Несмотря на то что оба типа устройств предназначены для пересылки данных, алгоритмы и процессы пересылки, а также тип устройств, которым могут быть переданы потоки данных, существенно отличаются.

И хотя базовые функции устройств существенно различаются, тем не менее в коммутаторах и маршрутизаторах компании Cisco используется один и тот же интерфейс командной строки. В этой главе подробно рассмотрены функции интерфейса маршрутизаторов, которые отличаются от функций интерфейса командной строки коммутаторов, рассмотренных, в частности, в главе 8. В последнем разделе подробно описана установка маршрутизаторов компании Cisco, а также рассмотрен процесс начальной загрузки операционной системы IOS.

Контрольные вопросы: знаете ли вы уже темы главы

Этот раздел предназначен для того, чтобы читатель мог предварительно оценить свои знания и решить, нужно ли ему читать главу целиком. Если ответы на девять из десяти вопросов даны правильно, можно сразу же перейти к последнему разделу “Подготовка к экзамену”. Основные темы этой главы и предварительных контрольных вопросов перечислены в табл. 19.1. Отвечая на контрольные вопросы и используя таблицу, читатель сможет достаточно точно определить свои знания в той или иной области. Ответы на вопросы приведены в приложении А.

Таблица 19.1. Темы контрольных вопросов

Основная тема	Номера вопросов
Установка маршрутизаторов Cisco	1, 2
Интерфейс командной строки маршрутизатора	3–7
Обновление операционной системы Cisco IOS и процесс начальной загрузки устройства	8, 9

1. Какие этапы при установке устройства присущи маршрутизаторам компании Cisco, но отсутствуют у коммутаторов? (Выберите несколько ответов.)
 - а) Подключение кабелей Ethernet.
 - б) Подключение последовательных (serial) кабелей.
 - в) Подключение к консольному порту.
 - г) Подключение питания.
 - д) Переключение выключателя устройства в положение “включен”.
2. В какой из следующих ролей обычно выступает маршрутизатор SOHO с точки зрения присвоения IP-адресов? (Выберите несколько ответов.)
 - а) Сервер DHCP на интерфейсе, подключенном к провайдеру.
 - б) Сервер DHCP на интерфейсе, к которому подключен домашний ПК или офисные ПК.
 - в) Клиент DHCP на интерфейсе, подключенном к провайдеру.
 - г) Клиент DHCP на интерфейсе, к которому подключен домашний ПК или офисные ПК.
3. Какую из указанных ниже команд можно встретить в интерфейсе командной строки маршрутизатора, но не коммутатора?
 - а) Команда `clock rate`.
 - б) Команда `ip address` маска адрес.
 - в) Команда `ip address dhcp`.
 - г) Команда `interface vlan 1`.
4. Ваша компания только что приобрела два маршрутизатора компании Cisco для использования на лабораторном стенде. Устройства подключены к разным сегментам локальной сети интерфейсами `Fa0/0`, а последовательные интерфейсы (serial) подключены друг к другу напрямую. Какие из указанных ниже действий не нужно выполнять, чтобы обеспечить передачу пакетов IP? (Выберите несколько ответов.)
 - а) Настроить IP-адреса на интерфейсах FastEthernet и последовательных интерфейсах обоих маршрутизаторов.
 - б) Настроить команду `bandwidth` на последовательном интерфейсе для одного маршрутизатора.
 - в) Настроить команду `clock rate` на последовательном интерфейсе одного маршрутизатора.
 - г) Задать с помощью команды `description` описание на нужных интерфейсах FastEthernet и последовательных интерфейсах обоих маршрутизаторов.

5. Вывод команды `show ip interface brief` маршрутизатора показывает коды состояний “выключено” (“down” и “down”) для интерфейса Serial 0/0. В чем может заключаться причина?
- а) В данном интерфейсе введена команда `shutdown`.
 - б) В интерфейсе маршрутизатора было задано использование технологии Frame Relay, но на другом конце канала используется инкапсуляция PPP.
 - в) В соответствующий последовательный интерфейс не включен последовательный кабель.
 - г) Оба маршрутизатора на концах канала подключены к работающей среде передачи данных (через модуль CSU/DSU), но только на одном из них установлен IP-адрес.
6. Какая из указанных ниже команд не покажет настройки IP-адресов и масок в устройстве? (Выберите несколько ответов.)
- а) `show running-config`.
 - б) `show protocols тип номер`.
 - в) `show ip interface brief`.
 - г) `show interfaces`.
 - д) `show version`.
7. Чем отличаются интерфейсы командной строки маршрутизатора и коммутатора компании Cisco? (Выберите несколько ответов.)
- а) Командами для конфигурирования простой процедуры проверки паролей для консоли.
 - б) Количество заданных IP-адресов.
 - в) Типом вопросов, задаваемых в режиме начальной конфигурации устройства (`setup mode`).
 - г) Заданием имени хоста (`hostname`).
 - д) Заданием описаний для интерфейсов.
8. С помощью какой из указанных команд можно изменить источник загрузки операционной системы Cisco IOS? (Выберите несколько ответов.)
- а) Команды `reload`.
 - б) Команды `boot`.
 - в) Команды `reboot`.
 - г) Команды конфигурирования `boot system`.
 - д) Команды конфигурирования `reboot system`.
 - е) Сменой значения в конфигурационном регистре.
9. Какое шестнадцатеричное значение в последнем знаке конфигурационного регистра укажет маршрутизатору, что не нужно искать операционную систему Cisco IOS во флеш-памяти?
- а) 0. в) 4. д) 6.
 - б) 2. г) 5.

Основные темы

Установка маршрутизаторов Cisco

Маршрутизаторы обеспечивают работу основной службы сетевого уровня (эталонной модели) — пересылку пакетов через сеть в сквозном режиме. Как пояснялось в главе 5, маршрутизаторы пересыпают пакеты через различные физические сетевые соединения, например, каналы Ethernet, последовательные каналы, среду Frame Relay, а также используют алгоритмы уровня 3 для принятия решения о том, куда именно следует отправить каждый пакет. В качестве напоминания отметим, что в главе 3 были описаны физические соединения с сетью Ethernet, а в главе 4 рассмотрены технологии WAN и их кабельные подключения.

В первом разделе главы описаны подробности процесса установки маршрутизатора, сначала с точки зрения его развертывания в корпоративной сети, а потом — для подключения *малых и домашних офисов* (Small Office/Home Office — SOHO) к провайдеру Интернета с использованием высокоскоростных технологий абонентских каналов.

Установка маршрутизатора в корпоративной сети

В типичной сети крупного предприятия есть несколько централизованных *площадок* (site) и несколько небольших дистанционных филиалов. Для подключения устройств (компьютеров, IP-телефонов, принтеров и др.) на каждой площадке есть как минимум один коммутатор локальной сети. Кроме того, в сети каждой площадки должен присутствовать как минимум один маршрутизатор, с помощью которого локальная сеть (LAN) будет подключена к распределенной сети (WAN). Канал WAN в такой структуре используется для подключения дистанционных площадок к центральному офису и для других телекоммуникационных нужд.

На рис. 19.1 проиллюстрирована одна из возможных схем распределенной корпоративной сети, в частности, слева показана сеть филиала, в которой есть маршрутизатор, некоторое количество персональных компьютеров и условная сеть Ethernet (коммутатор на схеме опущен). Центральная площадка компании, показанная справа, построена практически на тех же компонентах, а между площадками используется двухточечный телекоммуникационный канал. В центральном офисе компании также есть *ферма серверов* (server farm) с двумя корпоративными серверами, хранящими некоторые данные.

На рис. 19.1 преднамеренно опущены некоторые детали, чтобы можно было подчеркнуть самые важные составляющие современной сети. На рис. 19.2 показана та же сеть, но более детально, вплоть до того, что показаны элементы кабельной системы.

На рис. 19.2 указаны как используемые схемы расположения выводов кабелей для локальных сетей (кабели UTP), так и два варианта подключения к сети WAN. В локальной сети преимущественно используются кабели с прямой распайкой контактов (так называемые прямые кабели), за исключением кабеля, соединяющего два коммутатора, для которого используется *перекрещенная* (crossover) распайка контактов.

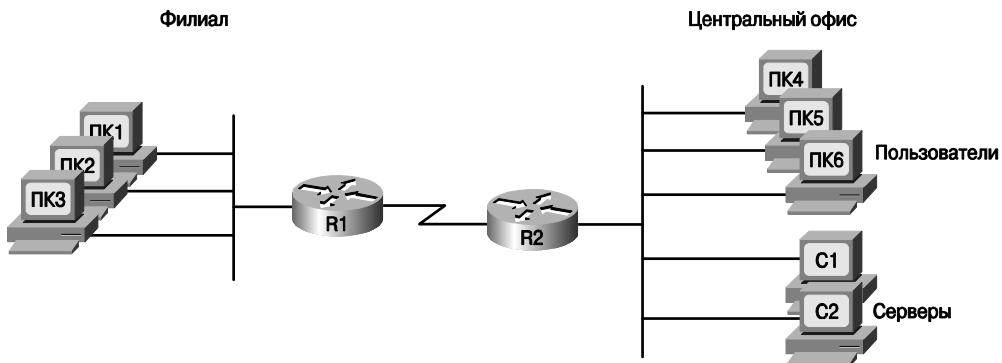


Рис. 19.1. Обобщенная схема корпоративной сети

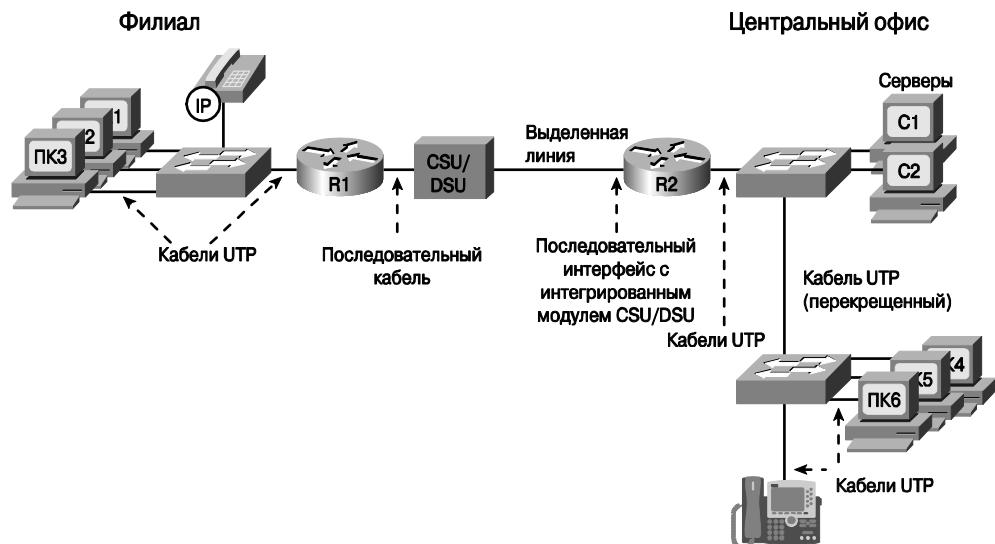


Рис. 19.2. Подробная схема корпоративной сети

Для последовательного канала показаны два возможных метода подключения с различными вариантами аппаратной реализации модуля *обслуживания канала/модуля обработки данных* (Channel Service Unit/Digital Service Unit — CSU/DSU): с установкой отдельного аппаратного модуля (такой вариант используется в филиале) и с использованием интегрированного в последовательный интерфейс маршрутизатора модуля (такой вариант используется в центральном офисе). В современном оборудовании модуль CSU/DSU обычно интегрирован в последовательный интерфейс маршрутизатора. Кабель WAN от оператора связи или поставщика услуг обычно заканчивается разъемом RJ-48, который по форме и размеру совпадает с разъемом RJ-45. Такой кабель включают в модуль CSU/DSU, а в рассмотренной схеме в центральном офисе он включен непосредственно в маршрутизатор главной площадки. Соответственно в филиале кабель включен в модуль CSU/DSU, а сам модуль подключен к последовательному интерфейсу маршрутизатора. (Последовательные кабели WAN показаны на рис. 4.4 главы 4.)

Маршрутизаторы с интегрированными службами компании Cisco

Производители сетевого оборудования, в том числе и компания Cisco, обычно выпускают несколько различных вариантов маршрутизаторов, как устройств, которые могут только маршрутизировать, так и устройств, которые могут выполнять многие другие функции. Типичному филиалу предприятия маршрутизатор нужен, прежде всего, для подключения локальной сети к распределенной, а коммутатор понадобится для построения высокоскоростной локальной сети и подключения к маршрутизатору. Во многих организациях на сегодняшний день используется технология *передачи голоса по сети IP* (Voice over IP — VoIP), кроме того, практически любому офису понадобятся базовые средства обеспечения безопасности. (Одна из наиболее популярных служб, связанная с безопасностью, а именно технология *виртуальной частной сети* (Virtual Private Network — VPN), описана в главе 6.) Вместо установки нескольких независимых устройств на одной площадке компания Cisco предлагает использовать устройства, которые могут работать одновременно и как маршрутизатор, и как коммутатор (рис. 19.2), а также обеспечивать дополнительные функции.

Развивая такую концепцию, компания Cisco производит несколько модельных серий маршрутизаторов, которые кроме маршрутизации могут выполнять также множество функций. У компании Cisco есть несколько серий маршрутизаторов, которые называют *маршрутизаторами с интегрированными службами* (Integrated Services Router — ISR), чтобы подчеркнуть тот факт, что множество служб интегрировано в одном устройстве. Если читатель никогда не видел маршрутизатор компании Cisco “вживую”, он может зайти на веб-сайт <http://www.cisco.com/go/isr> и посмотреть трехмерные демонстрации оборудования и сопутствующие им презентации для всех моделей маршрутизаторов ISR. Тем не менее для упрощения материала и повышения эффективности обучения в курсах и экзаменах CCNA маршрутизаторы и коммутаторы компании Cisco рассматриваются только как отдельные устройства, что облегчает понимание базовых технологий.

На рис. 19.3 показаны две фотографии, позаимствованные из интерактивной демонстрации маршрутизатора Cisco 1841 ISR, а также выделены некоторые важные компоненты. В верхней части рис. 19.3 показана фотография задней панели маршрутизатора, а в нижней — увеличенный фрагмент задней панели, на котором можно подробно рассмотреть интерфейсы FastEthernet, консольный и дополнительный (auxiliary — aux) порты, а также плату последовательного интерфейса со встроенным модулем CSU/DSU. (Полную презентацию, из которой были взяты фотографии, можно просмотреть на веб-сайте, указанном выше.)

Физическая установка устройства

Представляя себе типичную топологию корпоративной сети (см. рис. 19.2), порты и компоненты маршрутизатора (см. рис. 19.3), можно приступить к физической установке устройства. Этапы установки перечислены ниже.



Этапы установки маршрутизатора

- Этап 1 Подключите кабели локальной сети к портам LAN устройства.
- Этап 2 Если используется внешний модуль CSU/DSU, подключите последовательный интерфейс маршрутизатора к модулю, а сам модуль — к линии от телекоммуникационной компании.

- Этап 3** Если используется встроенный модуль CSU/DSU, подключите последовательный интерфейс маршрутизатора к линии от телекоммуникационной компании.
- Этап 4** Подключите консольный порт маршрутизатора к персональному компьютеру (с помощью *обратного (rollover)* кабеля, т.е. консольного).
- Этап 5** Подключите кабель питания к разъему питания устройства и настенной розетке.
- Этап 6** Включите питание маршрутизатора.

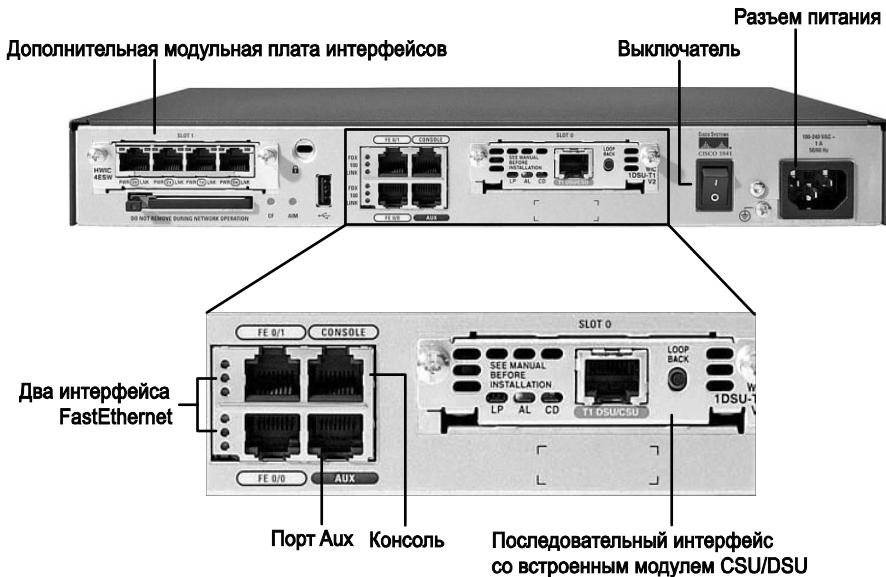


Рис. 19.3. Маршрутизатор Cisco модели 1841 ISR

Следует отметить, что указанные этапы установки практически полностью соответствуют этапам физической установки коммутатора локальных сетей: к его интерфейсам тоже нужно подключить кабели локальной сети и консольный порт, включить и проверить питание. Тем не менее есть одно отличие: в большинстве коммутаторов Catalyst компании Cisco нет выключателя питания, и как только устройство включено в розетку, оно сразу начинает загружать операционную систему и работать, а в маршрутизаторах такой выключатель есть.

Установка маршрутизатора доступа к сети

Маршрутизаторы играют ключевую роль в сетях SOHO, поскольку они соединяют подключенные к локальной сети устройства пользователей с высокоскоростной службой доступа к Интернету. Она может быть использована в малых и домашних сетях для доступа к центральной корпоративной сети, компании или учебного заведения.

Точно так же как и на рынке оборудования корпоративного уровня, производители в этом сегменте также стараются производить и продавать многофункциональные устройства. Тем не менее в курсе CCNA для упрощения понимания материала функции устройств разделены и разнесены по разным устройствам. Следуя такому подходу, ниже будут использоваться разные устройства для разных функций, а по-

том будет описана реальная ситуация, в которой разные функции интегрированы в одно устройство, и показан пример его использования.

Развертывание сети SOHO с отдельным коммутатором, маршрутизатором и кабельным модемом

На рис. 19.4 показана схема сети, а также устройства и кабели, использующиеся для подключения сети SOHO к Интернету через высокоскоростную службу передачи данных *кабельного телевидения* (Cable TV — CATV). Следует отметить, что в схеме сети показан один вариант использования сетевых устройств и кабелей, хотя на самом деле их множество.

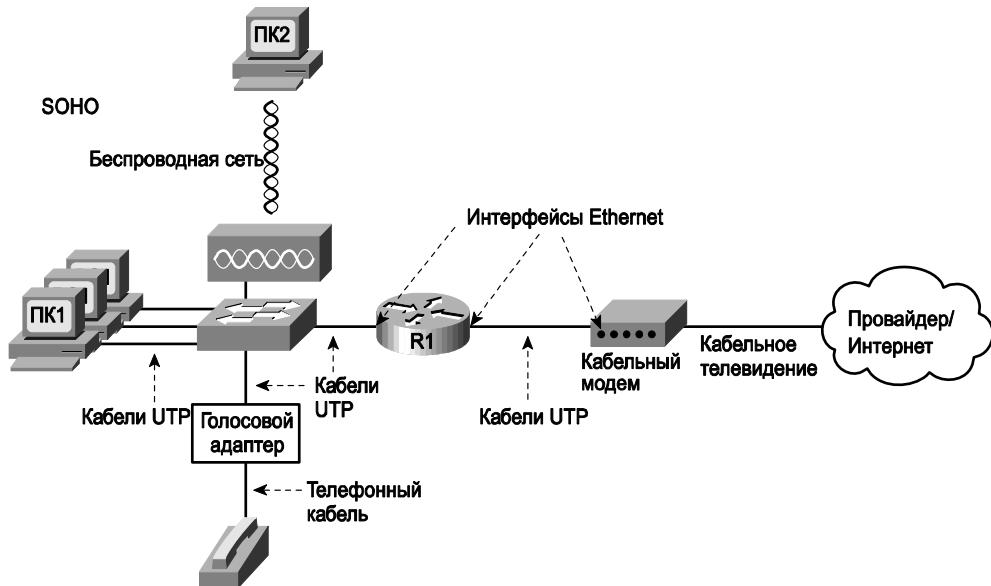


Рис. 19.4. Устройства сети SOHO и высокоскоростная служба передачи данных через канал кабельного телевидения

Схема сети на рис. 19.4 очень похожа на схему сети на рис. 19.2, на котором показан типичный дизайн сети и подключения офиса филиала крупного предприятия. Пользовательские рабочие станции подключены к коммутатору, а коммутатор подключен к интерфейсу Ethernet маршрутизатора. Маршрутизатор выполняет функции маршрутизации, преобразования и пересылки пакетов IP. Немного отличается реализация голосовых служб на двух схемах, в основном потому, что на рис. 19.4 показано типичное домашнее подключение к службам Интернета, а дома обычно есть аналоговая телефонная служба и опционально может использоваться адаптер для преобразования голоса и передачи его по пакетной сети IP.

Основное отличие между сетью SOHO, показанной на рис. 19.4, и инфраструктурой филиала предприятия (см. рис. 19.2) заключается в разных методах подключения к Интернету. Для канала Интернета, в котором используется инфраструктура кабельного телевидения или технология DSL, понадобится устройство, осуществляющее преобразование технологий и стандартов 1 и 2 уровней канала поставщика

услуг в среду Ethernet, к которой подключается маршрутизатор. Такие устройства-преобразователи называют *кабельными модемами* (cable modem) и *модемами DSL* (DSL modem) соответственно.

Несмотря на то что принципы работы и детали кабельных модемов и модемов DSL существенно отличаются, они являются аналогами модулей CSU/DSU для последовательного интерфейса. Модуль CSU/DSU осуществляет преобразование сигнала и стандартов уровня 1 канала WAN оператора связи или телефонной компании в стандарт последовательного интерфейса маршрутизатора. Аналогично кабельный модем преобразует сигналы формата кабельного телевидения (т.е. стандарты уровня 1 и 2) в формат, приемлемый для маршрутизатора, например Ethernet. Модем DSL, соответственно, конвертирует сигналы формата DSL для абонентского телефонного канала в стандарт Ethernet.

Чтобы осуществить физическую установку сети SOHO и развернуть в ней устройства (см. рис. 19.4), понадобятся соответствующие кабели UTP для соединений Ethernet и кабельный выход оператора кабельного телевидения или телефонная линия (для канала DSL). Обратите внимание: маршрутизатору в таком случае достаточно всего двух интерфейсов Ethernet: один нужен для подключения коммутатора локальной сети, а второй — для модема. Этапы установки сети SOHO перечислены ниже.

- Этап 1** Соедините прямым (straight-through) кабелем UTP коммутатор и маршрутизатор.
- Этап 2** Соедините прямым кабелем UTP модем и маршрутизатор.
- Этап 3** Подключите консольный порт маршрутизатора к персональному компьютеру с помощью консольного кабеля.
- Этап 4** Подключите кабель питания к разъему питания устройства и настенной розетке.
- Этап 5** Включите питание маршрутизатора.

Развертывание сети SOHO с интегрированными в одном устройстве коммутатором, маршрутизатором и кабельным модемом

В современных сетях SOHO обычно используются так называемые интегрированные устройства, т.е. устройства, объединяющие в себе несколько функций, а не отдельные коммутаторы, маршрутизаторы и тому подобное, показанные на рис. 19.4. Фактически современные маршрутизаторы для сетей SOHO объединяют в себе сразу несколько устройств:

- маршрутизатор;
- коммутатор;
- кабельный или модем DSL;
- голосовой адаптер;
- беспроводную точку доступа;
- аппаратный модуль шифрования трафика.

В экзамене CCNA, как уже не раз упоминалось выше, основной упор делается на независимые устройства, чтобы облегчить понимание и обучение. Тем не менее современная сеть SOHO обычно выглядит так, как показано на рис. 19.5.



Рис. 19.5. Сеть SOHO с интегрированным устройством и подключением к оператору кабельного телевидения

Устройства SOHO, описываемые в этой книге

Компания Cisco производит как устройства корпоративного уровня, так и сетевое оборудование уровня конечного потребителя. Устройства потребительского класса производятся под маркой Linksys. Такие маршрутизаторы, коммутаторы, точки доступа можно легко купить в Интернете и магазинах офисной техники. Устройства корпоративного уровня компания Cisco продает непосредственно крупным потребителям или через своих сертифицированных поставщиков и партнеров (Cisco Channel Partners). Следует помнить, что в экзамене CCNA не встречаются вопросы и задания, касающиеся устройств потребительского класса, т.е. продуктов Linksys, и методов их настройки через встроенный веб-интерфейс, а основной упор делается на интерфейс командной строки операционной системы IOS, используемой в маршрутизаторах корпоративного уровня.

Интерфейс командной строки маршрутизатора

В маршрутизаторах компании Cisco используется тот же интерфейс командной строки, что и в коммутаторах, который был описан в главе 8. Тем не менее функции маршрутизаторов и коммутаторов в сети различаются, что накладывает свой отпечаток и на команды интерфейса. В этом разделе сначала описаны наиболее важные настройки, которые одинаково выглядят как в маршрутизаторах, так и в коммутаторах, а также команды, которые в обоих типах устройств отличаются.

Сравнение интерфейса командной строки маршрутизатора и коммутатора

Ниже перечислены элементы конфигурации устройства, описанные в главе 8, которые в командной строке маршрутизатора и коммутатора выглядят абсолютно оди-

наково. Если читатель не очень хорошо помнит, как при помощи команд настраиваются разные функции, можно вернуться назад и просмотреть соответствующую главу еще раз.

Однаково выглядят следующие команды настройки и компоненты интерфейса командной строки маршрутизаторов и коммутаторов:

Однаковые команды и настройки интерфейса командной строки маршрутизатора и коммутатора



- режим обычного и привилегированного (enable) пользователей;
- команды переключения в режимы конфигурирования и команды выхода из него, в том числе команды `configure terminal`, `end`, `exit` и комбинация клавиш `<Ctrl+z>`;
- конфигурирование консольного, привилегированного паролей и аутентификации сеансов Telnet;
- конфигурирование ключей шифрования протокола SSH, настройка имен и паролей пользователей;
- задание имени хоста (`hostname`) устройства и описаний для интерфейсов;
- настройки интерфейсов Ethernet, автоматическое определение параметров, а также команды `speed` и `duplex`;
- команды выключения (`shutdown`) и включения (`no shutdown`) интерфейсов;
- переключение из одних режимов конфигурирования в другие с помощью таких команд, как `line console 0` и `interface`;
- функция встроенной интерактивной подсказки командной строки, а также методы и клавиши повторного вызова команд;
- функции различных конфигурационных файлов: `startup-config` в памяти NVRAM, `running-config` в оперативной памяти (RAM); взаимодействие с внешними хранилищами, например сервером TFTP; а также принципы использования команды `copy` для перемещения конфигурационных файлов и образов операционной системы Cisco IOS;
- методы запуска интерактивного диалога начального конфигурирования устройства (`setup`) через перезагрузку коммутатора или маршрутизатора с предварительным удалением начальной конфигурации `startup-config` или с помощью команды `setup`.

На первый взгляд может показаться, что все важные команды уже были описаны в главе 8, и это действительно так — многие команды начального конфигурирования устройства там были рассмотрены подробно. Тем не менее некоторые службы и функции работают в коммутаторах и маршрутизаторах совсем по-разному, а именно:

Команды и настройки (см. главу 8), которые отличаются в маршрутизаторах и коммутаторах



- несколько отличается конфигурирование IP-адресов;
- отличаются вопросы диалога начального конфигурирования устройства;

- в маршрутизаторах есть специальный дополнительный порт (Auxiliary — AUX), предназначенный для подключения внешнего модема и телефонной линии, чтобы была возможность получить дистанционный доступ к командной строке устройства через телефонную сеть.

Кроме трех указанных выше моментов, коммутаторы и маршрутизаторы отличаются по своим функциям, следовательно, отличаются команды в интерфейсе командной строке. В примере 10.5 главы 10 был показан результат выполнения команды `show mac address-table dynamic`, в котором приведена наиболее важная с точки зрения коммутатора информация, связанная с пересылкой фреймов. В операционной системе IOS маршрутизаторов такой команды нет, зато есть команда `show ip route`, выводящая известные устройству маршруты, которые с точки зрения маршрутизатора являются наиболее важной для него информацией, поскольку таблица маршрутов используется устройством для пересылки пакетов. Вполне очевидно, что коммутаторы второго уровня, рассматриваемые в курсе CCNA, не поддерживают команду `show ip route`, так как они не выполняют маршрутизацию IP.

В оставшейся части раздела будут описаны различия между интерфейсами командной строки маршрутизатора и коммутатора. В главе 20 будет продолжено рассмотрение отличий маршрутизаторов и коммутаторов, в частности, речь пойдет о том, как настроить маршрутизацию IP в устройствах. В текущей главе основное внимание будет уделено следующим компонентам:

- интерфейсам маршрутизатора;
- настройке IP-адреса маршрутизатора;
- диалогу начального конфигурирования маршрутизатора.

Интерфейсы маршрутизатора

Для специалиста уровня CCNA нужно хорошо знать и понимать принцип работы, а также конфигурирование двух типов интерфейсов маршрутизаторов: интерфейсов Ethernet и последовательных (serial) интерфейсов. Под термином *интерфейс Ethernet* в данном случае понимают любой тип технологии Ethernet. Однако следует помнить, что в команде `interface` указывается по максимальной скорости, на которой он может работать. Например, если в маршрутизаторе есть интерфейс Ethernet, который может работать только на скорости 10 Мбит/с, будет использоваться команда `interface ethernet номер` в режиме глобального конфигурирования устройства. Если же в маршрутизаторе есть интерфейс, который может работать на максимальной скорости в 100 Мбит/с, даже несмотря на то, что за счет автоопределения характеристик может быть выставлена как скорость 10, так и 100 Мбит/с, в конфигурации устройства такой интерфейс указывается по наибольшей скорости, т.е. командой `interface fastethernet номер`. Аналогично, если порт поддерживает стандарт Gigabit Ethernet и работает на гигабитовых скоростях, то он указывается командой `interface gigabitethernet номер`.

Последовательные порты — это второй наиболее распространенный тип интерфейсов маршрутизатора. Как уже отмечалось в главе 4, двухточечные выделенные линии, каналы Frame Relay и некоторые другие соединения используют одни и те же стандарты уровня 1. Такие стандарты реализованы в последовательных интерфейсах маршрутизаторов компании Cisco. В задачу сетевого инженера обычно входит выбор

используемой технологии канального уровня: *высокоуровневый протокол управления каналом* (High-Level Data Link Control — HDLC), *протокол двухточечного соединения* (Point-to-Point Protocol — PPP) для выделенных линий либо инкапсуляцию Frame Relay для доступа к среде Frame Relay, а впоследствии инженеру нужно правильно настроить выбранную технологию. (Следует помнить, что обычно на последовательных интерфейсах маршрутизаторов компании Cisco установлена инкапсуляция HDLC в качестве технологии канального уровня.)

В маршрутизаторах используются числовые идентификаторы для различия интерфейсов одного и того же типа. В маршрутизаторах интерфейс может быть обозначен одним числом, двумя числами через косую черту и тремя числами, разделенными косой чертой. Например, три указанные ниже варианта конфигурационных команд можно встретить в разных моделях маршрутизаторов компании Cisco.

```
interface ethernet 0
interface fastEthernet 0/1
interface serial 1/0/1
```

Получить важную информацию об интерфейсах можно с помощью нескольких команд, например, их краткий список можно отобразить с помощью команды `show ip interface brief`. Краткую информацию по определенному интерфейсу можно получить с помощью команды `show protocols тип номер` (следует помнить, что эта команда доступна не во всех версиях операционной системы Cisco IOS). Подробную информацию и множество деталей об интерфейсе, в том числе статистику входящих и исходящих пакетов, можно узнать с помощью команды `show interfaces`. Опционально во многих таких командах можно указать тип и номер интерфейса, например `show interfaces тип номер`, и просмотреть всю информацию только по какому-либо конкретному порту. В примере 19.1 показаны результаты выполнения перечисленных выше команд.

Пример 19.1. Получение информации об интерфейсах маршрутизатора

```
Albuquerque#show ip interface brief
Interface          IP-Address  OK? Method      Status           Protocol
FastEthernet0/0    unassigned   YES  unset      up              up
FastEthernet0/1    unassigned   YES  unset      administratively down  down
Serial0/0/0        unassigned   YES  unset      administratively down  down
Serial0/0/1        unassigned   YES  unset      up              up
Serial0/1/0        unassigned   YES  unset      up              up
Serial0/1/1        unassigned   YES  unset      administratively down  down
Albuquerque#show protocols fa0/0
FastEthernet0/0 is up, line protocol is up
Albuquerque#show interfaces s0/1/0
Serial0/1/0 is up, line protocol is up
Hardware is GT96K Serial
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)
CRC checking enabled
Last input 00:00:03, output 00:00:01, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: weighted fair
```

```

Output queue: 0/1000/64/0 (size/max total/threshold/drops)
  Conversations 0/1/256 (active/max active/max total)
  Reserved Conversations 0/0 (allocated/max allocated)
  Available Bandwidth 1158 kilobits/sec
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
  70 packets input, 6979 bytes, 0 no buffer
  Received 70 broadcasts, 0 runts, 0 giants, 0 throttles
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
  36 packets output, 4557 bytes, 0 underruns
  0 output errors, 0 collisions, 8 interface resets
  0 output buffer failures, 0 output buffers swapped out
  13 carrier transitions
  DCD=up  DSR=up  DTR=up  RTS=up  CTS=up

```

ВНИМАНИЕ!

Команды для работы с интерфейсами можно значительно сократить. Например, запись `sh int fa0/0` является полным аналогом команды `show interfaces fastethernet 0/0`. Зачастую, заглядывая через чье-то плечо, инженеры говорят что-либо похожее на фразу “Покажи-ка мне `show int F-A` и т.д.”, а не пытаются произнести полный вариант команды.

Коды состояний интерфейсов

Каждая из команд в примере 19.1 выводит два *кода состояния интерфейса*. Если в обоих кодах указано слово “*up*”, значит, интерфейс работает и маршрутизатор может передавать через него пакеты. Первый код состояния относится к уровню 1, а второй обычно (но не всегда) указывает состояние протокола канального уровня. В табл. 19.2 описаны два кода состояний и их значение.



Таблица 19.2. Коды состояния интерфейсов и их значение

Название	Местоположение	Значение
Состояние линии	Первый код состояния	Описывает состояние уровня 1, например, подключен ли кабель, правильный ли это кабель, включено ли питание устройства на другом конце канала
Состояние протокола	Второй код состояния	Описывает состояние уровня 2. В этом поле всегда выдается слово “ <i>down</i> ”, если не работает первый уровень (его состояние — “ <i>down</i> ”). Если код состояния линии равен “ <i>up</i> ”, состояние протокола, равное “ <i>down</i> ”, обычно означает ошибки в конфигурировании протокола канального уровня

Существуют четыре комбинации значений в кодах состояний, которые нужно четко различать для успешного поиска и устранения неисправностей в сетях. В табл. 19.3 перечислены как сами комбинации, так и приведено их объяснение и описание возможных причин такого состояния. Обратите внимание на то, что если состояние линии не равно “*up*” (первый код состояния), то второй код всегда будет установлен в состояние “*down*”, поскольку канальный уровень не может функционировать, если есть проблемы на физическом уровне.

Таблица 19.3. Типичные комбинации кодов состояния интерфейсов



Состояние линии и протокола	Типичные причины
Administratively down, down	В конфигурации интерфейса введена команда shutdown
down, down	В конфигурации интерфейса введена команда no shutdown, но есть проблемы на физическом уровне. Например, в интерфейс не включен кабель; если используется канал Ethernet, то интерфейс коммутатора на другом конце канала выключен или выключено питание самого коммутатора
up, down	Практически всегда эти коды состояний указывают на проблемы канального уровня, зачастую — на проблемы в конфигурации. Например, для последовательных интерфейсов на одном конце канала может быть указана инкапсуляция PPP, а на другом — HDLC
up, up	Все отлично! Интерфейс работает

IP-адрес интерфейса маршрутизатора

Как неоднократно упоминалось выше, в маршрутизаторе необходимо установить IP-адрес на каждом интерфейсе. Если на интерфейсе не указан адрес, то даже несмотря на то, что состояние его может быть “up, up”, пакеты IP через такой порт передаваться не будут.

Конфигурирование IP-адреса для интерфейса относительно простое, нужно всего лишь указать IP-адрес и маску с помощью команды `ip address` адрес маска в подрежиме конфигурирования интерфейса. В примере 19.2 проиллюстрирован процесс присвоения IP-адресов двум интерфейсам, а также показано, как будут выглядеть в таком случае команды `show ip interface brief` и `show interfaces`, упомянутые в примере 19.1. (В примере 19.1 IP-адреса не были установлены на момент выполнения указанных команд.)

Пример 19.2. Конфигурирование IP-адресов в маршрутизаторах Cisco

```
Albuquerque#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Albuquerque (config)#interface Fa0/0
Albuquerque (config-if)#ip address 10.1.1.1 255.255.255.0
Albuquerque (config-if)#interface S0/0/1
Albuquerque (config-if)#ip address 10.1.2.1 255.255.255.0
Albuquerque (config-if)#+Z
Albuquerque#show ip interface brief
Interface      IP-Address  OK?   Method  Status          Protocol
FastEthernet0/0  10.1.1.1   YES    manual   up            up
FastEthernet0/1  unassigned  YES    NVRAM   administratively down
Serial0/0/0      unassigned  YES    NVRAM   administratively down
Serial0/0/1      10.1.2.1   YES    manual   up            up
Serial0/1/0      unassigned  YES    NVRAM   up            up
Serial0/1/1      unassigned  YES    NVRAM   administratively down
Albuquerque#show interfaces fa0/0
FastEthernet0/0 is up, line protocol is up
  Hardware is Gt96k FE, address is 0013.197b.5004 (bia 0013.197b.5004)
  Internet address is 10.1.1.1/24
```

[!] Часть информации опущена для краткости

Установка параметров Bandwidth и Clock Rate для интерфейсов

Интерфейсы Ethernet работают или на одной скорости, или могут переключаться всего в несколько режимов работы с разными скоростями, если используется автоопределение параметров канала. Как было указано в главе 4, разнообразие технологий и скоростей каналов WAN очень велико. Чтобы использовать разные скорости передачи данных, маршрутизаторы работают в качестве ведомого устройства и получают настройки скорости от модуля CSU/DSU в ходе *синхронизации* (*clocking*). В результате последовательные каналы маршрутизатора работают без дополнительного конфигурирования, автоопределения скорости канала и т.п. Устройство CSU/DSU всегда “знает” скорость работы телекоммуникационного канала, пересыпает синхроимпульсы по кабелю маршрутизатору, а последний подстраивает свой интерфейс согласно таким импульсам. Фактически модуль CSU/DSU указывает маршрутизатору, когда следует отправить следующий бит по кабелю и принять бит, а маршрутизатор просто слепо следует таким инструкциям.

Физический механизм работы процесса определяет, с какой скоростью и в какие моменты времени маршрутизатор может передавать биты информации, а логическая скорость линии может не совпадать с той, что задана синхроимпульсами от модуля CSU/DSU¹. Поэтому вполне логично, что в маршрутизаторах используются две команды режима конфигурирования интерфейса для установки скорости канала WAN, подключенного к последовательному интерфейсу, а именно подкоманды *clock rate* и *bandwidth*.

Команда *clock rate* задает действительную скорость передачи битов по последовательному каналу, но она используется только в том случае, когда два маршрутизатора соединены между собой кабелем напрямую (например, в лабораторной сети). Такое *непосредственное подключение последовательных интерфейсов* (back-to-back serial cables) используется в примерах этой книги, и в лабораторных сетях, сетевые инженеры также могут делать для себя временные стенды для проверки чего-либо, например, вопросов экзамена CCNA и т.п. (Такое подключение подробно описано в главе 4.) В непосредственном лабораторном подключении устройств не используются модули CSU/DSU, поэтому один маршрутизатор должен выступать в качестве ведущего, т.е. генерировать импульсы синхронизации, а второй — в качестве ведомого, т.е. подстраиваться под них. Причем второй, т.е. ведомый, маршрутизатор работает в обычном режиме так, как если бы он был подключен к модулю CSU/DSU, — о том, что синхронизацию ведет другой маршрутизатор, он и не знает. В примере 19.3 показана конфигурация маршрутизатора с обсуждавшимися выше настройками, а также еще одна полезная команда.

ВНИМАНИЕ!

В примере 19.3 опущена большая часть вывода команды *show running-config*, т.е. убрано все, что не относится к обсуждаемой теме.

Пример 19.3. Конфигурация с использованием команды *clock rate*

```
Albuquerque#show running-config
! Остальная информация опущена для краткости
```

¹ Например, если используется сжатие данных в канале. — Примеч. ред.

```
interface Serial0/0/1
    clock rate 128000
!
interface Serial0/1/0
    clock rate 128000
    bandwidth 128
!
interface FastEthernet0/0
! Остальная информация опущена для краткости
Albuquerque#show controllers serial 0/0/1
Interface Serial0
Hardware is PowerQUICC MPK860
DCE V.35, clock rate 128000
idb at 0x8169BB20, driver data structure at 0x816A35E4
! Остальная информация опущена для краткости
```

Команда `clock rate` скорость поддержана конфигурирования интерфейса задает скорость работы порта и вводится для того интерфейса, в который включен кабель DCE. Если не известно, в какой маршрутизатор включен кабель DCE, то тип подключенного кабеля можно узнать с помощью команды `show controllers`, как показано в примере 19.3. Есть небольшая особенность: операционная система Cisco IOS принимает команду `clock rate` на интерфейсе либо в том случае, если кабель вообще не подключен, либо если тип кабеля — DCE. Если к интерфейсу подключен кабель DTE, операционная система тихо игнорирует команду, и в настройках она не появляется, при этом сообщение об ошибке не выводится.

Вторая полезная команда связана с настройкой скорости последовательного канала: `bandwidth` скорость (см. настройки интерфейса `serial 0/1/0` в примере 19.3). Команда `bandwidth` задает операционной системе скорость канала в Кбит/с, причем такая скорость никоим образом не зависит от синхроимпульсов и физической скорости соединения. Тем не менее команда `bandwidth` не меняет физическую скорость передачи и приема битов интерфейсом, а влияет на расчет параметров загруженности канала, метрик протоколов маршрутизации и т.п. В частности, например, протоколы маршрутизации EIGRP и OSPF используют значение команды `bandwidth` интерфейса для подсчета своих стандартных метрик, которые повлияют на то, какой именно маршрут будет выбран в качестве оптимального к какой-либо сети. (Подробно протоколы маршрутизации и использование упомянутой команды рассмотрены во втором томе книги.)

У каждого интерфейса есть стандартная настройка ширины полосы пропускания, которая используется, если для интерфейса не настроена команда `bandwidth`. Например, для последовательных интерфейсов стандартно используется значение параметра `bandwidth`, равное 1544, что означает 1544 Кбит/с, или 1,544 Мбит/с, другими словами, используется скорость канала T1. Другой вариант — скорость интерфейса Ethernet связана с текущей скоростью его работы и технологией Ethernet. Например, если интерфейс `FastEthernet` работает на скорости 100 Мбит/с, то его полоса пропускания (т.е. значение параметра `bandwidth`) будет равна 100 000 (Кбит/с); но если интерфейс работает на скорости 10 Мбит/с, то его полоса пропускания будет равна 10 000 (Кбит/с). Указание команды `bandwidth` в конфигурации интерфейса переопределяет стандартные значения.

ВНИМАНИЕ!

Следует запомнить, что в команде `clock rate` указывается значение в бит/с, а в команде `bandwidth` — в Кбит/с. Следовательно, если команда `show` показывает значение полосы пропускания 10 000, то это означает 10 000 Кбит/с, или 10 Мбит/с.

Дополнительный порт маршрутизатора

В маршрутизаторах есть так называемый *дополнительный* (*auxiliary* — *aux*) порт, через который можно получить доступ к интерфейсу командной строки при посредничестве программы эмулятора терминала. Обычно порт aux подключен кабелем (с разъемом RJ-45, четырехпарным с прямой распайкой) к внешнему аналоговому модему. Сам модем подключен к телефонной линии, а сетевой инженер может подключиться к нему с дистанционного персонального компьютера, используя программу эмуляции терминала, опять же при посредничестве подключенного к компьютеру модема и телефонной линии. Подключившись, инженер получит стандартный доступ к интерфейсу командной строки устройства так, как если бы он был подключен к консольному порту.

Параметры порта aux задаются после перехода в режим конфигурирования соответствующей линии с помощью команды `line aux 0`. В режиме конфигурирования линии порта aux можно ввести многие команды, которые обсуждались в главе 8. Например, можно настроить простую аутентификацию с помощью команд `login` и `password`; в результате при входящем дистанционном соединении у пользователя будут запрашиваться имя и пароль.

Диалог начальной настройки

Процесс начальной настройки маршрутизатора подчиняется тем же правилам и принципам, что и соответствующий диалог коммутаторов. Подробное описание интерактивного диалога приведено в главе 8, ниже указаны ключевые моменты, которые одинаковы как для маршрутизаторов, так и для коммутаторов.



Краткий список важных сведений о диалоге начального конфигурирования

- Диалог начальной настройки предназначен для конфигурирования базовых параметров в интерфейсе командной строки, которые вводятся в интерактивном режиме в виде ответов на вопросы.
- Запустить режим начального конфигурирования маршрутизатора можно, удалив файл начальной конфигурации (`startup-config`) и перезагрузив устройство, или с помощью команды `setup` в режиме привилегированного пользователя.
- В конце диалога будет выведено меню с тремя вариантами выбора (цифрами 0, 1 и 2), с помощью которого можно, проигнорировав сделанные настройки, перейти в интерфейс командной строки (0), перезапустить диалог начального конфигурирования, опять же проигнорировав только что введенные настройки (1), или сохранить и начать использовать введенную конфигурацию (2).
- Если процесс конфигурирования через диалог вам надоел, то можно нажать комбинацию клавиш `<Ctrl+c>`, чтобы его прервать и перейти к интерфейсу командной строки.

- Если в конце диалога выбрать сохранение полученной конфигурации, она будет записана как в файл стартовой (startup-config), так и в файл текущей (running-config) конфигурации.

Основные отличия в диалоге начальной конфигурации устройства для маршрутизаторов и коммутаторов заключаются в запрашиваемой информации в процессе ответа на вопросы диалога. Например, в отличие от коммутаторов, у которых есть только один адрес на все устройство, в маршрутизаторах нужно установить IP-адрес и маску для каждого интерфейса. В примере 19.4 показан режим начального конфигурирования маршрутизатора (setup). Если у читателя нет маршрутизатора, в котором он может запустить диалог, то следует потратить некоторое время на изучение приведенных в примере вопросов и требуемой маршрутизатору информации.

ВНИМАНИЕ!

Вопросы, задаваемые интерактивным диалогом начальной настройки, могут слегка отличаться. Тип, количество и формат вопросов зависит от версии операционной системы Cisco IOS, набора функций системы, устройства и модели маршрутизатора.

Пример 19.4. Интерактивный диалог начального конфигурирования маршрутизатора

```
--- System Configuration Dialog ---
Would you like to enter the initial configuration dialog? [yes/no]: yes
At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '['].Basic management setup
configures
only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system

Would you like to enter basic management setup? [yes/no]: no
First, would you like to see the current interface summary? [yes] :
Any interface listed with OK? value "NO" does not have a valid
configuration

Interface          IP-Address  OK?   Method  Status      Protocol
Ethernet0         unassigned  NO    unset    up        down
Serial0           unassigned  NO    unset    down     down
Serial1           unassigned  NO    unset    down     down

Configuring global parameters:

Enter host name [Router]: R1
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.
Enter enable secret: cisco
The enable password is used when you do not specify an
enable secret password, with some older software versions, and
some boot images.
Enter enable password: fred
The virtual terminal password is used to protect
access to the router over a network interface.
```

```
Enter virtual terminal password: barney
Configure SNMP Network Management? [yes]: no
Configure bridging? [no]:
Configure DECnet? [no]:
Configure AppleTalk? [no]:
Configure IPX? [no]:
Configure IP? [yes]:
Configure RIP routing? [yes]:
Configure CLNS? [no]:
Configure bridging? [no]:

Configuring interface parameters:
Do you want to configure Ethernet0 interface? [yes]:
Configure IP on this interface? [yes]:
IP address for this interface: 172.16.1.1
Subnet mask for this interface [255.255.0.0] : 255.255.255.0
Class B network is 172.16.0.0, 24 subnet bits; mask is /24
Do you want to configure Serial0 interface? [yes]:
Configure IP on this interface? [yes]:
Configure IP unnumbered on this interface? [no]:
IP address for this interface: 172.16.12.1
Subnet mask for this interface [255.255.0.0] : 255.255.255.0
Class B network is 172.16.0.0, 24 subnet bits; mask is /24
Do you want to configure Serial1 interface? [yes]:
Configure IP on this interface? [yes]:
Configure IP unnumbered on this interface? [no]:
IP address for this interface: 172.16.13.1
Subnet mask for this interface [255.255.0.0] : 255.255.255.0
Class B network is 172.16.0.0, 24 subnet bits; mask is /24

The following configuration command script was created:
hostname R1
enable secret 5 $1$VOLh$pkIe0Xjx2sgjgZ/Y6Gt1s.
enable password fred
line vty 0 4
password barney
no snmp-server
!
ip routing
!
interface Ethernet0
ip address 172.16.1.1 255.255.255.0
!
interface Serial0
ip address 172.16.12.1 255.255.255.0
!
interface Serial1
ip address 172.16.13.1 255.255.255.0
!
router rip
network 172.16.0.0
!
end
[0] Go to the IOS command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration to nvram and exit.
```

```
Enter your selection [2] : 2
Building configuration...
[OK] Use the enabled mode 'configure' command to modify this
configuration.
Press RETURN to get started!
```

ВНИМАНИЕ!

В приведенном выше примере используется операционная система Cisco IOS, в которой нет дополнительной функции, называемой *автоматической настройкой безопасности Cisco* (Cisco Auto Secure), поэтому в диалоге она не отображается. В определенных версиях операционной системы эта функция есть, она автоматически задает оптимальные настройки безопасности, например отключает протокол CDP.

Обновление операционной системы Cisco IOS и процесс начальной загрузки устройства

Сетевому инженеру обязательно нужно знать, как обновить операционную систему Cisco IOS, т.е. как перейти на старшую версию программного обеспечения. Обычно образ операционной системы хранится во флеш-памяти маршрутизатора, и именно эта версия системы используется при загрузке устройства. (Термином *образ системы IOS* называют файл операционной системы.) Процесс обновления операционной системы IOS может включать в себя несколько этапов: копирование нового образа операционной системы во флеш-память; указание с помощью конфигурационных команд, какой файл и откуда должен загружать маршрутизатор; удаление старого образа операционной системы после того, как работоспособность нового проверена и известно, что все службы функционируют правильно. Альтернативный вариант предполагает, что образ системы IOS можно скопировать на сервер TFTP, выполнить дополнительные конфигурационные команды в маршрутизаторе, которые укажут, что загрузка системы после перезагрузки устройства должна выполняться с сервера.

В текущем разделе описано, как обновить операционную систему, скопировав новый образ IOS во флеш-память маршрутизатора, и как указать устройству, из какого источника нужно проводить загрузку. Поскольку источник загрузки выбирается в процессе инициализации устройства, ниже также будет рассмотрен процесс начальной загрузки и самотестирования. В коммутаторах используется аналогичный процесс, их процедура загрузки отличается от таковой в маршрутизаторах только в мелких деталях, которые будут оговорены отдельно.

Обновление операционной системы Cisco IOS во флеш-памяти

Обычно образ операционной системы Cisco IOS хранится во флеш-памяти маршрутизатора или коммутатора. Такая память является перезаписываемой и энергонезависимой (т.е. данные в ней сохраняются при выключении питания), поэтому она представляет собой идеальный вариант хранилища для данных, которые будут нужны каждый раз при загрузке маршрутизатора. В устройствах компании Cisco преднамеренно используется флеш-память, а не накопители на жестких дисках, потому что в ней нет механических движущихся частей, следовательно, вероятность отказа операционной системы и потери данных крайне мала. Кроме того, операци-

онная система может быть размещена на внешнем сервере TFTP, но такой подход часто используется только для проверки, в реальных сетях операционная система во избежание проблем загружается из локальной флеш-памяти.

На рис. 19.6 показан процесс обновления операционной системы Cisco IOS во флеш-памяти.

- Этап 1** Получить образ операционной системы от компании Cisco, обычно образ загружается с веб-сайта компании [Cisco.com](http://www.cisco.com) с помощью протокола HTTP или FTP.
- Этап 2** Поместить файл операционной системы в стандартную (корневую) папку сервера TFTP, а сам сервер должен быть доступен для маршрутизатора по сети.
- Этап 3** Использовать команду `copy` с параметрами в маршрутизаторе и скопировать файл во флеш-память.

В примере 19.5 показан последний этап — копирования образа операционной системы во флеш-память. Обратите внимание на то, что показанная в нем команда `copy tftp flash` работает аналогично описанной выше команде `copy tftp startup-config`, которая использовалась для сохранения резервной копии конфигурационного файла в памяти NVRAM.

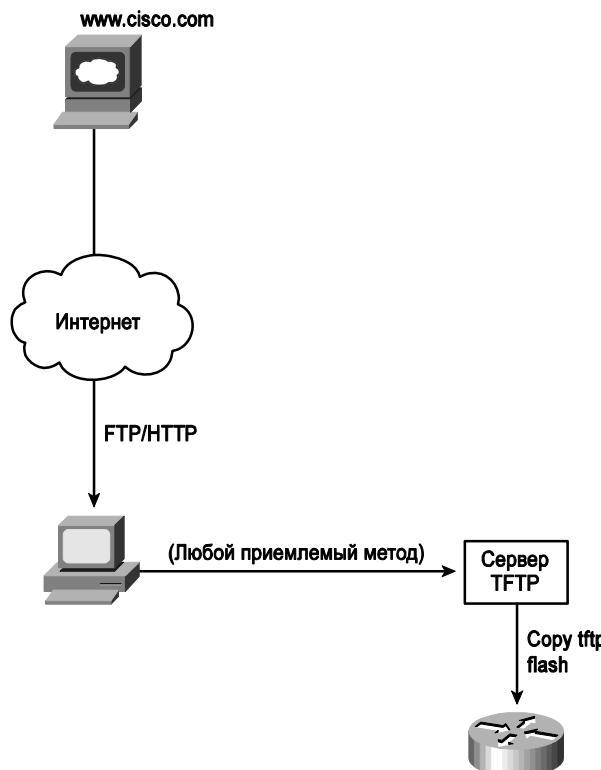


Рис. 19.6. Процесс обновления операционной системы Cisco IOS

Пример 19.5. Копирование образа операционной системы Cisco IOS во флеш-память с помощью команды copy tftp flash

```
R1#copy tftp flash
System flash directory:
File    Length   Name/status
 1    7530760   c4500-d-mz.120-2.bin
[7530824 bytes used, 857784 available, 8388608 total]
Address or name of remote host [255.255.255.255]? 134.141.3.33
Source file name? c4500-d-mz.120-5.bin
Destination file name [c4500-d-mz.120-5.bin]?
Accessing file c4500-d-mz.120-5.bin ' on 134.141.3.33...
Loading c4500-d-mz.120-5.bin from 134.141.3.33 (via Ethernet0): ! [OK]

Erase flash device before writing? [confirm]
Flash contains files. Are you sure you want to erase? [confirm]

Copy 'c4500-d-mz.120-5.bin' from server
  as 'c4500-d-mz.120-5.bin' into Flash WITH erase? [yes/no]y
Erasing device... eeeeeeeeeeeeeeeeeeeeeeeeeeeee...erased
Loading c4500-d-mz.120-5.bin from 134.141.3.33 (via Ethernet0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! (здесь опущено много восклицательных знаков!)
[OK 7530760/8388608 bytes]

Verifying checksum... OK (0xA93E)
Flash copy took 0:04:26 [hh:mm:ss]
```

В процессе копирования образа системы IOS во флеш-память маршрутизатору необходимо получить некоторую важную информацию.

1. IP-адрес сервера TFTP.
2. Название файла образа.
3. Проверить, достаточно ли места во флеш-памяти.
4. Проверить, есть ли файл с указанным именем на сервере.
5. Спросить у пользователя, хочет ли он удалить старые файлы.

Интерфейс командной строки маршрутизатора переспросит всю нужную ему информацию в диалоге. Для каждого вопроса нужно либо ввести ответ, либо нажать клавишу <Enter>, чтобы использовать стандартную настройку (показанную в квадратных скобках), если она есть. После окончания диалога маршрутизатор удалит все, что есть во флеш-памяти, если это было указано, проверит контрольную сумму файла, чтобы убедиться, что он был передан устройству без ошибок. После завершения процедуры можно проверить содержимое памяти с помощью команды show flash, как показано в примере 19.6. (Вывод этой команды может отличаться в зависимости от модели или серии устройства. В примере 19.6 показан вывод команды show flash для маршрутизатора серии 2500.)

Пример 19.6. Проверка содержимого флеш-памяти с помощью команды show flash

```
fred#show flash
System flash directory:
File    Length   Name/status
 1    13305352   c2500-ds-l.122-1.bin
[13305416 bytes used, 3471800 available, 16777216 total]
16384K bytes of processor board System flash (Read ONLY)
```

В примере 19.6 выделена строка, в которой показан размер флеш-памяти, объем используемой и свободной памяти. При копировании образа операционной системы во флеш-память команда `copy` запросит, нужно ли очистить память, а стандартным ответом будет “да” (`[yes]`). Если ответить “нет” (`no`) на такой вопрос и команда обнаружит, что памяти недостаточно для новой операционной системы, копирование оборвется. Аналогично, даже если ответить “да” на вопрос о памяти будет очищена, если образ больше, чем флеш-память устройства, копирование будет прервано.

После того как новый образ операционной системы скопирован в маршрутизатор, устройство нужно перезагрузить, чтобы использовалась новая версия. В следующем разделе рассматривается процесс загрузки операционной системы Cisco IOS и описано, как указать маршрутизатору, какую именно операционную систему загружать.

Процедура загрузки операционной системы Cisco IOS

Маршрутизаторы фактически выполняют те же действия, что и любой компьютер, когда их перезагружают (с помощью команды `reload`) или включают питание. В большинстве персональных компьютеров установлена всего одна операционная система и стандартно загружается именно она. В маршрутизаторах может быть несколько вариантов операционной системы как во флеш-памяти устройства, так и на внешнем сервере TFTP, поэтому зачастую устройству нужно указать, какой образ IOS следует загружать. В текущем разделе рассмотрен весь процесс загрузки маршрутизатора, а особое внимание уделено тому, как маршрутизатор выбирает, какую операционную систему загрузить.

ВНИМАНИЕ!

Процедура загрузки маршрутизатора, описанная в этом разделе, в частности использование конфигурационных регистров и операционной системы ROMMON, отличается от аналогичной для коммутаторов, но применима для большинства моделей маршрутизаторов. В этой книге не описывается процесс загрузки и управление им для коммутаторов.

В процессе загрузки маршрутизатор проходит следующие этапы.

 **Ключевая тема** Четыре этапа загрузки маршрутизатора

1. После включения или переключения питания маршрутизатор выполняет процедуру *самотестирования при включении питания* (Power-On Self-Test — POST), с помощью которой обнаруживает аппаратные компоненты и проверяет, что все они работают правильно.
2. Далее маршрутизатор из постоянного запоминающего устройства (ПЗУ — ROM) копирует загрузочную подпрограмму (bootstrap) в оперативную память (RAM) и выполняет ее.
3. Загрузочная подпрограмма “решает”, какой образ операционной системы следует загрузить в оперативную память, и загружает ее. После загрузки образа IOS загрузочная подпрограмма передает управление устройством операционной системе Cisco IOS.
4. Если загрузочная подпрограмма успешно загрузила образ системы, операционная система Cisco IOS ищет конфигурационный файл (обычно файл `startup-config` в памяти NVRAM) и загружает его в оперативную память (RAM) в качестве файла текущей конфигурации (`running-config`).

Все маршрутизаторы используют описанный выше процесс из четырех этапов при включении и загрузке устройства. На первых двух этапах повлиять на работу маршрутизатора невозможно. Если в процессе их выполнения возникают сбои и ошибки, нужно обратиться в службу технической поддержки компании Cisco (Cisco Technical Assistance Center — TAC) или к поставщику устройства для гарантийного ремонта. Для этапов 3 и 4 есть специальные конфигурационные команды, с помощью которых можно управлять процессом дальнейшей загрузки маршрутизатора. На рис. 19.7 показаны различные возможности и этапы загрузки устройств 2–4.

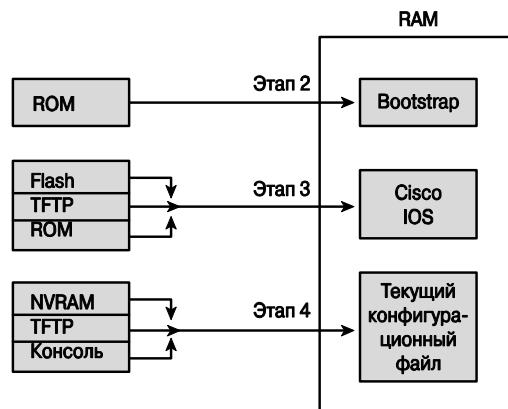


Рис. 19.7. Процесс загрузки операционной системы Cisco IOS

Из описания и иллюстрации процесса можно увидеть, что маршрутизатор способен загрузить операционную систему из трех источников, и конфигурационный файл он также ищет в трех местах. Строго говоря, практически всегда большинство маршрутизаторов загружает конфигурационный файл из памяти NVRAM (файл стартовой конфигурации *startup-config*). Каких-либо дополнительных преимуществ загрузка стартовой конфигурации из других источников не дает, поэтому этап 4 не будет очень детально рассматриваться в текущем разделе. Тем не менее неплохой практикой будет хранение нескольких образов IOS во флеш-памяти, а также сохранение резервной копии на каких-либо серверах, поэтому ниже будет подробно обсуждаться этап 3 описанного выше процесса. В частности, будут описаны несколько альтернативных операционных систем маршрутизаторов, а также что такое конфигурационные регистры и как они используются при загрузке устройства.

ВНИМАНИЕ!

Образ операционной системы Cisco IOS обычно находится в сжатом файле, чтобы он занимал меньше места во флеш-памяти. Маршрутизатор разархивирует образ операционной системы по мере загрузки ее в оперативную память (RAM).

Три операционные системы маршрутизатора

Обычно маршрутизатор нормально загружает полнофункциональную операционную систему Cisco IOS, позволяющую устройству выполнять все необходимые функции по маршрутизации пакетов. Тем не менее маршрутизаторы компании Cisco могут использовать альтернативную систему для поиска и устранения неисправностей, восстановления пароля устройства и копирования нового файла образа IOS

в том случае, если система во флеш-памяти была непреднамеренно удалена или повреждена. В новой линейке продуктов компании Cisco (например, в различных маршрутизаторах ISR Cisco) используется только одна альтернативная операционная система, а в старых моделях (например, в серии 2500) в действительности было две альтернативные операционные системы, которые выполняли разные наборы функций. В табл. 19.4 перечислены и описаны две альтернативные операционные системы, которые можно встретить в маршрутизаторах.



Таблица 19.4. Сравнение операционных систем ROMMON и RxBoot

Операционная система	Название	Где хранится	Где используется
Монитор ROM (ROM Monitor)	ROMMON	ROM	В старых и новых моделях маршрутизаторов
Загрузочная ROM (Boot ROM)	RxBoot, boot helper	ROM	В старых моделях маршрутизаторов

Поскольку операционная система RxBoot есть только в старых моделях маршрутизаторов и в настоящее время редко встречается, в текущей главе в основном будет описываться операционная система ROMMON и ее специальные функции.

Конфигурационный регистр

Конфигурационный регистр (configuration register) представляет собой специальное 16-битовое число, которое может быть установлено в любом маршрутизаторе компании Cisco. Биты конфигурационного регистра контролируют различные параметры работы устройства на низком уровне. Например, консольное подключение к маршрутизатору стандартно работает на скорости 9600 бод, но эта настройка может быть изменена в результате замены значений пары битов в конфигурационном регистре.

СОВЕТ

С помощью команды `show version`, которая описана в примере 19.7, можно увидеть текущее значение конфигурационного регистра, а также узнать, будет ли после перезагрузки установлено новое значение.

Значение конфигурационного регистра может быть установлено с помощью команды `config-register` в режиме глобальной конфигурации. Инженеры устанавливают различные значения для различных целей, но наиболее распространенное применение разных значений — повлиять на процесс загрузки образа операционной системы IOS и восстановить пароль устройства. Например, команда `config-register 0x2100` устанавливает в регистр шестнадцатеричное значение 2100, благодаря которому маршрутизатор загрузит операционную систему ROMMON, а не IOS. Следует помнить, что значение будет сохранено в стартовой конфигурации сразу же после нажатия клавиши `<Enter>`, сразу после команды `config-register`, поэтому не нужно сохранять текущий конфигурационный файл (`running-config`) в стартовый (`startup-config`) после смены значения. Тем не менее новое значение регистра будет использоваться только после перезагрузки устройства.

ВНИМАНИЕ!

В большинстве маршрутизаторов компании Cisco стандартное значение регистра равно шестнадцатеричному числу 2102.

Как маршрутизатор выбирает источник загрузки

Маршрутизатор выбирает источник загрузки операционной системы Cisco IOS на основании 4 младших битов конфигурационного регистра и параметров команды `boot system` в подразделе глобальной конфигурации устройства в стартовом конфигурационном файле. Младшие четыре бита (4-я шестнадцатеричная цифра) конфигурационного регистра называют *загрузочным полем* (*boot field*), и оно проверяется первым, когда маршрутизатор загружается и решает, какой образ операционной системы IOS использовать. Значение загрузочного поля регистра используется как при перезагрузке, так и при включении питания устройства.

ВНИМАНИЕ!

Чтобы различать, например, десятичные и шестнадцатеричные числа, в документации и книгах компании Cisco перед шестнадцатеричным числом ставится префикс “0x”, например, “0x4” будет означать шестнадцатеричное число 4.

Алгоритм выбора источника операционной системы Cisco IOS для современных маршрутизаторов, в которых нет программного обеспечения RxBoot, описан ниже.

Этапы выбора источника операционной системы Cisco IOS в процессе загрузки устройства



- Этап 1** Если загрузочное поле регистра равно 0, будет загружаться система ROMMON.
- Этап 2** Если загрузочное поле регистра равно 0, будет загружаться первый² образ операционной системы Cisco IOS из флеш-памяти.
- Этап 3** Если загрузочное поле регистра содержит значение от 2 до F:
 - а) выполняется перебор всех команд `boot system` в стартовом конфигурационном файле по порядку, до тех пор, пока какой-либо из вариантов команды не сработает;
 - б) если ни одна из команд `boot system` не сработала, загружается первый образ операционной системы Cisco IOS из флеш-памяти.

ВНИМАНИЕ!

Указанные номера этапов не важны, список действий пронумерован просто для удобства.

Первые два действия маршрутизатора достаточно просты, но на третьем этапе маршрутизатор использует второй возможный метод указания источника загрузки устройства: команду глобальной конфигурации `boot system`. Эта команда может быть несколько раз введена в конфигурации устройства с разными параметрами, может указывать файлы-образы операционной системы во флеш-памяти, названия файлов и IP-адреса серверов, на которых необходимо искать образ операционной системы Cisco IOS. Если маршрутизатор успешно загрузил операционную систему из источника, указанного такой командой, процесс поиска завершается и оставшиеся команды `boot system` игнорируются. Если же все варианты команды в глобальной конфигурации дали отрицательный результат, маршрутизатор возвращается на этап 2 и пытается загрузить первый образ из флеш-памяти.

На этапах 2 и 3 б маршрутизатор, как указано в описанном выше алгоритме, загружает первый файл системы IOS. Что же означает в данном случае “первый”?

² Т.е. файл образа с наиболее поздней датой создания или записи. — Примеч. ред.

Маршрутизаторы нумеруют файлы, хранимые во флеш-памяти, а каждый новый файл получает больший номер, чем предыдущий. Когда устройство пытается выполнить этап 2 или 3 б, оно начинает перебор с номера 1, а затем проверяет число 2 и так далее, пока не найдет файл образа операционной системы с меньшим номером, и загружает такой файл.

Следует отметить, что большинство маршрутизаторов находят файл образа операционной системы на этапе 3 б. Стандартные заводские настройки устройства предполагают, что в маршрутизаторах Cisco нет команд `boot system`, в действительности в них нет вообще никакой стартовой конфигурации, т.е. файл `startup-config` отсутствует. Компания Cisco копирует в маршрутизаторы единственный файл операционной системы Cisco IOS, а значение конфигурационного регистра устанавливается в 0x2102, т.е. значение загрузочного поля равно 0x2. С такими настройками устройство сначала выполняет этап 3 (поскольку загрузочное поле равно 2), не находит команд `boot system` (поскольку файл стартовой конфигурации или отсутствует, или пуст), следовательно, ищет первый файл образа операционной системы во флеш-памяти.

На рис. 19.8 представлена схема ключевых этапов поиска и загрузки образа операционной системы.

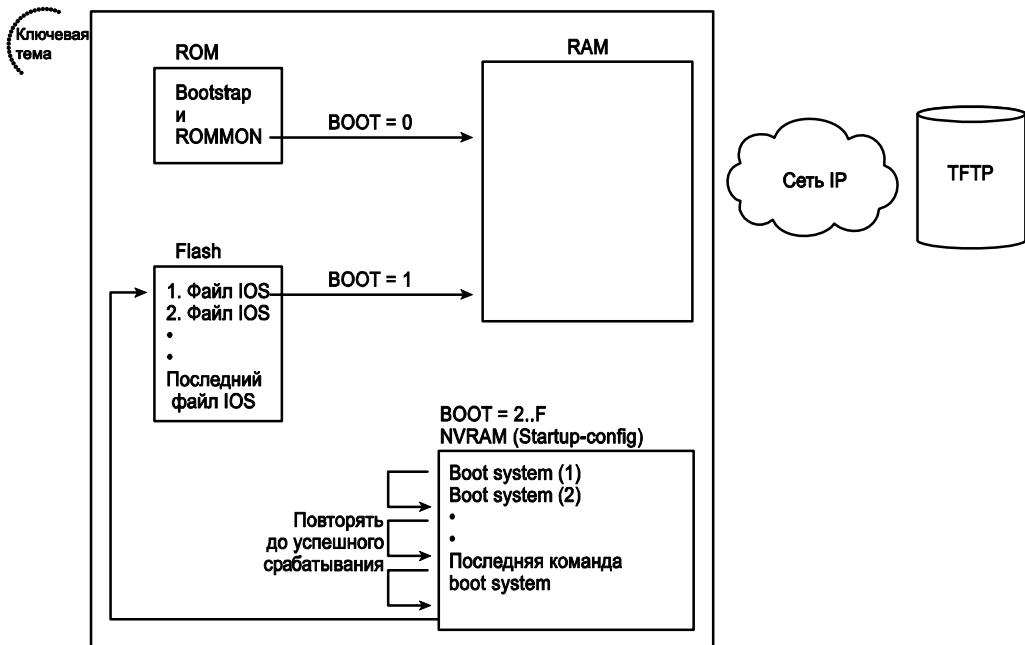


Рис. 19.8. Варианты загрузки операционной системы в современных маршрутизаторах Cisco

В команде `boot system` должно быть точно указано название файла, которое будет загружать маршрутизатор. В табл. 19.5 приведено несколько примеров этой команды.

В определенных случаях маршрутизатор после выполнения трехэтапного процесса не сможет загрузить операционную систему. Такая ситуация произойдет, например, в том случае, если кто-то случайно удалил все содержимое флеш-памяти, в том числе и образ системы IOS. Устройство должно что-то предпринять в такой неожиданной, но вполне вероятной ситуации. Если маршрутизатор не находит операционную систему

му на этапе 3, он рассыпает широковещательные запросы поиска сервера TFTP, пытается угадать название файла образа системы IOS и загрузить его (если сервер найден). На практике такая возможность вряд ли заработает. В качестве последнего средства устройство загружает систему ROMMON, которая частично и предназначена как раз для таких событий — для восстановления работоспособности маршрутизатора в случае возникновения нештатных ситуаций. Например, с помощью системы ROMMON можно вручную скопировать образ операционной системы с сервера TFTP.

Таблица 19.5. Примеры команды `boot system`

Команда <code>boot system</code>	Результат
<code>boot system flash</code>	Будет загружен первый образ операционной системы из флеш-памяти
<code>boot system flash название_файла</code>	Образ IOS с названием <code>название_файла</code> будет загружен из флеш-памяти
<code>boot system tftp название_файла 10.1.1.1</code>	Образ IOS с названием <code>название_файла</code> будет загружен с сервера TFP

Для устаревших моделей маршрутизаторов Cisco, в которых есть система RxBoot (или boot helper) в памяти ROM, процесс выбора загружаемого образа операционной системы IOS работает в общем-то очень похоже, без существенных отличий. Если в загрузочном поле конфигурационного регистра установлено значение 0x1, маршрутизатор загрузит систему RxBoot из памяти ROM. Опять же, если попытки загрузить систему из всех источников не увенчиваются успехом, маршрутизатор использует образ RxBoot и попробует его загрузить.

Команда `show version` и значение конфигурационного регистра

Команда `show version` выдает очень много разнообразной и полезной информации о маршрутизаторе, в том числе текущее и ожидаемое после перезагрузки значение конфигурационного регистра. Наиболее полезная информация, выводимая этой командой, приведена ниже.

Список наиболее важной информации, которую можно получить с помощью команды `show version`



1. Версия операционной системы Cisco IOS.
2. Время непрерывной работы устройства (uptime или время, прошедшее с последней перезагрузки устройства).
3. Причина последней перезагрузки операционной системы (выполнена команда `reload`, отключено питание, произошел отказ программного обеспечения).
4. Время последней загрузки маршрутизатора (если в устройстве были правильно выставлены дата и время).
5. Источник, из которого был загружен используемый образ системы IOS.
6. Объем оперативной памяти (RAM) устройства.
7. Количество и тип интерфейсов устройства.
8. Объем памяти NVRAM.
9. Объем флеш-памяти устройства.
10. Текущее и будущее значения конфигурационного регистра (если они отличаются).

В примере 19.7 показан результат выполнения команды `show version`, в котором выделены наиболее важные сведения. Обратите внимание: в списке выше ключевая информация указана в том же порядке, что и в выводе команды.

Пример 19.7. Вывод команды `show version`

```
Albuquerque#show version
Cisco IOS Software, 1841 Software (C1841-ADVENTERPRISEK9-M), Version
12.4(9)T, RELEASE
  SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Fri 16-Jun-06 21:26 by prod_rel_team

OM: System Bootstrap, Version 12.3(8r)T8, RELEASE SOFTWARE (fc1)

Albuquerque uptime is 5 hours, 20 minutes
System returned to ROM by reload at 13:12:26 UTC Wed Jan 17 2007
System restarted at 13:13:38 UTC Wed Jan 17 2007
System image file is "flash:c1841-adventerprisek9-mz.124-9.T.bin"
```

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:

<http://www.cisco.com/wwl/export/crypto/tool/stqrg.html>

If you require further assistance please contact us by sending email to export@cisco.com.

```
Cisco 1841 (revision 4.1) with 354304K/38912K bytes of memory.
Processor board ID FTX0906Y03T
2 FastEthernet interfaces
4 Serial(sync/async) interfaces
1 Virtual Private Network (VPN) Module
DRAM configuration is 64 bits wide with parity disabled.
191K bytes of NVRAM.
125440K bytes of ATA CompactFlash (Read/Write)
```

```
Configuration register is 0x2102 (will be 0x2101 at next reload)
```

Выделенную в выводе команды информацию можно легко ассоциировать с указанным выше списком. Следует отметить, что объем оперативной памяти (RAM) указан в виде двух чисел, разделенных косой чертой: 354304K/38912K. Сумма обоих чисел как раз и даст искомый общий объем оперативной памяти устройства, или в данном случае 72 Мбайт.

Подготовка к экзамену

Повторите все ключевые темы

Повторите все ключевые темы данной главы, помеченные пиктограммой “Ключевая тема”. Ключевые темы и соответствующие им страницы перечислены в табл. 19.6.

Таблица 19.6. Ключевые темы главы 19

Элемент	Описание	Страница
Список	Этапы установки маршрутизатора	492
Список	Однаковые команды и настройки интерфейса командной строки маршрутизатора и коммутатора	497
Список	Команды и настройки (см. главу 8), которые отличаются в маршрутизаторах и коммутаторах	497
Табл. 19.2	Коды состояния интерфейсов и их значение	500
Табл. 19.3	Типичные комбинации кодов состояния интерфейсов	501
Список	Краткий список важных сведений о диалоге начального конфигурирования	504
Список	Четыре этапа загрузки маршрутизатора	510
Табл. 19.4	Сравнение операционных систем ROMMON и RxBoot	512
Список	Этапы выбора источника операционной системы Cisco IOS в процессе загрузки устройства	513
Рис. 19.8	Варианты загрузки операционной системы в современных маршрутизаторах Cisco	514
Список	Список наиболее важной информации, которую можно получить с помощью команды show version	515

Заполните таблицы и списки по памяти

Распечатайте приложение M (Appendix L) с компакт-диска или его раздел, относящийся к этой главе, и заполните таблицы и списки по памяти. В приложении Н (Appendix M) приведены заполненные таблицы и списки для самоконтроля.

Ключевые термины

Дайте определения перечисленных ниже терминов и проверьте правильность их написания в списке терминов:

полоса пропускания (bandwidth), загрузочное поле регистра (boot field), частота синхроимпульсов (clock rate), конфигурационный регистр (configuration register), образ системы IOS (IOS image), самотестирование при включении питания (Power-On Self-Test — POST), ROMMON, RxBoot.

Задания приложения К

В приложении К представлены два дополнительных задания, которые помогут проанализировать различные структуры сетей, проблемы и результаты выполнения команд. Сейчас следует обратиться ко второму заданию, в котором проиллюстрировано использование протокола CDP.

Список команд

В табл. 19.7 и 19.8 приведен список команд этой главы, а также даны их краткие описания. Для успешной сдачи большинства сертификационных экзаменов компании Cisco указанные команды нужно помнить наизусть. Чтобы потренироваться в их запоминании, следует закрыть левую часть таблицы листком бумаги и по описанию в правом столбце по памяти записать соответствующие команды, а потом проверить, правильно ли был дан ответ.

Таблица 19.7. Команды для конфигурирования маршрутизаторов Cisco

Команда	Описание
bandwidth Кбит/с	Задает полосу пропускания в Кбит/с для интерфейса. Команда вводится в режиме конфигурирования интерфейса
clock rate значение	Задает частоту синхроимпульсов и скорость передачи данных через интерфейс. Эта команда применима только для интерфейсов, к которым подключен кабель DCE. Команда вводится в режиме конфигурирования интерфейса
config-register значение	Команда режима глобальной конфигурации устройства. Задает значение конфигурационного регистра в шестнадцатеричном формате
boot system { url-файла название}	Команда режима глобальной конфигурации устройства, задающая внешний источник системы IOS
boot system flash [flash-fs:] [название]	Команда режима глобальной конфигурации устройства, задающая источник системы IOS во флеш-памяти
boot system rom	Команда режима глобальной конфигурации устройства, указывающая, что нужно загрузить систему RxBoot из памяти ROM
boot system {rcp tftp ftp} название [ip-адрес]	Команда режима глобальной конфигурации устройства, указывающая внешний сервер, протокол и название файла, которые будут использоваться для загрузки операционной системы

Таблица 19.8. Команды для поиска и устранения неисправностей

Команда	Описание
show interfaces [тип номер]	Показывает подробную информацию о состоянии интерфейса, настройках и его счетчиках
show ip interface brief	Показывает строку информации о каждом интерфейсе, в том числе IP-адрес, код состояния линии и протокола, а также метод получения IP-адреса: вручную или через протокол DHCP

Окончание табл. 19.8

Команда	Описание
Show protocols тип номер	Показывает строку информации о каждом интерфейсе, в том числе IP-адрес, маску и коды состояний линии и протокола
show controllers [тип номер]	Выводит множество информации об интерфейсе, а именно об аппаратном контроллере. Для последовательных интерфейсов эта команда позволяет определить, подключен кабель DTE или DCE
show version	Выводит много полезной информации, например, номер версии операционной системы Cisco IOS и др. (см. пример 19.7)
setup	Режим привилегированного пользователя. Команда запускает интерактивный диалог начальной настройки маршрутизатора (или коммутатора)
copy откуда куда	Режим привилегированного пользователя. Команда копирует файл из одного места в другое. В качестве отправителя и получателя файла может использоваться текущая и стартовая конфигурации, сервер TFTP и RPK, флеш-накопитель
show flash	Перечисляет имена и размер файлов во флеш-памяти, а также указывает объем использованной и доступной флеш-памяти
reload	Режим привилегированного пользователя. Команда вызывает перезагрузку коммутатора или маршрутизатора

В этой главе...

- **Введение в подсети.** Описывается весь процесс создания подсетей и разделение сети на меньшие группы, называемые подсетями.
- **Анализ потребности в подсетях и адресации.** Анализируется, где в реальной топологии сети необходимы подсети. Кроме того, обсуждается концепция размера подсети, который определяют потребности бизнеса.
- **Выбор проекта.** Правила IP-адресации и создания подсетей позволяют сетевым инженерам выбрать подходящий проект. В частности, выбрать используемую сеть IP и маску. В этом разделе обсуждается, что следует учесть при выборе.
- **Реализация плана.** Завершается обсуждение проектирования и начинается описание реализации проекта, включая перечень идентификаторов подсетей, используемых в конкретных местах сетевой топологии, а также какие именно IP-адреса использовать для различных устройств.

ГЛАВА 20

Концепции и конфигурирование протоколов маршрутизации

Почтовая служба США пересыпает огромное количество писем каждый день. Сначала почта сортируется почтовыми машинами, которые могут быстро обработать большое количество конвертов. Письма раскладываются в специальные контейнеры, которые потом наземным транспортом или самолетом доставляются до точки назначения. Тем не менее, если не запрограммировать машины, чтобы они правильно распознавали индексы на почтовых отправлениях, они не смогут работать. Аналогично маршрутизаторы компании Cisco могут маршрутизировать десятки и сотни тысяч пакетов в секунду, но если у них нет маршрутов — т.е. записей о том, куда отправлять пакеты, — такие устройства не смогут выполнять свою основную задачу.

В этой главе описаны основные концепции маршрутизации и рассказано, как маршрутизаторы заполняют свои таблицы маршрутизации. Маршрутизаторы могут получать информацию о маршрутах из разных источников: непосредственно из подключенных к ним сетей и подсетей, из статически заданных записей, а также с помощью протоколов динамической маршрутизации.

Вполне очевидно на данный момент, что, чтобы понять все нюансы работы протоколов маршрутизации, необходимо хорошо понимать процесс маршрутизации вообще, т.е. механизм пересылки пакетов, а также знание IP-адресации и принципов построения подсетей. Поэтому в текущей главе добавлены дополнительные сведения к материалу, изложенному в главе 5, во всех главах части III и в главе 19, а также предпринята попытка связать воедино основные идеи, которые были изложены в указанных главах.

Контрольные вопросы: знаете ли вы уже темы главы

Этот раздел предназначен для того, чтобы читатель мог предварительно оценить свои знания и решить, нужно ли ему читать главу целиком. Если ответы на девять из десяти вопросов даны правильно, можно сразу же перейти к последнему разделу “Подготовка к экзамену”. Основные темы этой главы и предварительных контрольных вопросов перечислены в табл. 20.1. Отвечая на контрольные вопросы и используя таблицу, читатель сможет достаточно точно определить свои знания в той или иной области. Ответы на вопросы приведены в приложении А.

Таблица 20.1. Темы контрольных вопросов

Основная тема	Номера вопросов
Подключенные и статические маршруты	1,2
Обзор протоколов маршрутизации	3–6
Конфигурирование и проверка работы протокола RIP-2	7–10

1. Какое из указанных ниже требований должно выполняться, чтобы статический маршрут был установлен в таблицу маршрутизации устройства? (Выберите несколько ответов.)
 - a) Выходной интерфейс, указанный в маршруте, должен быть в состоянии “up\up”.
 - б) Маршрутизатор должен получить анонс маршрутизации от соседнего маршрутизатора.
 - в) В конфигурацию устройства должна быть добавлена команда `ip route`.
 - г) В команде `ip address` выходного интерфейса в конце должно быть добавлено ключевое слово `special`.
2. Какая из указанных ниже команд правильно задает статический маршрут в устройстве?
 - а) `ip route 10.1.3.0 255.255.255.0 10.1.130.253`.
 - б) `ip route 10.1.3.0 serial 0`.
 - в) `ip route 10.1.3.0 /24 10.1.130.253`.
 - г) `ip route 10.1.3.0 /24 serial 0`.
3. Какие из указанных ниже протоколов работают по дистанционно-векторному (distance vector) алгоритму? (Выберите несколько ответов.)
 - а) RIP.
 - б) IGRP.
 - в) EIGRP.
 - г) OSPF.
4. Какие из указанных ниже протоколов работают по алгоритму с учетом состояния каналов (link-state)? (Выберите несколько ответов.)
 - а) RIP.
 - б) RIP-2.
 - в) IGRP.
 - г) EIGRP.
 - д) OSPF.
 - е) IS-IS.
5. Какие из указанных ниже протоколов маршрутизации поддерживают технологию VLSM? (Выберите несколько ответов.)
 - а) RIP.
 - б) RIP-2.

- в) IGRP.
- г) EIGRP.
- д) OSPF.
- е) IS-IS.

6. Какие из указанных ниже протоколов маршрутизации склонны к быстрой конвергенции? (Выберите несколько ответов.)

- а) RIP.
- б) RIP-2.
- в) IGRP.
- г) EIGRP.
- д) OSPF.
- е) IS-IS.

7. У маршрутизатора №1 на интерфейсах установлены IP-адреса 9.1.1.1 и 10.1.1.1. Маршрутизатор №2 подключен к маршрутизатору №1 через последовательный канал, и на его интерфейсах установлены адреса 10.1.1.2 и 11.1.1.2. Какие из указанных команд нужно внести в конфигурацию протокола RIP-2 маршрутизатора №2, чтобы он рассыпал анонсы через все имеющиеся у него интерфейсы и анонсировал все сети? (Выберите несколько ответов.)

- а) router rip.
- б) router rip 3.
- в) network 9.0.0.0.
- г) version 2.
- д) network 10.0.0.0.
- е) network 10.1.1.1.
- ж) network 10.1.1.2.
- з) network 11.0.0.0.
- и) network 11.1.1.2.

8. Какой из указанных ниже вариантов команды `network`, введенной после команды `router rip`, заставит процесс маршрутизации протокола RIP рассыпать обновления маршрутных таблиц через интерфейсы с IP-адресами 10.1.2.1, 10.1.1.1 и маской 255.255.255.0?

- а) network 10.0.0.0.
- б) network 10.1.1.0 10.1.2.0.
- в) network 10.1.1.1.. 10.1.2.1.
- г) network 10.1.0.0 255.255.0.0.
- д) network 10..

з) Поставленная задача не может быть решена с помощью одной команды `network`.

9. Какая команда (или команды) выводит информацию, в которой указаны соседние маршрутизаторы, пересылающие обновления маршрутной информации данному маршрутизатору?

- а) show ip.
- б) show ip protocol.
- в) show ip routing-protocols.
- г) show ip route.
- е) show ip route neighbor.
- ж) show ip route received.

В выводе команды show ip route есть следующая строка:

R 10.1.2.0 [120/1] via 10.1.128.252, 00:00:13, Serial0/0/1

10. Какие утверждения справедливы для показанной записи в таблице маршрутов?
(Выберите несколько ответов.)

- а) Административное расстояние маршрута равно 1.
- б) Административное расстояние маршрута равно 120.
- в) Метрика маршрута равна 1.
- г) Метрика маршрута не указана.
- д) Маршрутизатор добавил эту запись в таблицу 13 секунд назад.
- е) Маршрутизатор анонсирует указанную сеть через 13 секунд.

Основные темы

Подключенные и статические маршруты

Чтобы процесс пересылки (или маршрутизации) работал, в таблицах маршрутизаторов должны присутствовать маршруты. Два основных источника маршрутной информации — это подсети, связанные с интерфейсами устройства, и маршруты, добавленные с помощью глобальных конфигурационных команд, называемые статическими маршрутами. В этом разделе описаны оба типа маршрутов, а в оставшейся части главы подробно рассмотрен третий метод получения маршрутов — динамические протоколы маршрутизации.

Маршруты к сетям, подключенными напрямую

Маршрутизатор автоматически добавляет в свою таблицу маршрутизации маршруты до подсетей, подключенных к его интерфейсам. Чтобы маршрут был добавлен в таблицу, IP-адрес и маска должны быть настроены на интерфейсе: статически с помощью команды `ip address` или динамически с помощью протокола DHCP, а оба кода состояния интерфейса должны быть в режиме “`up`” (работает). Концепция такого подхода очень проста: если у маршрутизатора есть интерфейс в какой-либо подсети, у него должен быть метод пересылки пакетов в такую подсеть, следовательно, ему нужен маршрут в таблице маршрутизации.

На рис. 20.1 показана структура сети, которая будет использоваться в примере 20.1 для иллюстрации маршрутов к сетям, подключенными к маршрутизатору непосредственно (*directly connected networks*) и демонстрации некоторых полезных команд `show`. Сеть на рис. 20.1 состоит из шести подсетей, подключенных к трем маршрутизаторам. В локальной сети (LAN) каждого маршрутизатора может быть один коммутатор, один концентратор или много коммутаторов и концентраторов и еще больше рабочих станций. На данном этапе детали локальных сетей и количество устройств в них не важны. После того как интерфейсы всех маршрутизаторов в представленной схеме сети будут настроены и нормально работать (находятся в состоянии “`up`”), у каждого из трех маршрутизаторов в таблице маршрутизации должно быть по три маршрута для подключенных к ним сетей.

В примере 20.1 показаны маршруты к сетям, подключенными напрямую к маршрутизатору *Albuquerque*, при этом предполагается, что для интерфейсов были правильно настроены IP-адреса, показанные на рис. 20.1. В примере также показаны дополнительные комментарии, а выводы команд подробно описаны ниже.

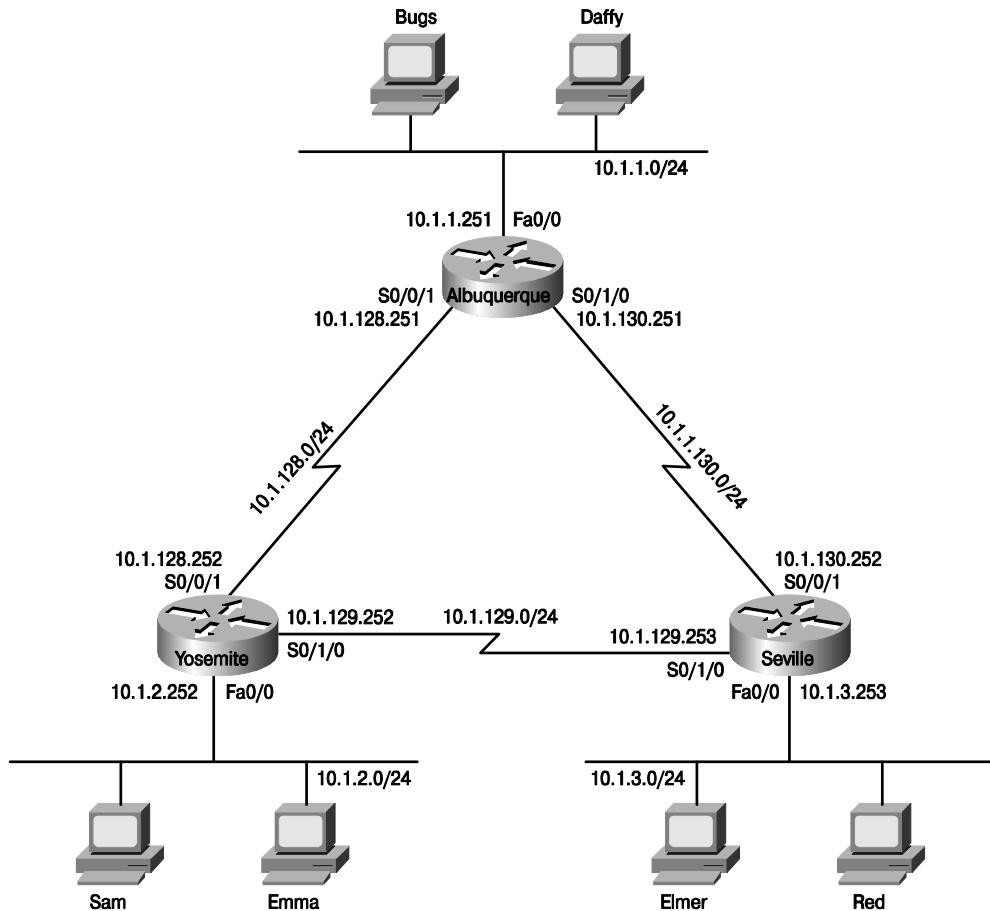


Рис. 20.1. Простая схема сети, используемая в примерах главы 20

Пример 20.1. Маршруты на сети, подключенные к маршрутизатору Albuquerque

! В команде ниже просто указаны IP-адреса интерфейсов маршрутизатора Albuquerque.
! Часть выводимой информации была опущена и оставлены только строки, связанные с интерфейсами, которые показаны на рис. 20.1.
!

```
Albuquerque#show running-config
interface FastEthernet0/0
  ip address 10.1.1.251 255.255.255.0
!
interface Serial 0/0/1
  ip address 10.1.128.251 255.255.255.0
!
interface Serial 0/1/0
  ip address 10.1.130.251 255.255.255.0
! Остальные строки вывода команды опущены.
!
! Следующая команда выводит список интерфейсов и лишний раз подтверждает,
```

! что три интерфейса маршрутизатора Albuquerque (см. рис. 20.1) находятся в состоянии "up и up" и им присвоены правильные IP-адреса.

!

Albuquerque#show ip interface brief

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	10.1.1.251	YES	manual	up	up
FastEthernet0/1	unassigned	YES	manual	administratively down	down
Serial0/0/0	unassigned	YES	NVRAM	administratively down	down
Serial0/0/1	10.1.128.251	YES	NVRAM	up	up
Serial0/1/0	10.1.130.251	YES	NVRAM	up	up
Serial0/1/1	unassigned	YES	NVRAM	administratively down	down

!

! Указанная ниже команда выводит все маршруты, известные маршрутизатору Albuquerque – все непосредственно подключенные к нему сети.

!

Albuquerque#show ip route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set

```
10.0.0.0/24 is subnetted, 3 subnets
C      10.1.1.0 is directly connected, FastEthernet0/0
C      10.1.130.0 is directly connected, Serial0/1/0
C      10.1.128.0 is directly connected, Serial0/0/1
```

!

! Используемая ниже команда меняет формат отображения маски в команде show ip route

!

Albuquerque#terminal ip netmask-format decimal

Albuquerque#show ip route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set

```
10.0.0.0 255.255.255.0 is subnetted, 3 subnets
C      10.1.1.0 is directly connected, FastEthernet0/0
C      10.1.130.0 is directly connected, Serial0/1/0
C      10.1.128.0 is directly connected, Serial0/0/1
```

Сначала обратимся к команде show ip interface brief в примере 20.1. Она подтверждает, что три интерфейса маршрутизатора Albuquerque соответствуют требованиям, при которых подключенные к ним сети будут занесены в таблицу мар-

шрутизации. Обратите внимание: для этих интерфейсов в кодах состояний указаны значения “up” и “up”, а также заданы IP-адреса.

В выводимой командой `show ip route` информации подтверждается, что у маршрутизатора `Albuquerque` есть три ожидаемых маршрута в таблице маршрутизации. Запись маршрута начинается с однобуквенного кода, в данном случае — буквы “C”, которая означает, что это подсоединенная к устройству сеть (от англ. `connected`). Все записи маршрутов начинаются с однобуквенного кода, по которому можно определить источник маршрута, в данном случае все три маршрута обозначены буквой “C”. Следует обратить внимание на то, что если для всех подсетей используется одинаковая маска, другими словами, *маска подсети постоянной длины* (*Static-Length Subnet Masking* — *SLSM*), то в команде `show ip route` маска выводится в строке сверху, т.е. там, где указана классовая сеть, а не во всех подсетях. В данном примере в строках с записями сетей `10.1.1.0`, `10.1.128.0` и `10.1.130.0` маска не выводится, но в строке над ними указана классовая сеть, в которую входят перечисленные подсети, в ней же и отображается маска для подсетей (см. выделенные строки в примере 20.1).

И наконец, по желанию можно сменить формат отображения маски в командах `show`. Такая настройка будет действовать на протяжении текущего сеанса связи с маршрутизатором, и вводится она с помощью команды `terminal ip netmask-format decimal`, как показано в конце примера 20.1.

ВНИМАНИЕ!

Чтобы хорошо подготовиться к экзамену, следует внимательно просматривать выводимую командами `show ip interface brief` и `show ip route` информацию в каждом из примеров текущей главы. В примере 20.6 ниже будут даны более подробные комментарии к результатам выполнения команды `show ip route`.

Статические маршруты

Маршруты, не подключенные к устройству сети, несомненно, важны, но маршрутизаторам также нужно знать маршруты к другим подсетям в сети, чтобы передавать туда пакеты. Так, например, рассматриваемый маршрутизатор `Albuquerque` вполне успешно отправляет пакеты эхо-запросов и получает ответы для адресов, находящихся на другом конце последовательного канала (*serial link*), или для IP-адресов из его локальной сети (`10.1.1.0/24`). Тем не менее команда `ping` вернет отрицательный результат для адресов сетей, не подключенных к данному маршрутизатору (пример 20.2). В примере 20.2 предполагается, что у маршрутизатора `Albuquerque` нет других маршрутов, помимо трех обсуждавшихся выше.

Пример 20.2. Команда ping дает положительный результат только для сетей, непосредственно подключенных к маршрутизатору `Albuquerque`

```
! Эхо-запросы отправляются на интерфейс S0/0/1 маршрутизатора Yosemite
Albuquerque#ping 10.1.128.252
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.128.252, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/8 ms
! Эхо-запросы отправляются на интерфейс Fa0/0 маршрутизатора Yosemite
Albuquerque#ping 10.1.2.252
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 10.1.2.252, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

Команда ping отправляет пакеты ICMP эхо-запросов по указанному IP-адресу получателя. Программное обеспечение стека TCP/IP станции-получателя отвечает на пакеты эхо-запросов похожим пакетом, который называется *пакетом ICMP эхо-ответа*. Команда ping отправляет первый пакет и ожидает ответа. Если ответ получен, в выводе команды отображается восклицательный знак (!). Если ответ не получен в течение стандартного интервала времени (2 секунды), то команда выводит точку (.). Обычно в программном обеспечении Cisco IOS пересылается пять таких пакетов.

В примере 20.2 команда ping 10.1.128.252 выдает положительный результат (т.е. выводит пять восклицательных знаков), поскольку в маршрутизаторе Albuquerque адрес получателя 10.1.128.252 попадает под маршрут на сеть 10.1.128.0/24. Команда ping 10.1.2.252 дает отрицательный результат, поскольку у маршрутизатора нет маршрута на сеть 10.1.2.0/24, в которой находится адрес 10.1.2.252. В результате устройство Albuquerque не может даже отправить пять пакетов-запросов, поэтому в выводе команды отображаются пять точек.

Самым простым и логичным решением этой проблемы будет конфигурирование какого-либо протокола маршрутизации на трех маршрутизаторах. Тем не менее для начала можно ограничиться конфигурированием статических маршрутов. В примере 20.3 показано конфигурирование двух команд ip route в режиме глобальной конфигурации маршрутизатора Albuquerque, с помощью которых добавляются два статических маршрута на локальные сети маршрутизаторов Yosemite и Seville. Конфигурирование указанных двух команд ip route приведет к тому, что команда ping во второй части примера 20.2 также будет возвращать положительный результат.

Пример 20.3. Настройка статических маршрутов для маршрутизатора Albuquerque



```
Albuquerque#configure terminal
Albuquerque(config)#ip route 10.1.2.0 255.255.255.0 10.1.128.252
Albuquerque(config)#ip route 10.1.3.0 255.255.255.0 10.1.130.253
Albuquerque#show ip route static
  10.0.0.0/24 is subnetted, 5 subnets
S      10.1.3.0 [1/0] via 10.1.130.253
S      10.1.2.0 [1/0] via 10.1.128.252
```

С помощью команды ip route в режиме глобальной конфигурации устройства задается адрес сети, маска и IP-адрес следующего транзитного узла (next-hop). Первая команда ip route задает маршрут на сеть 10.1.2.0 (с маской 255.255.255.0), которая находится “за” маршрутизатором Yosemite, следовательно, IP-адрес следующего транзитного узла для маршрутизатора Albuquerque будет равен 10.1.128.252, т.е. адресу интерфейса Serial0/0/1 маршрутизатора Yosemite. Аналогично маршрут на сеть 10.1.3.0/24, локальную сеть маршрутизатора Seville, указывает на IP-адрес интерфейса Serial0/0/1 устройства Seville, т.е. адрес 10.1.130.253. Обратите внимание на тот факт, что IP-адрес следующего транзитного узла (next-hop) должен находиться в непосредственно подключенной к маршрутизатору сети. На данном этапе маршрутизатор Albuquerque знает, куда отправлять пакеты для обеих подсетей.

Просмотреть все маршруты в таблице маршрутизации можно с помощью команды `show ip route`; команда `show ip route static` выводит только статические маршруты IP. Буква “S” в первой колонке означает, что маршруты были указаны статически (static). В действительности, чтобы маршруты были добавлены в таблицу маршрутизации, нужно не только настроить соответствующие команды `ip route`, но и выходной интерфейс, в сети которого находится транзитный маршрутизатор, указанный в команде, должен быть в состоянии “`up`” и “`up`” (т.е. такими должны быть два кода состояний маршрутизатора). Например, транзитный маршрутизатор для первой команды `ip route` устройства `Albuquerque` имеет IP-адрес `10.1.128.252`, входящий в подсеть интерфейса `S0/0/1` последнего. Если для интерфейса `S0/0/1` маршрутизатора `Albuquerque` не отображаются коды состояний “`up`” и “`up`”, то маршрут на указанную подсеть не будет занесен в таблицу маршрутизации.

Синтаксис команды `ip route` для двухточечных последовательных каналов может отличаться от указанного в примере выше. Для двухточечных каналов вместо IP-адреса следующего транзитного узла можно указать выходной интерфейс. Например, для первого маршрута в примере 20.3 вместо использовавшейся команды можно указать команду `ip route 10.1.2.0 255.255.255.0 serial0/0/1`, и результат будет абсолютно одинаковым.

К сожалению, конфигурирование статических маршрутов в устройстве `Albuquerque` не решает всех проблем с маршрутизацией в рассматриваемой сети. На двух оставшихся маршрутизаторах также нужно настроить статические маршруты. На данный момент у маршрутизатора `Albuquerque` есть статические маршруты, через которые он может пересыпать пакеты в две дистанционные локальные сети, но два оставшихся маршрутизатора маршрутов к локальным сетям друг друга и маршрутизатора `Albuquerque` не имеют. Например, из локальной сети маршрутизатора `Albuquerque` (рабочая станция с названием `Bugs`) не может переслать эхо-запросы в локальную сеть маршрутизатора `Yosemite` (станция с названием `Sam`). Проблема состоит в следующем: несмотря на то что у маршрутизатора `Albuquerque` есть маршрут на подсеть `10.1.2.0` (в которой находится станция `Sam`), у маршрутизатора `Yosemite` нет маршрута на локальную подсеть `10.1.1.0` (в которой находится станция `Bugs`). От станции `Bugs` до станции `Sam` пакеты эхо-запросов доходят вполне успешно, а вот ответы на них от станции `Sam` не могут быть перенаправлены маршрутизатором `Yosemite` по обратному пути, поскольку у него нет маршрута на нужную подсеть в таблице маршрутизации — команда `ping` возвращает отрицательный результат.

Расширенный вариант команды ping

На практике сетевой администратор вряд ли сможет найти дружелюбного пользователя (например, пользователя компьютера `Bugs` на используемой нами схеме сети), который согласится по требованию запускать программу `ping` со своего компьютера для проверки сети. Кроме того, зачастую очень проблематично и неэффективно физически путешествовать от филиала к филиалу (например, за сотни километров), чтобы выполнить команду `ping` на компьютере пользователя и посмотреть, как проходят эхо-запросы. В качестве альтернативы можно использовать следующий подход: подключиться с помощью программы `Telnet` к ближайшему к пользователю маршрутизатору и использовать команду `ping` для проверки работоспособности сети. Команда в качестве адреса отправителя будет подставлять адрес выходного интерфейса маршру-

тизатора, а иногда нужно проверить, как проходят пакеты через устройство из определенного сегмента сети. Решение такой задачи может быть получено с помощью расширенной команды ping, в которой есть дополнительные возможности.

Расширенный вариант команды доступен в операционной системе Cisco IOS из режима привилегированного пользователя. Он позволяет указывать множество опциональных параметров, в частности, указать явно IP-адрес отправителя для пакетов ICMP, количество пересылаемых пакетов, время ожидания ответов и др. В примере 20.4 показано отличие двух вариантов команды: сначала в маршрутизаторе Albuquerque используется стандартная команда, ping 10.1.2.252, потом — расширенная команда ping, которая работает так, как если бы она была запущена с компьютера Bugs, а в качестве получателя указывается компьютер Sam. Во втором случае команда дает отрицательный результат, поскольку маршрутизатор Yosemite не может отправить пакеты ICMP эхо-ответов устройству Albuquerque по обсуждавшейся выше причине.

Пример 20.4. Маршрутизатор Albuquerque: команда ping работает после добавления стандартных маршрутов, расширенный вариант команды дает отрицательный результат

```
Albuquerque#show ip route static
10.0.0.0/24 is subnetted, 5 subnets
S 10.1.3.0 [1/0] via 10.1.130.253
S 10.1.2.0 [1/0] via 10.1.128.252
Albuquerque#ping 10.1.2.252

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.2.252, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/8 ms

Albuquerque#ping
Protocol [ip]:
Target IP address: 10.1.2.252
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 10.1.128.251
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose [none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.2.252, timeout is 2 seconds:
. . .
Success rate is 0 percent (0/5)
```

Простой (т.е. стандартный) вариант команды, ping 10.1.2.252, дает положительный результат (т.е. на запросы приходят ответы) по двум причинам: одна из них очевидна, вторая — не совсем. Маршрутизатор Albuquerque пересыпает пакет в подсеть 10.1.2.0, поскольку у него есть статический маршрут на нее. Обратный пакет, отправленный маршрутизатором Yosemite, пересыпается на адрес 10.1.128.251 — IP-

адрес интерфейса Serial0/0/1 маршрутизатора Albuquerque. Почему? На то есть две указанные ниже причины.

- Команда `ping` в маршрутизаторах Cisco использует IP-адрес выходного интерфейса в качестве адреса отправителя, если адрес не указан в команде `ping` явно. Первая команда `ping` в примере 20.4 использует адрес отправителя 10.1.128.251, поскольку маршрут, используемый в маршрутизаторе Albuquerque, указывает на интерфейс Serial0/0/1 в качестве выходного интерфейса, и его адрес как раз и равен указанному значению.
- В ответах на эхо-запросы IP-адреса меняются местами. Следовательно, раз IP-адрес 10.1.128.251 маршрутизатора Albuquerque был использован в качестве адреса отправителя для пакетов запросов, то маршрутизатор Yosemite будет использовать адрес 10.1.128.251 в качестве адреса получателя в пакетах эхо-ответов. Сеть 10.1.128.0/24 для маршрутизатора Yosemite является сегментом, подключенным напрямую, т.е. у него есть интерфейс в этой сети, следовательно, устройство знает маршрут к ней и может отправить пакет по назначению.

В процессе поиска и устранения неисправностей расширенный вариант команды `ping` может использоваться так, чтобы пакеты выглядели, будто они были отправлены из какой-то определенной сети, но при этом не нужно было просить кого-то выполнить команду на своем компьютере в сети. Такой вариант команды может быть использован для уточнения причин и точной диагностики проблемы в сети. Например, в реальной сети, когда команда `ping` дает положительный результат, т.е. пакеты проходят, при запуске с маршрутизатора без дополнительных параметров, а при запуске с персонального компьютера пакеты не проходят, с помощью расширенного варианта команды `ping` можно воссоздать нужную ситуацию без общения с пользователем по телефону и долгих объяснений, что и как нужно запустить на компьютере.

Как показано в примере 20.4, в расширенном варианте команды `ping` в качестве адреса отправителя пакетов используется IP-адрес 10.1.1.251 (т.е. адрес интерфейса Fa0/0 маршрутизатора Albuquerque), а в качестве получателя — 10.1.2.252 (т.е. адрес интерфейса Fa0/0 маршрутизатора Yosemite). По выводимой командой информации видно, что ответы на эхо-запросы не получены. При этом ответы от обычного варианта команды `ping` успешно принимаются, поскольку для отправки запросов в качестве адреса отправителя используется IP-адрес выходного интерфейса маршрутизатора Albuquerque. В первом случае (расширенный вариант) запросы ICMP приходят как бы из подсети 10.1.1.0, т.е. с точки зрения маршрутизатора и его таблицы маршрутизации запросы идут от пользовательской станции в соответствующем сегменте. Маршрутизатор Yosemite строит ответ таким образом, что адрес получателя равен 10.1.1.251, но в этом маршрутизаторе нет маршрута на сеть 10.1.1.0/24. Поэтому устройство не может отправить ответ на эхо-запрос, и команда выдает отрицательный результат.

Решением описанной проблемы будет добавление статического маршрута в маршрутизаторе Yosemite на сеть 10.1.1.0/24 или включение какого-либо протокола динамической маршрутизации на всех трех маршрутизаторах.

Стандартные маршруты

Процесс маршрутизации предполагает, что маршрутизатор сравнивает IP-адрес получателя пакета с таблицей маршрутизации. Если маршрутизатор не обнаружива-

ет в своей таблице маршрут на сеть получателя, такой пакет будет отброшен и попытка как-то исправить ситуацию не предпринимается.

Стандартный маршрут (default route) — это маршрут, с которым “совпадает” любой IP-адрес получателя. Если в таблице маршрутизации есть стандартный маршрут, то когда для пакета с определенным IP-адресом получателя нет явного маршрута в таблице маршрутизации, маршрутизатор пересыпает такой пакет на стандартный маршрут.

Стандартные маршруты лучше всего работают в том случае, если к какой-либо части сети есть всего один путь или один канал. Например, как показано на рис. 20.2, маршрутизатор филиала R1 подключен единственным последовательным каналом к корпоративной сети. Сотни сетей могут существовать в корпоративной сети вне филиала и быть доступны через маршрутизатор R1. У сетевого инженера в такой ситуации есть три варианта реализации механизмов маршрутизации:

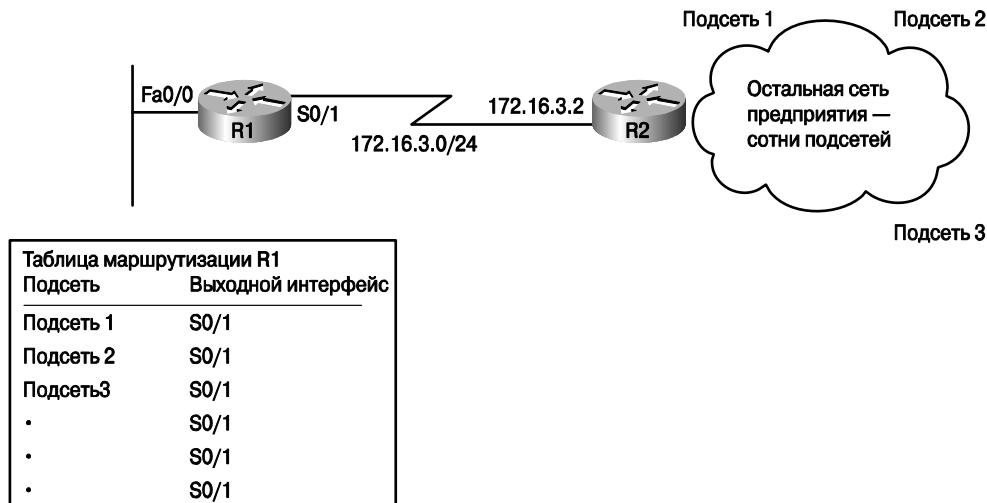


Рис. 20.2. Пример сети, в которой следует использовать стандартный маршрут

- настроить сотни статических маршрутов на маршрутизаторе R1; все такие маршруты будут использовать интерфейс S0/1 маршрутизатора R1 в качестве выходного интерфейса и IP-адрес следующего транзитного узла 172.16.3.2 (R2);
- включить и настроить какой-либо протокол динамической маршрутизации на маршрутизаторах;
- добавить стандартный маршрут на маршрутизаторе R1 с указанием в качестве выходного интерфейса порта S0/1.

Если задан специальный статический маршрут, называемый стандартным, то у маршрутизатора R1 будет всего один маршрут, по которому он будет через интерфейс S0/1 пересыпать пакеты устройству R2. В команде `ip route` в данном случае указано специальное значение для сети и маски, 0.0.0.0, под которое попадают все пакеты. В примере 20.5 показан стандартный статический маршрут маршрутизатора R1, указывающий на маршрутизатор R2 (172.16.3.2) как на следующий по маршруту транзитный узел.

Пример 20.5. Статический стандартный маршрут для маршрутизатора R1 и таблица маршрутизации

```
R1(config)#ip route 0.0.0.0 0.0.0.0 172.16.3.2
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
      * - candidate default, U - per-user static route, o - ODR
      P - periodic downloaded static route

Gateway of last resort is 172.16.3.2 to network 0.0.0.0

172.16.0.0/24 is subnetted, 3 subnets
C    172.16.1.0 is directly connected, FastEthernet0/0
C    172.16.3.0 is directly connected, Serial0/1
S*   0.0.0.0/0 [1/0] via 172.16.3.2
```

С помощью команды `show ip route` можно увидеть пару интересных фактов о специальном статическом стандартном маршруте. В выводимой командой информацией для маршрута указан код S, как и для любого другого статического маршрута, но для маршрута также указан символ *. Символ * означает, что маршрут может быть использован в качестве стандартного (default), т.е. по нему будут пересыпаться пакеты, для адресов получателей которых нет в явном виде записи маршрута на соответствующую сеть в таблице маршрутизации. При наличии стандартного маршрута в таблице маршрутизации устройство будет отправлять пакеты, получатели которых не совпадают с имеющимися маршрутами, следовательно, в рассматриваемом примере стандартный маршрут будет покрывать все корпоративные сети.

ВНИМАНИЕ!

Стандартные маршруты подробнее описаны во втором томе книги.

Статические стандартные маршруты, как и обычные статические маршруты, можно использовать на всех устройствах в телекоммуникационной сети, но традиционно в сетях предприятий используется какой-либо динамический протокол маршрутизации для построения таблиц маршрутизации. В следующем разделе описаны концепции и терминология динамических протоколов маршрутизации.

Обзор протоколов маршрутизации

У всех протоколов динамической маршрутизации одна цель — заполнять таблицу маршрутизации актуальными оптимальными маршрутами. Цель проста, но процессы и их детали могут быть очень сложными.

Протоколы маршрутизации позволяют маршрутизаторам изучать маршруты за счет того, что каждый маршрутизатор анонсирует (т.е. рассыпает) те маршруты, которые у него есть. Каждое устройство быстрее всего узнает свои собственные маршруты, т.е. маршруты к сетям, подключенными к нему напрямую (directly connected). Далее, каждый маршрутизатор рассыпает сообщения, формат и структура которых

определяется конкретным протоколом маршрутизации. Устройство, принимающее такие обновления маршрутной информации от других маршрутизаторов, добавляет обнаруженные таким образом маршруты в свою таблицу маршрутизации. Если все маршрутизаторы в сети участвуют в таком процессе, в итоге все маршрутизаторы получат информацию обо всех подсетях в сети.

Обнаруживая и пересылая маршрутную информацию, протоколы маршрутизации должны обеспечить отсутствие кольцевых маршрутов, зачастую называемых *петлями маршрутизации* (routing loop). Кольцевым считается маршрут, в котором пакет возвращается к тому маршрутизатору, который его отправил, из-за ошибок в маршрутах в таблицах маршрутизации многих устройств. Кольцевые маршруты — нормальное явление в маршрутизируемых сетях, хотя одна из важных задач протоколов маршрутизации — обеспечить маршруты без петель.

В этом разделе в качестве первого примера протокола маршрутизации описан RIP-2 чуть более подробно, чем в главе 5. Ниже приведено подробное сравнение различных протоколов маршрутизации.

Основные концепции протокола RIP-2

Маршрутизаторы, на которых запущен протокол маршрутизации RIP-2, анонсируют небольшие порции простой информации о каждой известной им подсети соседним устройствам. Соседние маршрутизаторы в свою очередь анонсируют такую информацию своим соседям и так далее, пока все маршрутизаторы в сети не изучат имеющиеся у других устройств маршруты. Фактически такой механизм похож на процесс распространения слухов в каком-то районе, школе или компании. Кто-то вышел на улицу выгулять собаку, встретил на лестничной клетке соседа, выносящего ведро с мусором, и рассказал ему свежую сплетню. Сосед, чуть позже отправившись в магазин за хлебом, в свою очередь встречает другого соседа и передает ему только что услышанную сплетню и так далее, до тех пор, пока слух не распространится по всему дому. Дистанционно-векторные протоколы маршрутизации, в частности RIP, работают аналогичным образом, но в отличие от слухов, распространяющихся между соседями, маршрутная информация не искажается при передаче.

Например, рассмотрим схему и процесс передачи информации на рис. 20.3. Здесь показано, как протокол RIP-2 анонсирует адрес подсети и маску (записанную в префиксном формате), а также метрику маршрута “соседям”.

Чтобы не перегружать схему обилием информации, на рис. 20.3 показана рассылка маршрутизаторами маршрута к сети 172.16.3.0/24, но следует помнить, что устройства рассыпают маршруты и других сетей. Процесс рассылки выглядит следующим образом.

1. Маршрутизатор R2 обнаруживает маршрут на непосредственно подключенную к нему подсеть 172.16.3.0/24.
2. Маршрутизатор R2 рассыпает *анонс маршрутизации* (routing update) своим “соседям”, в котором указаны подсеть (172.16.3.0), маска (/24) и расстояние до нее, т.е. метрика (в данном случае 1).
3. Маршрутизатор R3 принимает анонс маршрутизации и добавляет маршрут на сеть 172.16.3.0/24 в свою таблицу маршрутизации, а в качестве следующего *транзитного узла* (next hop) на маршруте указывает маршрутизатор R3.

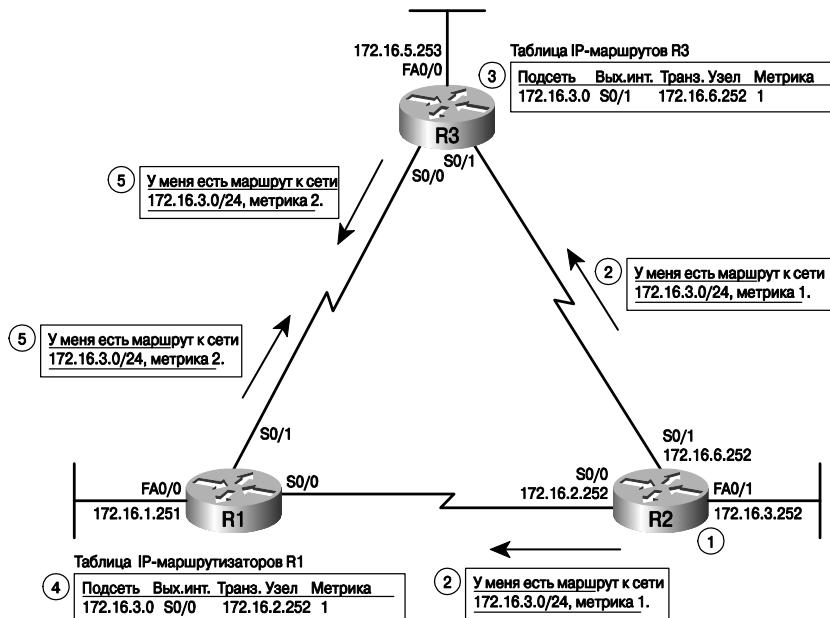


Рис. 20.3. Пример рассылки маршрутов протоколом RIP-2

4. Приблизительно в то же время маршрутизатор R1 получает анонс, отправленный устройством R2. Маршрутизатор R1 добавляет маршрут на подсеть 172.16.3.0/24 в свою таблицу маршрутизации и указывает маршрутизатор R2 в качестве следующего транзитного узла на пути к подсети.
5. В finale маршрутизаторы R1 и R3 обмениваются информацией о маршрутах к сети 172.16.3.0/24 друг с другом, но уже с метрикой 2.

После завершения процесса обмена у маршрутизаторов R1 и R3 будет два возможных маршрута к подсети 172.16.3.0/24: один с метрикой 1, а второй с метрикой 2. Каждый из маршрутизаторов использует соответствующий маршрут с минимальной метрикой (т.е. равной 1) для сети 172.16.3.0.

Следует запомнить, что дистанционно-векторные протоколы, в том числе и RIP-2, периодически повторяют такой процесс рассылки. Например, маршрутизаторы с включенным протоколом RIP пересыпают такие периодические анонсы раз в 30 секунд. Если маршрутизаторы получают те же маршруты с теми же самыми метриками, то они не перестраивают свои таблицы маршрутизации. Тем не менее, если что-то происходит и маршрутная информация меняется, следующий анонс маршрутизации или вызовет изменения в таблице соседних устройств, или не дойдет вообще, и устройства отреагируют на потерю маршрута пересмотром известной им информации.

Итак, основной принцип работы протокола маршрутизации нам уже известен, ниже мы рассмотрим несколько особенностей различных протоколов маршрутизации.

Сравнение разных протоколов маршрутизации

Долгая история протокола IP и его огромная популярность привели к возникновению в разные периоды времени нескольких конкурирующих протоколов маршрутизации.

тизации. Проще всего запомнить протоколы маршрутизации и оценить их возможности, сравнивая их преимущества и недостатки. В этом разделе описаны некоторые технические моменты, на основе которых можно сравнивать протоколы, а ниже подробно описан протокол RIP-2. Протоколы маршрутизации OSPF и EIGRP подробно описаны во втором томе книги.

Первый критерий, по которому можно сравнивать протоколы, — его открытость. Например, если протокол описан в документах RFC, то он представляет собой открытый стандарт, другой вариант — собственный протокол, например, его разработала компания Cisco, и он защищен патентами. Второй критерий связан с механизмами работы протокола: поддерживает ли протокол *маски подсети переменной длины* (Variable-Length Subnet Masking — VLSM). Технология VLSM подробно описана только во втором томе книги, тем не менее, это одна из самых важных характеристик любого протокола маршрутизации на сегодняшний день. В этом разделе описаны наиболее важные термины и концепции протоколов, которые используются для описания и сравнения протоколов маршрутизации, а в табл. 20.4 приведено сравнение наиболее распространенных протоколов.

Протоколы маршрутизации внешнего и внутреннего шлюзов

Все протоколы маршрутизации можно отнести к одному из двух классов:



Определения протоколов IGP и EGP

- *протоколы маршрутизации внутреннего шлюза* (Interior Gateway Protocol — IGP) предназначены для маршрутизации в автономной системе, т.е. это протоколы локального уровня;
- *протоколы маршрутизации внешнего шлюза* (Exterior Gateway Protocol — EGP) отвечают за маршрутизацию между автономными системами.

ВНИМАНИЕ!

В терминах IGP и EGP используется такое понятие, как *шлюз*, потому что раньше маршрутизаторы называли *шлюзами* (gateway), но на сегодняшний день такое название устарело.

В приведенных выше определениях используется специфический термин *автономная система* (autonomous system). Под автономной системой понимают сеть или набор сетей под единым административным управлением, обычно относящихся к одной организации. Например, сеть или сетевой комплекс, созданные и оплачиваемые какой-либо одной компанией, скорее всего, будет автономной системой; сеть, принадлежащая крупному учебному заведению, также, скорее всего, будет представлять собой единую автономную систему. В качестве дополнительных примеров автономных систем можно указать крупные государственные и правительственные организации, транснациональные корпорации и другие, хотя государственные службы могут строить свои независимые сети.

Итак, некоторые протоколы лучше всего работают именно в одной автономной системе благодаря своим механизмам и структуре, поэтому их называют протоколами IGP. Всего только один протокол лучше всего работает в качестве средства мар-

шрутизации между автономными системами — это протокол граничного шлюза (Border Gateway Protocol — BGP).

Каждой автономной системе может быть присвоен номер, называемый (что неудивительно!) номером автономной системы (Autonomous System Number — ASN). Как и зарегистрированные IP-адреса, номера ASN выдает Ассоциация по присвоению имен и номеров портов Интернета (Internet Corporation for Assigned Network Numbers — ICANN), которая делегировала выдачу номеров, точно так же, как и зарегистрированных IP-адресов своим региональным представительствам. За счет присвоения каждой автономной системе уникального номера в протоколе BGP может быть гарантировано, что пакет не зацикляется в глобальной сети Интернет и не будет проходить через ту же автономную систему дважды.

На рис. 20.4 показана уменьшенная схематическая модель всемирной сети Интернет. Одна компания и три провайдера услуг Интернета (Internet Service Provider — ISP) используют протоколы IGP (OSPF и EIGRP) в собственных сетях, а между их автономными системами используется протокол BGP.

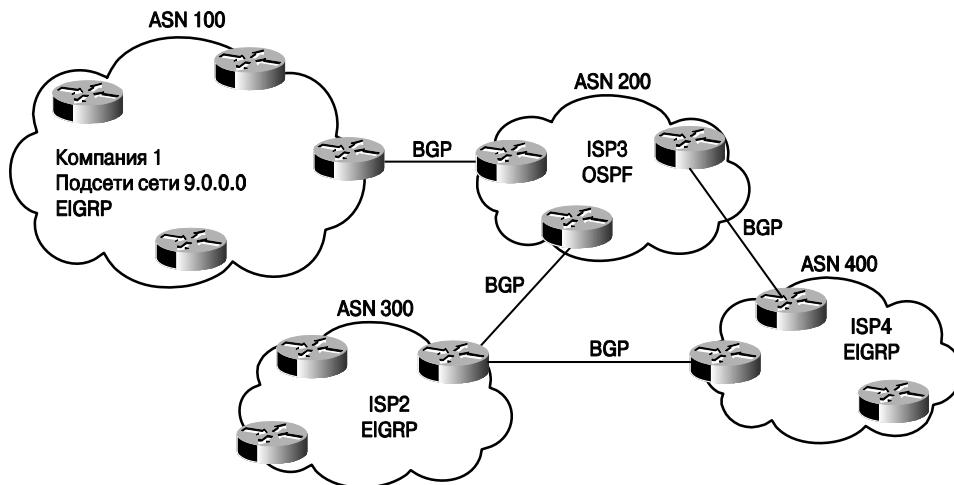


Рис. 20.4. Сравнение расположений с использованием протоколов IGP и EGP

Типы и алгоритмы протоколов маршрутизации

Все протоколы IGP могут быть отнесены к определенному классу, или типу, в соответствии с алгоритмом работы. В табл. 20.2 описаны три возможных варианта работы протоколов и приведены примеры протоколов для каждого класса.



Таблица 20.2. Классификация протоколов маршрутизации на основе алгоритмов их работы

Класс/Алгоритм	Пример протокола
Дистанционно-векторный (Distance vector)	RIP-1, RIP-2, IGRP
С учетом состояния каналов (Link-state)	OSPF, Integrated IS-IS
Сбалансированный гибридный (иногда называемый расширенным дистанционно-векторным)	EIGRP

Во втором томе подробно описаны теория и алгоритмы работы практических всех перечисленных выше протоколов маршрутизации. Тем не менее, поскольку в первом томе детально рассматривается только протокол RIP-2, фактически ниже подробно рассмотрен только класс дистанционно-векторных протоколов маршрутизации.

Метрики

Протоколам маршрутизации нужен некоторый механизм, который позволит выбрать наилучший маршрут, если маршрутизатор обнаружил несколько маршрутов к какой-либо подсети. Для этой цели в протоколах маршрутизации используется параметр, называемый *метрикой* (metric), определяющий “предпочтительность” маршрута. Чем меньше метрика, тем лучше маршрут. Так (см. рис. 20.3), маршрутизатор R1 обнаружил маршрут с метрикой 1 к подсети 172.16.3.0/24 от маршрутизатора R2 и маршрут к той же подсети с метрикой 2 через маршрутизатор R3. Устройство R1 выберет и установит в таблицу маршрутизации маршрут с меньшей метрикой (1) через маршрутизатор R2.

Некоторые метрики являются более оптимальными. Чтобы проиллюстрировать такое утверждение, обратимся к рис. 20.5. На рисунке показан процесс анализа некоторой сети с точки зрения выбора маршрутизатором В маршрута к подсети 10.1.1.0, расположенной в локальной сети слева от маршрутизатора А. В рассматриваемом примере скорость канала между маршрутизаторами А и В составляет всего 64 Кбит/с, а два оставшихся канала работают на скорости T1, т.е. 1,544 Мбит/с каждый. На верхней схеме на рис. 20.5 показано, какой маршрут выберет маршрутизатор В, если он использует протокол маршрутизации RIP (версии 1 или 2, неважно), а на нижней схеме — какой из маршрутов будет использоваться в протоколе EIGRP.

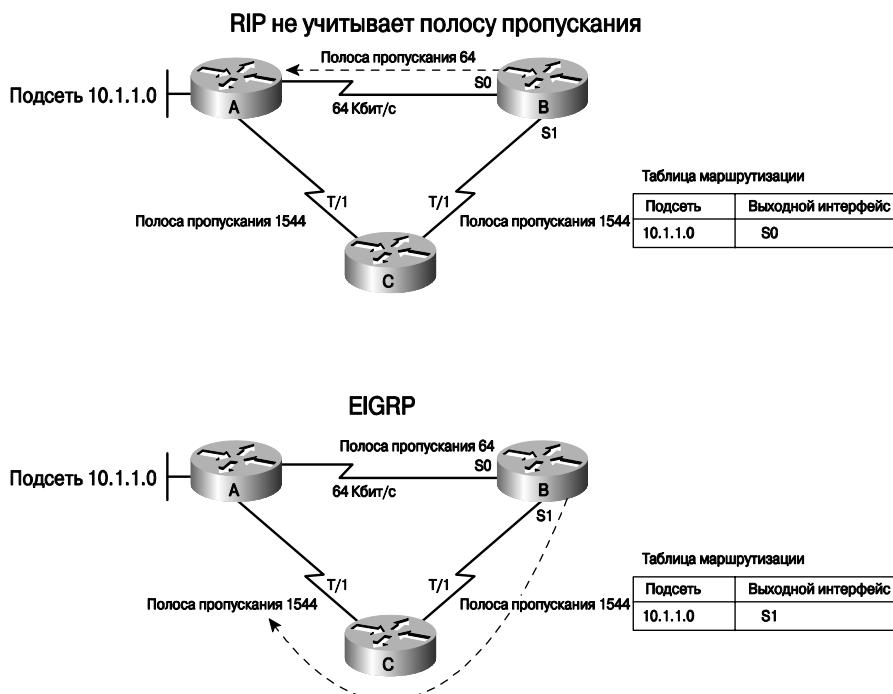


Рис. 20.5. Сравнение метрик протоколов RIP и EIGRP

В протоколе маршрутизации RIP используется метрика, называемая *счетчиком транзитных узлов* (hop count), в которой учитывается, через сколько маршрутизаторов (транзитных узлов — hop) пролегает маршрут к какой-либо подсети. При использовании протокола RIP маршрутизатор В обнаружит два маршрута к подсети 10.1.1.0: маршрут с одним транзитным переходом через маршрутизатор А и маршрут с двумя транзитными переходами через маршрутизатор С. Итак, если маршрутизатор В использует протокол RIP, то с его точки зрения оптимальным маршрутом к сети 10.1.1.0 будет путь через маршрутизатор А в качестве следующего транзитного узла (показан пунктирной линией на рис. 20.5).

Протокол EIGRP использует метрику, в которой стандартно учитываются полоса пропускания и кумулятивная задержка для маршрута через интерфейс и подаются на вход некоторого математического алгоритма для расчета метрики. Если в маршрутизаторах А, В и С на интерфейсах корректно указана команда `bandwidth`, то, как показано на рис. 20.5, протокол EIGRP установит в таблицу маршрутизации оптимальный с его точки зрения маршрут через маршрутизатор С с использованием каналов большей пропускной способности (обозначен пунктиром на нижней схеме).

ВНИМАНИЕ!

Команда `bandwidth` подробно описана в главе 19.

Автоматическое суммирование и суммирование вручную

Чем меньше таблица маршрутизации, тем быстрее работают маршрутизаторы. Суммирование (или агрегирование) маршрутов может заметно уменьшить размер таблицы маршрутизации, но сохранить маршрутную информацию.

Существуют два метода суммирования маршрутов. Какой метод суммирования доступен, зависит от конкретного протокола маршрутизации: *автоматическое суммирование* (*autosummarization*) и *суммирование вручную* (*manual summarization*). Суммирование маршрутов вручную дает сетевому инженеру прекрасную возможность самостоятельно контролировать таблицы маршрутов и строить наиболее гибкую маршрутизацию в сети, например, выбирать, какие суммарные маршруты будут анонсироваться, а не пересылать только маршруты классовых сетей. Таким образом, поддержка возможности суммирования маршрутов вручную на сегодняшний день является важным фактором при выборе протокола маршрутизации в сети.

В главе 6 второго тома описаны автоматическое суммирование и агрегирование маршрутов вручную.

Классовые и бесклассовые протоколы маршрутизации

Некоторые протоколы маршрутизации должны учитывать класс сети при маршрутизации. Другие протоколы маршрутизации игнорируют классовый признак сети. Протоколы маршрутизации, в которых используются правила для классовых сетей, называют *классовыми протоколами маршрутизации* (*classful routing protocol*); протоколы, не учитывающие класс сети, называют *бесклассовыми протоколами маршрутизации* (*classless routing protocol*).

Классовые и бесклассовые протоколы маршрутизации различают по трем критериям, перечисленным в табл. 20.3.



Таблица 20.3. Сравнение классовых и бесклассовых протоколов маршрутизации

Функция	Бесклассовый протокол	Классовый протокол
Поддерживает маски VLSM	Да	Нет
Пересыпает маску подсети в анонсах маршрутизации	Да	Нет
Поддерживает суммирование маршрутов вручную	Да	Нет

Конвергенция

Термином *конвергенция* (convergence) описывают процесс, происходящий в протоколе маршрутизации, когда что-то меняется в топологии сети. Когда канал начинает работать или разрывается, или когда маршрутизатор включается, или происходит отказ, возможные маршруты в сети, очевидно, изменяются. Процесс обнаружения изменений в сети, поиска и установки в таблицы маршрутизации оптимальных маршрутов, изменения таблиц маршрутизации называется конвергенцией. Конвергенция фактически определяет, как быстро маршрутизаторы в сети с определенным протоколом маршрутизации согласуют свои таблицы маршрутизации.

Некоторые протоколы маршрутизации осуществляют конвергенцию быстрее, чем другие. Вполне очевидно, что чем быстрее протокол маршрутизации осуществляет конвергенцию, тем лучше, поскольку во многих случаях, если маршрутизаторы не согласовали свои таблицы (т.е. не осуществили конвергенцию), пользователь не сможет пересыпать пакеты в какие-то подсети. (В табл. 20.4 описана относительная скорость конвергенции разных протоколов маршрутизации, а также другая полезная информация.)

Дополнительные параметры для сравнения

Есть еще два не самых важных параметра, которые могут быть использованы для сравнения разных протоколов IGP. Прежде всего следует отметить, что в стандартах некоторых протоколов указано, что обновления таблиц маршрутизации должны отправляться на широковещательный адрес, который прослушивают все сетевые хосты, — 255.255.255.255. После того как такой механизм был заложен в некоторые из протоколов маршрутизации, появились методы многоадресатной рассылки сообщений (multicast), поэтому в более новых протоколах маршрутизации анонсы маршрутизации рассылаются только заинтересованным в них хостам с использованием специальных зарезервированных многоадресатных IP-адресов. Это первый параметр для сравнения протоколов.

Старые протоколы маршрутизации в локальных сетях не поддерживали функций аутентификации. Время шло, и становилось понятно, что злоумышленники могут организовать атаки на *отказ в обслуживании* (Denial-of-Service — DoS) с использованием протоколов маршрутизации. Например, атакующий может подключить маршрутизатор к сети и анонсировать множество маршрутов с маленькой метрикой для огромного количества подсетей, следовательно, пакеты будут перенаправляться по неправильным маршрутам и, возможно, будут перехвачены злоумышленником. В более новых протоколах IGP обычно есть поддержка некоторого типа аутентификации для защиты от таких типов атак на отказ в обслуживании (DoS).

Резюме по протоколам маршрутизации внутреннего шлюза

Для удобства сравнения и подготовки к экзамену в табл. 20.4 перечислены основные характеристики протоколов маршрутизации внутреннего шлюза. Следует запомнить, что наиболее важным для сертификационного экзамена ICND1 является протокол маршрутизации RIP, а именно RIP-2. А в экзаменах ICND2 и CCNA попадаются более сложные вопросы по теории работы протокола маршрутизации RIP-2, а также по теории, конфигурированию и устранению неисправностей протоколов OSPF и EIGRP.



Таблица 20.4. Сравнение протоколов маршрутизации внутреннего шлюза

Характеристика	RIP-1	RIP-2	EIGRP	OSPF	IS-IS
Бесклассовый	Нет	Да	Да	Да	Да
Поддерживает маски VLSM	Нет	Да	Да	Да	Да
Пересыпает маску в анонсах маршрутов	Нет	Да	Да	Да	Да
Дистанционно-векторный	Да	Да	Нет ¹	Нет	Нет
С учетом состояния каналов	Нет	Нет	Нет	Да	Да
Поддерживает автоматическое суммирование	Да	Да	Да	Нет	Нет
Поддерживает суммирование маршрутов вручную	Нет	Да	Да	Да	Да
Собственный (т.е. закрытый)	Нет	Нет	Да	Нет	Нет
Обновления таблицы маршрутизации пересыпаются на многоадресатный адрес	Нет	Да	Да	Да	-
Поддерживается аутентификация	Нет	Да	Да	Да	Да
Конвергенция	Медленная	Медленная	Очень быстрая	Быстрая	Быстрая

ВНИМАНИЕ!

Протоколу IGRP присущи те же характеристики, которые указаны в табл. 20.4 для протокола RIP-1. Единственное отличие двух протоколов — IGRP является собственным (и закрытым патентами), а RIP — нет.

Конфигурирование и проверка работы протокола RIP-2

Конфигурирование протокола RIP-2 с какой-то точки зрения намного проще, чем теория протоколов маршрутизации. В конфигурации используются всего три команды, а в действительности только одна из них, команда `network`, является самой важной. Тем не менее для практической работы понадобится несколько полезных команд группы `show`, которые чаще всего используются для анализа сети, процесса маршрутизации, а также для поиска и устранения неисправностей.

¹ Протокол EIGRP относят к классу сбалансированных гибридных протоколов, у которых есть как признаки дистанционно-векторных, так и протоколов с учетом состояния канала. В некоторых книгах и документации EIGRP называют расширенным дистанционно-векторным протоколом маршрутизации. — Примеч. авт.

Конфигурирование протокола RIP-2

Запустить протокол маршрутизации RIP версии 2 (RIP-2) очень просто: нужно выполнить всего три обязательные команды, которые представлены в виде формализованного процесса ниже.



Этапы настройки протокола маршрутизации RIP-2

- Этап 1** В режиме глобальной конфигурации следует ввести команду `router rip`, чтобы перейти в режим конфигурирования протокола маршрутизации.
- Этап 2** В режиме конфигурирования протокола маршрутизации следует ввести команду `version 2`, чтобы указать, что будет использоваться исключительно версия 2 протокола.
- Этап 3** Ввести одну или больше команд `network адрес_сети`, чтобы включить протокол RIP на правильных интерфейсах.
- Этап 4** Необязательный этап. Если это необходимо, можно отключить протокол маршрутизации RIP на интерфейсе с помощью команды `passive-interface тип номер`.

Из всех перечисленных выше этапов только третий, команда `network`, требует серьезного обдумывания перед ее введением. Каждая команда `network` включает протокол RIP для набора интерфейсов. В качестве параметра в этой команде можно указать только адрес классовой сети. Для любого интерфейса в рамках такой классовой сети маршрутизатор будет выполнять следующие действия:



Три действия, выполняемые для интерфейса, который включен в процесс маршрутизации протокола RIP

- рассыпать обновления маршрутизации на зарезервированный многоадресатный IP-адрес 224.0.0.9 через интерфейс;
- прослушивать входящие обновления на том же интерфейсе;
- анонсировать подсеть, настроенную на интерфейсе.

Пример конфигурации протокола RIP

Помня об указанных фактах, попробуем настроить протокол маршрутизации RIP на одном маршрутизаторе. Рассмотренные выше этапы попробуем применить к схеме сети, указанной на рис. 20.6, т.е. включим протокол маршрутизации для всех интерфейсов устройства.

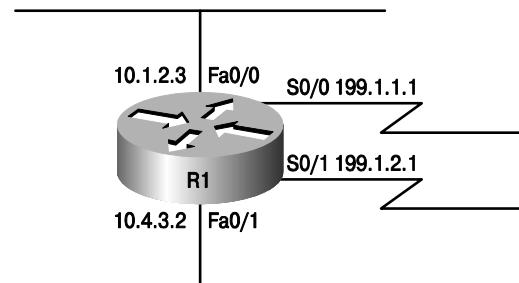


Рис. 20.6. Конфигурирование протокола RIP-2 для одного маршрутизатора с четырьмя интерфейсами

Две первые команды конфигурирования очень простые: в режиме глобальной конфигурации нужно ввести сначала **router rip**, а затем **version 2** без каких-либо дополнительных параметров. Далее нужно выбрать, какие параметры следует указать в команде или командах **network**, чтобы выполнить этап 3. Чтобы указать, что сеть интерфейса и сам интерфейс S0/0 должны участвовать в маршрутизации, необходимо сначала определить, что IP-адрес 199.1.1.1 входит в сеть класса С 199.1.1.0, следовательно, нужно будет ввести команду **network 199.1.1.0** при конфигурировании протокола RIP. Аналогично для интерфейса S0/1 понадобится команда **network 199.1.2.0**, поскольку IP-адрес 199.1.2.1 относится к классовой сети класса С 199.1.2.0. И наконец, на обоих интерфейсах локальной сети установлены адреса из сети класса А 10.0.0.0, следовательно, одна команда **network 10.0.0.0** включит протокол маршрутизации на двух интерфейсах. В примере 20.6 проиллюстрирован весь процесс конфигурирования устройства, состоящий из шести команд, пять из которых относятся к конфигурированию протокола маршрутизации.

Пример 20.6. Пример конфигурирования протокола RIP в маршрутизаторе

```
R1#configure terminal  
R1(config)#router rip  
R1(config-router)#version 2  
R1(config-router)#network 199.1.1.0  
R1(config-router)#network 199.1.2.0  
R1(config-router)#network 10.0.0.0
```

Ввод перечисленных выше команд приведет к тому, что маршрутизатор R1 начнет использовать протокол маршрутизации RIP, т.е. прослушивать входящие обновления маршрутизации для данного протокола и анонсировать сети, непосредственно подключенные к устройству на каждом из четырех интерфейсов. Представим себе более сложную ситуацию, предположим, нам нужно включить протокол маршрутизации RIP на интерфейсе Fa0/0 маршрутизатора R1, но на интерфейсе Fa0/1 мы не хотим включать протокол. Оба интерфейса относятся к сети 10.0.0.0, следовательно, команда **network 10.0.0.0** будет относиться к обоим портам.

В протоколе маршрутизации RIP нет механизма, позволяющего включить маршрутизацию только на некоторых интерфейсах, относящихся к сети класса А, В или С. Следовательно, если нужно включить протокол маршрутизации только на интерфейсе Fa0/0, а на интерфейсе Fa0/1 — нет, то следует ввести команду **network 10.0.0.0**, которая включит маршрутизацию на обоих портах, а потом отключить рассылку обновлений маршрутизации для интерфейса Fa0/1 с помощью команды **passive-interface тип номер** в режиме конфигурирования протокола маршрутизации RIP. Например, чтобы включить протокол RIP для всех портов устройства на рис. 20.6 за исключением интерфейса Fa0/1, нужно ввести команды из примера 20.6 и добавить к ним еще одну команду — **passive-interface Fa0/1**. Данная команда указывает маршрутизатору R1, что он должен перестать отправлять обновления протокола RIP через порт Fa0/1, т.е. она отключает одну из двух основных функций протокола для заданного интерфейса.

ВНИМАНИЕ!

Команда `passive-interface` отключает рассылку обновлений маршрутизации протокола RIP через интерфейс, но входящие анонсы маршрутов принимаются и обрабатываются. Методы отключения обработки входящих обновлений таблицы маршрутизации выходят за рамки рассмотрения данной книги.

Следует отметить еще одну особенность команды `network`: операционная система Cisco IOS примет в качестве параметра не только классовый вариант сети, а любую сеть и не выдаст сообщения об ошибке. Тем не менее операционная система “знает”, что в протоколе RIP должна использоваться классовая сеть, и она автоматически изменит вводимую информацию, когда будет добавлять ее в текущую конфигурацию устройства. Например, если сетевой инженер ввел строку команды в виде `network 10.1.2.3` в режиме конфигурирования протокола RIP, система IOS примет такую команду и не выдаст никаких предупреждений. Тем не менее если посмотреть после ввода команды текущую конфигурацию устройства, там будет присутствовать команда `network 10.0.0.0`, которая, естественно, включит протокол маршрутизации RIP на всех интерфейсах, подсети которых входят в данную классовую сеть класса А.

Проверка протокола RIP-2

В операционной системе Cisco IOS есть три наиболее важные команды `show`, с помощью которых можно проверить работоспособность протокола RIP-2 (табл. 20.5).

Таблица 20.5. Команды проверки работоспособности протокола маршрутизации RIP

Команда	Назначение команды
<code>show ip interface brief</code>	Выдает одну строку информации на каждый интерфейс маршрутизатора, в том числе его IP-адрес и коды состояния. У интерфейса должен быть IP-адрес, и в кодах состояния должно быть указано два раза “up”, чтобы протокол RIP мог работать с интерфейсом
<code>show ip route [rip]</code>	Выводит таблицу маршрутизации устройства, в том числе и маршруты протокола RIP. Если указать ключевое слово <code>rip</code> , то в выводе команды будут показаны только маршруты протокола RIP
<code>show ip protocols</code>	Выводит информацию о конфигурации протокола RIP, IP-адреса соседних устройств RIP, от которых маршрутизатор получает маршруты

Для иллюстрации перечисленных выше команд используется схема сети, показанная на рис. 20.1. Прежде всего опишем кратко конфигурацию протокола RIP для такой схемы сети. Все три интерфейса каждого из трех маршрутизаторов принадлежат к классовой сети 10.0.0.0. Следовательно, в каждом из устройств нужно ввести только одну команду для объявления сетей интерфейсов — `network 10.0.0.0`. Конфигурация протокола маршрутизации для каждого из трех устройств выглядит следующим образом:

```
router rip
version 2
network 10.0.0.0
```

Теперь посмотрим разные варианты команды `show ip route` в примере 20.7; в нем даны некоторые объяснения того, что происходит, дополнительные описания приведены после примера. В примере 20.8 показан результат выполнения команды `show ip protocols`. Выводимая командой `show ip interfaces brief` информация для маршрутизатора Albuquerque была показана в примере 20.1 и здесь не повторяется.

Пример 20.7. Команда `show ip route`

```
Albuquerque#show ip route
Codes: C - connected, S - static, 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
      i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS
      level-2
      ia - IS-IS inter area, * - candidate default, U - per-user static
route
      o - ODR, P - periodic downloaded static route
Gateway of last resort is not set

  10.0.0.0/24 is subnetted, 6 subnets
R    10.1.3.0 [120/1] via 10.1.130.253, 00:00:16, Serial0/1/0
R    10.1.2.0 [120/1] via 10.1.128.252, 00:00:09, Serial0/0/1
C    10.1.1.0 is directly connected, FastEthernet0/0
C    10.1.130.0 is directly connected, Serial0/1/0

R    10.1.129.0 [120/1] via 10.1.130.253, 00:00:16, Serial0/1/0
      [120/1] via 10.1.128.252, 00:00:09, Serial0/0/1
C    10.1.128.0 is directly connected, Serial0/0/1
!
! Указанная ниже команда показывает только маршруты протокола RIP,
! поэтому описание кодов маршрутов не выводится
!
Albuquerque#show ip route rip
  10.0.0.0/24 is subnetted, 6 subnets
R    10.1.3.0 [120/1] via 10.1.130.253, 00:00:20, Serial0/1/0
R    10.1.2.0 [120/1] via 10.1.128.252, 00:00:13, Serial0/0/1
R    10.1.129.0 [120/1] via 10.1.130.253, 00:00:20, Serial0/1/0
      [120/1] via 10.1.128.252, 00:00:13, Serial0/0/1
!
! Показанная ниже команда выводит подробную информацию о маршруте
! только для IP-адреса 10.1.2.1.
!
Albuquerque#show ip route 10.1.2.1
Routing entry for 10.1.2.0/24
  Known via "rip", distance 120, metric 1
  Redistributing via rip
  Last update from 10.1.128.252 on Serial0/0/1, 00:00:18 ago
  Routing Descriptor Blocks:
    * 10.1.128.252, from 10.1.128.252, 00:00:18 ago, via Serial0/0/1
      Route metric is 1, traffic share count is 1
!
! Пример выполнения той же команды, но для адреса, соответствующий
! маршруту к которому отсутствует в таблице маршрутизации устройства.
!
Albuquerque#show ip route 10.1.7.1
% Subnet not in table
Albuquerque#
```

Интерпретация вывода команды `show ip route`

В примере 20.7 показаны команда `show ip route`, выводящая все маршруты IP, команда `show ip route rip`, показывающая все маршруты, полученные через протокол маршрутизации RIP и установленные в таблицу маршрутизации, и два варианта команды `show ip route адрес`, выводящей подробную информацию о маршруте для определенного IP-адреса. При использовании команды `show ip route` следует помнить, что буквой “R” обозначаются маршруты, полученные через протокол маршрутизации RIP, поэтому в трех маршрутах первого варианта команды мы можем увидеть такое обозначение. В примере 20.7 в выводе первой команды также выделена запись для маршрута к подсети 10.1.3.0/24. Из такой записи можно получить следующие полезные сведения:

- адрес (номер) подсети и маску;
- IP-адрес следующего транзитного узла, в данном случае 10.1.130.253, который является адресом интерфейса S0/0/1 маршрутизатора Seville;
- через какой выходной интерфейс доступна такая сеть, в данном случае это интерфейс S0/1/0 маршрутизатора Albuquerque;
- период времени, прошедший с момента последнего обновления маршрута, полученного устройством Albuquerque, в данном случае прошло 20 секунд;
- метрику протокола RIP для маршрута (1 в данном случае), которая указана после косой черты в квадратных скобках, в нашем примере между маршрутизатором Albuquerque и рассматриваемой сетью есть только один транзитный маршрутизатор (Seville);
- *административное расстояние* (administrative distance) маршрута — первое число в квадратных скобках (в данном случае — 120).

Рассмотрите также два оставшихся маршрута RIP в таблице маршрутизации и опишите их так, как это было сделано для первого маршрута. В команде `show ip route rip` показаны маршруты в том же самом формате, но только для протокола RIP, а в верхней части вывода команды не показывается описание обозначений в таблице маршрутизации. Команда `show ip route адрес` показывает подробную информацию о маршруте, под который подходит указанный в качестве параметра IP-адрес.

Административное расстояние

Если в сети есть резервные каналы и используется единственный протокол маршрутизации, каждый маршрутизатор может обнаружить несколько маршрутов к одной подсети. Как рассказывалось выше, протокол маршрутизации в таком случае использует *метрику* (metric), чтобы выбрать оптимальный (т.е. наилучший) маршрут и установить только один маршрут в таблицу маршрутизации.

В некоторых случаях в сети может использоваться несколько протоколов маршрутизации одновременно. В такой ситуации маршрутизатор может получить несколько маршрутов к одной и той же подсети через несколько протоколов маршрутизации, и в таком случае метрики не помогут в выборе оптимального маршрута, поскольку метрики разных протоколов не совместимы и не соизмеримы между собой. Например, в протоколе RIP используется количество транзитных переходов в качестве метрики, а в протоколе маршрутизации EIGRP применяется специальная фор-

мула, в которую входят полоса пропускания и задержка в качестве компонентов метрики. В таком случае метрику протокола RIP, равную 3, очень сложно сравнить с метрикой протокола EIGRP, которая будет равна, например, 4 132 768 для одной и той же подсети. (Да, в протоколе EIGRP, так сложилось, используются очень большие числа!) Поскольку оба числа имеют совершенно разное значение и связаны с разными параметрами, сравнивать их между собой так же корректно, как сравнивать по вкусу помидоры и апельсины.

Тем не менее маршрутизатору все равно нужно выбирать оптимальный маршрут, поэтому в операционной системе Cisco IOS проблема выбора решается за счет присвоения некоторого числа каждому протоколу маршрутизации. Система IOS выбирает маршрут от протокола маршрутизации с меньшим числом. Такое число называли *административным расстоянием* (Administrative Distance — AD) протокола маршрутизации. Например, у протокола маршрутизации EIGRP стандартно AD равно 90, а у протокола RIP, как видно из примера 20.7, — 120. Таким образом, если есть два маршрута к одной и той же подсети, маршрут протокола EIGRP будет установлен в таблицу маршрутизации. В табл. 20.6 перечислены значения административного расстояния для наиболее распространенных источников маршрутов.

 **Таблица 20.6. Стандартные значения административного расстояния в операционной системе IOS**

Источник маршрутной информации	Административное расстояние
Сети, подключенные непосредственно	0
Статические маршруты	1
EIGRP	90
IGRP	100
OSPF	110
IS-IS	115
RIP (V1 и V2)	120
Неизвестный или недостоверный	255

После того как было описано, что такое административное расстояние протокола, рассмотрим еще одну концепцию — специализированный статический маршрут, называемый *резервным статическим* (backup static route). У статических маршрутов значение AD таково, что статический маршрут к подсети будет всегда лучше, чем маршрут от любого протокола маршрутизации к той же подсети, следовательно, статический маршрут всегда будет вытеснять все остальные маршруты к определенной подсети из таблицы маршрутизации. Тем не менее можно создать ситуацию, в которой статический маршрут будет использоваться только в том случае, если маршрута от динамического протокола маршрутизации нет. В таком случае индивидуальный статический маршрут конфигурируется с большим значением AD, чем протокол маршрутизации, поэтому с точки зрения маршрутизатора протокол маршрутизации выдает более достоверную информацию.

Например, если ввести команду `ip route 10.1.1.0 255.255.255.0 10.2.2.2 150`, то она создаст статический маршрут с административным расстоянием в 150, которое выше, чем стандартное значение (см. табл. 20.6). Если маршрут

к подсети 10.1.1.0/24 будет получен тем же самым маршрутизатором от протокола RIP, именно он будет помещен в таблицу маршрутизации, поскольку стандартное значение AD для данного протокола составляет 120, что меньше, чем для настроенного выше статического маршрута.

Команда `show ip protocols`

И наконец, последняя команда, которую мы рассмотрим в привязке к протоколу RIP, — `show ip protocols`. Эта команда показывает некоторые детали работы протокола маршрутизации, в данном случае — протокола RIP. В примере 20.8 показана выводимая этой командой информация; как обычно, команда запущена на маршрутизаторе Albuquerque. Поскольку команда выводит очень много информации, комментарии помещены прямо в вывод команды, а в реальном устройстве читатель никаких объяснений, конечно же, не увидит.

Пример 20.8. Команда `show ip protocols` и ее применение для поиска и устранения неисправностей в протоколе RIP



```
Albuquerque#show ip protocols
Routing Protocol is "rip"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
!
! В следующей строке указан интервал периодической рассылки обновлений и
! показано, когда будет отправлено следующее обновление.
  Sending updates every 30 seconds, next due in 22 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  Redistributing: rip
!
! Несколько следующих строк указывают на то, что используется
! версия 2 протокола
  Default version control: send version 2, receive version 2
    Interface      Send      Recv     Triggered   RIP   Key-chain
    FastEthernet0/0  2          2
    Serial0/0/1     2          2
    Serial0/1/0     2          2
  Automatic network summarization is in effect
  Maximum path: 4
!
! Несколько строк ниже указывают на то, что использовалась только одна
! команда network, а именно network 10.0.0.0. Если бы были указаны
! другие команды network, то их сети также были бы указаны в выводе
! команды.
  Routing for Networks:
  10.0.0.0
!
! В следующем разделе вывода команды указаны IP-адрес соседних
! маршрутизаторов, от которых устройство Albuquerque получило обновления
! таблицы маршрутизации, и время последнего обновления информации от
! соседей.
! Следует заметить, что адрес 10.1.130.253 — это маршрутизатор Seville,
! а 10.1.128.252 — Yosemite.
  Routing Information Sources:
    Gateway          Distance   Last Update
    10.1.130.253      120       00:00:25
    10.1.128.252      120       00:00:20
  Distance: (default is 120)
```

Наиболее полезная информация, выводимая рассматриваемой командой, — это версия протокола и источники маршрутной информации. Если инженер вдруг забудет настроить команду `version 2` в протоколе маршрутизации, то протокол RIP будет отправлять анонсы только в формате первой версии и в колонке “Send” (отправка) будет цифра 1, а не 2. Остальные маршрутизаторы будут игнорировать обновления маршрутов от такого устройства, если у них включена вторая версия протокола.

Чтобы посмотреть, из каких источников локальный маршрутизатор получает обновления маршрутов по протоколу RIP, следует внимательно изучить последний блок в выводимой командой `show ip protocols` информации. Например, для сети, представленной на рис. 20.1, мы увидим, что маршрутизатор `Albuquerque` получает обновления из двух источников, т.е. от двух маршрутизаторов: `Yosemite` и `Seville`. В нижней части вывода команды в примере 20.8 показано, что это именно так, а также что маршрутизатор `Albuquerque` получал обновления маршрутов от двух устройств чуть меньше, чем 30 секунд назад. Если бы в выводимом блоке информации был указан всего один маршрутизатор, то, связав адрес с именем, можно было бы узнать, от какого устройства не приходят обновления, и начать искать ошибки и неисправности в нем.

Анализ сообщений протокола RIP с помощью команды `debug`

Правильно ли работает протокол RIP, можно определить с помощью команды `debug ip rip`. Эта команда включает режим отладки (`debug`) в маршрутизаторе, в котором создаются сообщения в системный журнал устройства каждый раз, когда маршрутизатор отправляет или принимает сообщение протокола RIP. В таких сообщениях есть информация о всех подсетях, которые включены в анонсы, а расшифровать сами сообщения относительно несложно, — они вполне удобочитаемы и понятны.

В примере 20.9 показан вывод команды `debug ip rip` для маршрутизатора `Albuquerque` для схемы сети, приведенной на рис. 20.1. Следует помнить, чтобы увидеть такие сообщения, пользователь должен быть подключен через консольный порт устройства или ввести команду `terminal monitor` в привилегированном режиме в сеансе Telnet или SSH. Комментарии в выводе команды описывают значения пяти наиболее важных групп сообщений отладки. В первых трех группах сообщений описаны обновления маршрутизации, рассылаемые маршрутизатором `Albuquerque` через каждый из трех его интерфейсов; к четвертой группе относятся сообщения, создаваемые при получении устройством `Albuquerque` обновления от маршрутизатора `Seville`; в пятой, и последней, группе описано обновление, полученное от маршрутизатора `Yosemite`.

Пример 20.9. Вывод команды `debug` для протокола RIP

```
Albuquerque#debug ip rip
RIP protocol debugging is on
Albuquerque#
! Обновление отправлено устройством Albuquerque через интерфейс Fa0/0:
! В двух сообщениях ниже указано, что отправлено обновление версии 2
! через интерфейс Fa0/0 на многоадресатный IP-адрес 224.0.0.9.
! Далее в пяти строках указано пять подсетей в обновлении.
*Jun 9 14:35:08.855: RIP: sending v2 update to 224.0.0.9 via
FastEthernet0/0 (10.1.1.251)
*Jun 9 14:35:08.855: RIP: build update entries
*Jun 9 14:35:08.855: 10.1.2.0/24 via 0.0.0.0, metric 2, tag 0
```

```
*Jun 9 14:35:08.855:      10.1.3.0/24 via 0.0.0.0, metric 2, tag 0
*Jun 9 14:35:08.855:      10.1.128.0/24 via 0.0.0.0, metric 1, tag 0
*Jun 9 14:35:08.855:      10.1.129.0/24 via 0.0.0.0, metric 2, tag 0
*Jun 9 14:35:08.855:      10.1.130.0/24 via 0.0.0.0, metric 1, tag 0
```

! В пяти сообщениях режима debug ниже указано, что
! маршрутизатор отправляет анонс через интерфейс S0/1/0, в котором
! указано 3 подсети и маски.

```
*Jun 9 14:35:10.351:      RIP: sending v2 update to 224.0.0.9 via
Serial0/1/0 (10.1.130.251)
*Jun 9 14:35:10.351:      RIP: build update entries
*Jun 9 14:35:10.351:      10.1.1.0/24 via 0.0.0.0, metric 1, tag 0
*Jun 9 14:35:10.351:      10.1.2.0/24 via 0.0.0.0, metric 2, tag 0
*Jun 9 14:35:10.351:      10.1.128.0/24 via 0.0.0.0, metric 1, tag 0
```

! В пяти сообщениях режима debug ниже указано, что маршрутизатор
! отправляет анонс через интерфейс S0/0/1, в котором указано 3 подсети
! и маски.

```
*Jun 9 14:35:12.443:      RIP: sending v2 update to 224.0.0.9 via
Serial0/0/1 (10.1.128.251)
*Jun 9 14:35:12.443:      RIP: build update entries
*Jun 9 14:35:12.443:      10.1.1.0/24 via 0.0.0.0, metric 1, tag 0
*Jun 9 14:35:12.443:      10.1.3.0/24 via 0.0.0.0, metric 2, tag 0
*Jun 9 14:35:12.443:      10.1.130.0/24 via 0.0.0.0, metric 1, tag 0
```

! В четырех сообщениях ниже указано, что маршрутизатор Albuquerque
! получает через протокол RIP версии 2 (v2) обновления маршрутной
! информации от маршрутизатора Seville (S0/1/0), в котором есть три
! маршрута. Обратите внимание, что маска указана в формате /24.

```
*Jun 9 14:35:13.819:      RIP: received v2 update from 10.1.130.253 on
Serial0/1/0
*Jun 9 14:35:13.819:      10.1.2.0/24 via 0.0.0.0 in 2 hops
*Jun 9 14:35:13.819:      10.1.3.0/24 via 0.0.0.0 in 1 hops
*Jun 9 14:35:13.819:      10.1.129.0/24 via 0.0.0.0 in 1 hops
```

! В четырех сообщениях ниже указано, что маршрутизатор Albuquerque
! получает через протокол RIP версии 2 (v2) обновления маршрутной
! информации от маршрутизатора Yosemite (S0/0/1), в котором есть три
! маршрута. Обратите внимание, что маска указана в формате /24.

```
*Jun 9 14:35:16.911:      RIP: received v2 update from 10.1.128.252 on
Serial0/0/1
*Jun 9 14:35:16.915:      10.1.2.0/24 via 0.0.0.0 in 1 hops
*Jun 9 14:35:16.915:      10.1.3.0/24 via 0.0.0.0 in 2 hops
*Jun 9 14:35:16.915:      10.1.129.0/24 via 0.0.0.0 in 1 hops
```

Albuquerque#**undebug all**

All possible debugging has been turned off

Albuquerque#**show process**

CPU utilization for five seconds: 0%/0%; one minute: 0%; five minutes: 0%						
PID	QTy	PC	Runtime (ms)	Invoked	uSecs	Stacks TTY
Process						
1	Cwe	601B2AE8	0	1	0	5608/6000 0 Chunk
Manager						

Прежде всего следует обратить внимание на наборы из пяти сообщений: в них указано, какие анонсы маршрутов должен получать и отправлять маршрутизатор Albuquerque и через какие порты. В сообщениях указано, что устройство рассыпает анонсы через порты Fa0/0, S0/0/1 и S0/1/0, т.е. через те интерфейсы, на которых

включен протокол RIP. В остальных сообщениях указано, что устройство Albuquerque получило анонс через интерфейс S0/1/0, к которому подключен маршрутизатор Seville, а также через интерфейс S0/0/1, к которому подключен маршрутизатор Yosemite.

Большинство сообщений интуитивно понятно, или, по крайней мере, очень легко догадаться, о чем они сигнализируют. В сообщениях есть комбинация символов “v2”, означающая, что используется протокол RIP версии 2, это также подтверждает тот факт, что анонсы пересыпаются на многоадресатный IP-адрес 224.0.0.9. (Протокол RIP-1 пересыпает обновления маршрутов на адрес 255.255.255.255, т.е. широковещательный адрес.) В большинстве сообщений примера указана маршрутная информация, содержащаяся в анонсах, а именно: адрес подсети, длина префикса (т.е. маска) и метрика маршрута.

Пристальное изучение адресов в анонсах позволяет сделать вывод, что маршрутизаторы не добавляют абсолютно все сети в анонсы. Если обратиться к рис. 20.1, мы увидим, что в сети есть шесть подсетей. Тем не менее в обновлениях в примере показаны три или пять подсетей. Причина такого поведения кроется в теории работы протокола маршрутизации RIP, а именно в так называемом правиле “расщепления горизонта” (split horizon). Этот механизм защиты от кольцевых маршрутов подробно описан в главе 10 второго тома и обеспечивает фильтрацию сетей в анонсах маршрутизации, чтобы исключить петли в маршрутизации.

И в завершение темы несколько комментариев о команде `debug`, которые могут оказаться полезными. Перед тем как использовать эту команду, следует посмотреть на загрузку процессора с помощью команды `show process`, которая показана в конце примера 20.9. В выводе этой команды показана загрузка центрального процессора за некоторый период времени. Если загрузка процессора маршрутизатора высока, т.е. превышает 30–40%, то команду `debug` следует использовать осмотрительно, иначе можно вызвать ситуацию, в которой устройство не сможет передавать пакеты и даже “зависнет”. Кроме того, читатель, может быть, обратил внимание на временные метки в выводе сообщений отладки. Чтобы устройство создавало и выводило их, следует указать команду `service timestamps` в режиме глобального конфигурирования маршрутизатора.

Подготовка к экзамену

Повторите все ключевые темы

Повторите все ключевые темы данной главы, помеченные пиктограммой “Ключевая тема”. Ключевые темы и соответствующие им страницы перечислены в табл. 20.7.

Таблица 20.7. Ключевые темы главы 20

Элемент	Описание	Страница
Пример 20.3	Настройка статических маршрутов для маршрутизатора Albuquerque	529
Определения	Определения протоколов IGP и EGP	537
Табл. 20.2	Классификация протоколов маршрутизации на основе алгоритмов их работы	538
Табл. 20.3	Сравнение классовых и бесклассовых протоколов маршрутизации	541
Табл. 20.4	Сравнение протоколов маршрутизации внутреннего шлюза	542
Список	Этапы настройки протокола маршрутизации RIP-2	543
Список	Три действия, выполняемые для интерфейса, который включен в процесс маршрутизации протокола RIP	543
Табл. 20.6	Стандартные значения административного расстояния в операционной системе IOS	548
Пример 20.8	Команда show ip protocols и ее применение для поиска и устранения неисправностей в протоколе RIP	549

Заполните таблицы и списки по памяти

Распечатайте приложение М (Appendix L) с компакт-диска или его раздел, относящийся к этой главе, и заполните таблицы и списки по памяти. В приложении Н (Appendix M) приведены заполненные таблицы и списки для самоконтроля.

Ключевые термины

Дайте определения перечисленных ниже терминов и проверьте правильность их написания в списке терминов:

административное расстояние (administrative distance), автономная система (autonomous system), резервный статический маршрут (backup static route), сбалансированный гибридный протокол маршрутизации (balanced hybrid routing protocol), бесклассовый протокол маршрутизации (classless routing protocol), классовый протокол маршрутизации (classful routing protocol), конвергенция (convergence), стандартный маршрут (default route), дистанционно-векторный протокол маршрутизации (distance vector routing protocol), протокол маршрутизации внешнего шлюза (Exterior Gateway Protocol — EGP), протокол маршрутизации внутреннего шлюза (Interior Gateway Protocol — IGP), состояние каналов (link state), метрика (metric), анонс маршрутизации (routing update), маски подсети переменной длины (Variable-Length Subnet Mask — VLSM).

Список команд

Заучивать наизусть информацию в таблицах не нужно, для удобства упоминавшиеся в главе команды конфигурирования перечислены в табл. 20.8, а команды контроля и устранения неисправностей — в табл. 20.9. На практике команды должны запомниться сами собой после выполнения практических лабораторных работ и в процессе подготовки к экзамену. Чтобы потренироваться в их запоминании, следует закрыть левую часть таблицы листком бумаги и по описанию в правом столбце по памяти записать соответствующие команды, а потом проверить, правильно ли был указан ответ.

Таблица 20.8. Команды для конфигурирования устройств

Команда	Описание
router rip	Команда глобального режима конфигурирования устройства, переводит интерфейс пользователя в режим конфигурирования протокола RIP
network адрес_сети	Команда поддержима конфигурирования протокола маршрутизации RIP, задает адрес классовой сети и включает протокол маршрутизации на всех интерфейсах, входящих в такую сеть
version {1 2}	Команда поддержима конфигурирования протокола маршрутизации RIP, включающая вторую версию протокола
passive-interface [default] {тип_интерфейса номер_интерфейса}	Команда поддержима конфигурирования протокола маршрутизации RIP, указывающая, что через заданный интерфейс не нужно рассыпать анонсы маршрутов
ip address адрес маска	Команда поддержима конфигурирования интерфейса, задающая его IP-адрес и маску
ip route префикс маска {IP-адрес тип_интерфейса номер_интерфейса }	Команда режима глобальной конфигурации устройства, задающая статический маршрут
service timestamps	Команда режима глобальной конфигурации устройства, включающая создание и отображение временных меток в системном журнале и сообщениях отладки (debug)

Таблица 20.9. Команды для конфигурирования устройств

Команда	Описание
show ip interface brief	Показывает строку информации о каждом интерфейсе, в том числе IP-адрес, код состояния линии и протокола, а также метод получения IP-адреса: вручную или через протокол DHCP
show ip route [rip static connected]	Команда для вывода на экран таблицы маршрутизации, в том числе маршруты от протокола RIP или определенный тип маршрутов, в зависимости от указанного в конце опционального параметра
show ip route IP-адрес	Команда для отображения подробной информации о маршруте для указанного IP-адреса
show ip protocols	Выдает информацию о конфигурации протокола RIP, IP-адреса соседних маршрутизаторов RIP, от которых локальное устройство получает маршруты

Окончание табл. 20.9

Команда	Описание
show process	Выдает информацию о процессах, запущенных операционной системой маршрутизатора, и, что очень важно, загрузку процессора устройства
terminal ip netmask-format decimal	Меняет формат отображения маски в текущем сеансе подключения к маршрутизатору. Данный вариант команды устанавливает десятичный формат маски вместо префиксного
debug ip rip	Указывает устройству, что нужно создавать и выводить сообщения для каждого отправленного и принятого сообщения протокола маршрутизации RIP

В этой главе...

- **Советы по устранению неисправностей и необходимый инструментарий.** Приведены советы по методам поиска и устранения неисправностей в маршрутах оконечных хостов, устранению проблем в маршрутизаторах и ошибок в IP-адресации, в частности, описаны дополнительные инструменты, которые в других главах не рассматриваются.
- **Сценарий поиска и устранения ошибок в маршрутизации.** Представлен некоторый сценарий, состоящий из трех частей, в каждой из них есть собственные задания, которые нужно выполнить и проверить правильность выполнения по готовым ответам.

ГЛАВА 21

Поиск и устранение неисправностей маршрутизации

Эта глава преследует две главные цели. Во-первых, в ней подробно описаны темы, которые в других главах только затрагивались, а именно: некоторые методы и команды для поиска и устранения неисправностей в маршрутизаторах и окончательных рабочих станциях. Во-вторых, мы повторим базовые концепции маршрутизации и адресации в сетях, но с точки зрения анализа и понимания процесса поиска и устранения ошибок. Кроме того, в текущей главе представлен сценарий некоторой ситуации, демонстрирующий использование ряда основных концепций и инструментов, описанных выше. В сценарии предусмотрено, что читатель сначала попробует устраниить описанную проблему сам, а потом сможет прочитать ответ и его описание.

Следует отметить, что если читатель приобрел также второй том книги, то после прочтения текущей главы следует прочитать части II и III второго тома.

Контрольные вопросы: знаете ли вы уже темы главы

Этот раздел предназначен для того, чтобы читатель мог предварительно оценить свои знания и решить, нужно ли ему читать главу целиком. Если ответы на девять из десяти вопросов даны правильно, можно сразу же перейти к последнему разделу “Подготовка к экзамену”. Основные темы этой главы и предварительных контрольных вопросов перечислены в табл. 21.1. Отвечая на контрольные вопросы и используя таблицу, читатель сможет достаточно точно определить свои знания в той или иной области. Ответы на вопросы приведены в приложении А.

Таблица 21.1. Темы контрольных вопросов

Основная тема	Номера вопросов
Советы по устранению неисправностей и необходимый инструментарий	1–6
Сценарий поиска и устранения ошибок в маршрутизации	7–9

1. В сети есть маршрутизатор, в котором настроена команда `ip subnet-zero`. Инженер ввел в текстовом редакторе несколько конфигурационных команд, чтобы позже скопировать их в конфигурацию маршрутизатора. Какой из указанных ниже IP-адресов в таких командах не может быть присвоен интерфейсу Fa0/0 устройства? (Выберите несколько ответов.)
 - a) 172.16.0.200 255.255.255.128.
 - b) 172.16.0.200 255.255.255.0.

- в) 225.1.1.1 255.255.255.0.
г) 10.43.53.63 255.255.255.192.

2. Какую из указанных ниже команд можно использовать для определения текущего IP-адреса и маски хоста в операционных системах компании Microsoft?

- а) tracert.
б) ipconfig /all.
в) arp -a.
г) ipconfig /displaydns.

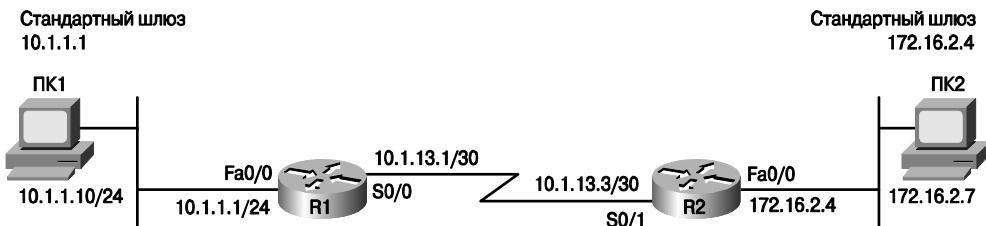
3. Изучите вывод указанной ниже команды. Если пользователь введет команду **resume**, что произойдет?

R1#show sessions

Conn	Host	Address	Byte	Idle	Conn Name
1	Fred	10.1.1.1	0	0	Fred
*	2 Barney	10.1.2.1	0	0	Barney

- а) Команда будет отклонена устройством, и маршрутизатор повторно выведет приглашение интерфейса командной строки.
б) Пользователь интерфейса командной строки будет подключен к приостановленному сеансу Telnet для маршрутизатора с IP-адресом 10.1.1.1.
в) Пользователь интерфейса командной строки будет подключен к приостановленному сеансу Telnet для маршрутизатора с IP-адресом 10.1.2.1.
г) Из показанной информации нельзя точно предсказать результат выполнения команды.

4. Для ответов на вопросы 4–9 следует использовать следующую схему.



5. Если в локальную сеть слева на схеме добавить третий компьютер (ПК3) с IP-адресом 10.1.1.130/25 и стандартным шлюзом 10.1.1.1, то какое утверждение будет верным? (Выберите несколько ответов.)

- а) Если на компьютере ПК1 выполнить команду ping 10.1.1.130, то он использует протокол ARP, чтобы узнать MAC-адрес компьютера ПК3.
б) Если на компьютере ПК3 выполнить команду ping 10.1.1.10, то он использует протокол ARP, чтобы узнать MAC-адрес компьютера ПК1.
в) Если на компьютере ПК1 выполнить команду ping 10.1.1.1, то он использует протокол ARP, чтобы узнать MAC-адрес для IP-адреса 10.1.1.131.
г) Если на маршрутизаторе R1 выполнить команду ping 10.1.1.130, то он использует протокол ARP, чтобы узнать MAC-адрес для IP-адреса 10.1.1.130.

6. Новый сотрудник, сетевой инженер, пытается найти и устраниить проблему на компьютере ПК1. Какое из указанных ниже действий покажет, что существует проблема на 1-м или 2-м уровне в сегменте сети Ethernet (расположенном на схеме слева)?
- Команда ping 10.1.1.1 на компьютере ПК1 дает отрицательный результат.
 - Команда ping 10.1.13.2 на компьютере ПК1 дает положительный результат, а команда ping 172.16.2.4 — отрицательный.
 - Команда ping 10.1.1.1 на компьютере ПК1 дает положительный результат, а команда ping 10.1.13.1 — отрицательный.
 - Команда ping 10.1.1.10 на компьютере ПК1 дает положительный результат.
7. На компьютере ПК2 пользователь выполнил команду tracert 10.1.1.10. Какие из указанных ниже адресов будут показаны в выводе команды? (Выберите несколько ответов.)
- 10.1.1.10.
 - 10.1.1.1.
 - 10.1.13.1.
 - 10.1.13.2.
 - 172.16.2.4.
8. Предположим, все устройства на схеме только что загрузились и ни одно из них не успело переслать какие-либо данные. В обоих персональных компьютерах (ПК) используются статически назначенные IP-адреса. С компьютера ПК1 выполнена команда ping на компьютер ПК2, и она дала положительный результат. Какие записи будут отображаться в таблице ARP? (Выберите несколько ответов.)
- В таблице ARP компьютера ПК1 будет запись для IP-адреса 172.16.2.7.
 - В таблице ARP компьютера ПК1 будет запись для IP-адреса 10.1.1.1.
 - В таблице ARP маршрутизатора R1 будет запись для IP-адреса 10.1.1.10.
 - В таблице ARP маршрутизатора R1 будет запись для IP-адреса 172.16.2.7.
9. Предположим, все устройства на схеме только что загрузились и ни одно из них не успело переслать какие-либо данные. В обоих персональных компьютерах (ПК) используются статически назначенные IP-адреса. С компьютера ПК1 выполнена команда ping на компьютер ПК2, и она дала положительный результат. Какие запросы ARP будут выполняться в сети? (Выберите несколько ответов.)
- Компьютер ПК1 выполнит широковещательный запрос ARP, чтобы обнаружить MAC-адрес интерфейса маршрутизатора R1 с IP-адресом 10.1.1.1.
 - Компьютер ПК2 выполнит широковещательный запрос ARP, чтобы обнаружить MAC-адрес интерфейса маршрутизатора R2 с IP-адресом 172.16.2.4.
 - Маршрутизатор R1 выполнит широковещательный запрос ARP, чтобы обнаружить MAC-адрес компьютера ПК1.
 - Маршрутизатор R2 выполнит широковещательный запрос ARP, чтобы обнаружить MAC-адрес компьютера ПК2.

- д) Компьютер ПК1 выполнит широковещательный запрос ARP, чтобы обнаружить MAC-адрес компьютера ПК2.
10. С компьютера ПК1 на компьютер ПК2 запущена команда `ping`. Она дает положительный результат (см. схему выше). Что из указанного ниже справедливо для передаваемых между ними пакетов? (Выберите несколько ответов.)
- а) Для фрейма, передающегося слева направо, когда он передается по локальной сети в левой части схемы, MAC-адрес получателя фрейма совпадает с MAC-адресом маршрутизатора R1.
 - б) Для фрейма, передающегося слева направо, когда он передается по локальной сети в правой части схемы, MAC-адрес получателя фрейма совпадает с MAC-адресом маршрутизатора R2.
 - в) Для фрейма, передающегося слева направо, когда он передается по последовательному каналу, его IP-адрес получателя совпадает с IP-адресом компьютера ПК2.
 - г) Для фрейма, передающегося справа налево, когда он передается по локальной сети в левой части схемы, MAC-адрес отправителя фрейма совпадает с MAC-адресом компьютера ПК2.
 - д) Для фрейма, передающегося справа налево, когда он передается по локальной сети в правой части схемы, MAC-адрес отправителя фрейма совпадает с MAC-адресом маршрутизатора R2.
 - е) Для фрейма, передающегося справа налево, когда он передается по последовательному каналу, его MAC-адрес отправителя совпадает с MAC-адресом маршрутизатора R2.

Основные темы

Советы по устранению неисправностей и необходимый инструментарий

Основная цель текущей главы — помочь читателю подготовиться к наиболее сложным заданиям и вопросам сертификационного экзамена, которые потенциально связаны с проблемами на уровне 3 эталонной модели. Задачи по поиску и устранению неисправностей совпадают или очень похожи на те, которые приходится решать в повседневной работе, и, как минимум, для решения реальных задач используются те же подходы и инструменты. В первом разделе главы рассмотрены типичные проблемы и неисправности, связанные с адресацией, маршрутизацией и логикой работы протоколов маршрутизации. В оставшейся части представлен некоторый сценарий, описывающий сеть, в которой есть несколько типичных проблем. Задания сценария помогут выработать методы анализа проблемы и показать методы решения наиболее часто возникающих ошибок и неисправностей, а также проиллюстрируют, как нужно искать правильные ответы на специфические вопросы.

IP-адресация

В этом подразделе рассмотрены некоторые основные характеристики и особенности IP-адресов. Что наиболее важно, ниже также даются полезные советы о том, как применить имеющиеся знания для решения экзаменационных задач и ответов на вопросы, а также для практической работы.

Не используйте зарезервированные IP-адреса

Первое, что нужно проверить, изучая ответы на вопрос в экзамене или решая практическую задачу, — относятся ли какие-либо из указанных IP-адресов к зарезервированным и могут ли они быть использованы для адресации хостов. Все зарезервированные адреса можно разделить на три большие группы:

- адреса, которые всегда зарезервированы (глобально);
- адреса, зарезервированные для определенной подсети;
- входят ли адреса в две специализированные подсети в каждой из классовых сетей, а именно: в нулевую и широковещательную подсети.

К первой группе адресов относятся две сети класса A, которые зарезервированы “навсегда” и никогда не будут использоваться, адреса класса D (многоадресатные), а также IP-адреса класса E (экспериментальные). Такие адреса можно достаточно легко распознать по значению в первом октете:

Зарезервированные значения адресов, которые ни в коем случае не могут быть назначены хостам



- 0 (сеть 0.0.0.0 глобально зарезервирована);
- 127 (сеть 127.0.0.0 глобально зарезервирована);
- 224–239 (все сети класса D, многоадресатные);
- 240–255 (все сети класса E, экспериментальные адреса).

Вторая группа, или категория, зарезервированных адресов включает в себя два зарезервированных адреса в каждой из подсетей. Разбивая сеть на подсети, мы не должны использовать для адресации хостов два значения — наименьший и наибольший адреса, известные как:

- адрес (номер) подсети;
- широковещательный адрес.

Поэтому умение быстро и безошибочно определять адрес подсети и широковещательный адрес понадобится, чтобы быстро выбрать из указанного набора адресов не подходящие для присвоения какому-либо хосту.

Третья группа зарезервированных IP-адресов может быть как применима, так и неприменима для какого-либо конкретного вопроса. Для классовой сети, в зависимости от нескольких факторов, следующие две подсети, возможно, придется отбросить при расчетах:

- *нулевая подсеть* (zero subnet);
- *широковещательная подсеть* (broadcast subnet).

Если в вопросе экзамена фигурирует адрес в нулевой или широковещательной подсети, следует внимательно прочитать задание и определить, разрешено ли в данной постановке вопроса использовать эти две подсети или нет. В табл. 21.2 перечислены основные критерии, по которым определяют, можно ли использовать подсети.



Таблица 21.2. Как определить, можно ли использовать нулевую и широковещательную подсети

Постановка вопроса	Зарезервированы ли подсети
О двух подсетях ничего не сказано	Нет
В конфигурации устройства или в вопросе указана команда <code>ip subnet-zero</code>	Нет
В вопросе указан бесклассовый протокол маршрутизации (RIP-2, EIGRP, OSPF)	Нет
В конфигурации устройства или в вопросе указана команда <code>no ip subnet-zero</code>	Да
В вопросе указан классовый протокол маршрутизации (RIP-1)	Да

Одна подсеть с одинаковой маской для каждой сети

Хосты в одной локальной сети (или в виртуальной сети VLAN), т.е. устройства, относящиеся к одному широковещательному домену, должны относиться к одной и той же адресной подсети. Следовательно, как IP-адрес интерфейса маршрутизатора, так и административный (management) адрес коммутатора и адреса на интерфейсах хостов должны сопровождаться одинаковой маской.

На экзамене прежде всего следует проверить детали схемы сети и посмотреть, какая маска установлена на устройствах в одном и том же сегменте. Зачастую в вопросе сертификационного экзамена информация не будет красиво и удобно размещена на прилагаемой схеме сети. Часть информации будет присутствовать на схеме, часть — выводиться в командах группы `show`, и к ней нужно будет применить расчеты, связанные с IP-адресами, которые подробно были описаны в части III.

На рис. 21.1 представлен пример локальной сети, которая может быть, например, частью экзаменационного вопроса. Для простоты и удобства IP-адреса и маски показаны непосредственно на схеме, хотя в экзамене, как уже упоминалось выше, на схеме может присутствовать только часть информации, оставшиеся детали придется получать через эмулятор устройства, какие-либо дополнительные текстовые блоки или примеры выполнения команд.

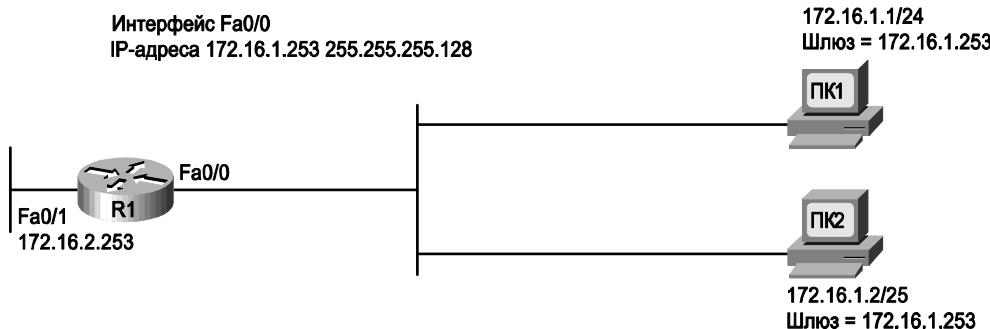


Рис. 21.1. Пример локальной сети

Рассмотрев схему сети на рис. 21.1, читатель может заметить, что на двух компьютерах установлена разная маска (показанная в префиксном формате). Чтобы разобраться в такой схеме, читателю нужно знать, как можно просмотреть конфигурацию устройства, найти в ней маску, установленную командой `ip address` в режиме конфигурирования интерфейса. Далее нужно уметь преобразовать маску из десятичного формата в префиксный (или наоборот) и сравнить ее с другими масками в примере сети. В табл. 21.3 указаны все варианты адресов и масок, использующиеся в данной сети.

Таблица 21.3. Варианты подсетей в схеме на рис. 21.1

	R1 Fa0/0	ПК1	ПК2
Маска	255.255.255.128	255.255.255.0	255.255.255.128
Адрес подсети	172.16.1.128	172.16.1.0	172.16.1.0
Широковещательный адрес	172.16.1.255	172.16.1.255	172.16.1.127

После того как схема адресации стала понятна, несколько проблем в такой локальной сети становятся вполне очевидными. Например, компьютер ПК1 предполагает, что адрес 172.16.1.253 (R1) находится в той же подсети, и он может пересыпать пакеты маршрутизатору R1 через локальную сеть. Тем не менее маршрутизатор R1 не относит компьютер ПК1 (172.16.1.1) к той же подсети, поскольку маршрут к непосредственно подключенной подсети (172.16.1.128/25) не включает в себя хост ПК1. Подобным образом можно обнаружить, что хосты, находящиеся в одной и той же локальной сети, по своим IP-адресам и маскам относятся к разным подсетям, и иногда на экзамене такой информации вполне достаточно, чтобы дать правильный ответ на вопрос или решить практическое задание. В табл. 21.7 ниже перечислены команды, которые помогут решить такие задания, а также собрать и проанализировать информацию.

Решение проблем с IP-адресами

Если читатель встретился с какой-либо практической проблемой с IP-адресами или с заданием в сертификационном экзамене, нужно выполнить указанные ниже действия и учесть перечисленные факторы для успешного ответа на вопрос или устранения проблемы.



Список советов по решению заданий, связанных с IP-адресацией на экзамене

1. Проверьте, какая маска установлена на всех устройствах в одной и той же локальной сети или сегменте; если маска отличается, то устройства могут по-разному интерпретировать диапазон адресов для такой сети.
2. В двухточечных каналах WAN проверьте IP-адреса и маски на двух концах канала и убедитесь, что оба адреса находятся в одной подсети.
3. Проверяя, находятся ли хосты в одной и той же подсети, проверьте не только адреса подсетей, но и маску, и диапазон, в который попадают установленные IP-адреса.
4. Запомните и будьте готовы использовать команды, указанные в табл. 21.4, чтобы определить адреса, маски и адреса подсетей хостов.

В следующем разделе рассмотрен алгоритм маршрутизации пакетов маршрутизатором, а также описаны некоторые полезные команды из операционных систем компании Microsoft, позволяющие определить IP-адрес и маску хоста.

Сетевые настройки оконечного хоста

В главе 5 был описан простой алгоритм, используемый хостом при отправке пакета, когда используются протоколы DHCP, DNS, ARP и ICMP. Сам алгоритм можно свести к следующему краткому списку механизмов, используемых при передаче данных.



Маршрутизация, IP-адресация, преобразование имен и запросы ARP с точки зрения хоста

- *Маршрутизация (routing).* Если IP-адрес получателя пакета находится в той же подсети, пакет передается напрямую получателю; если же нет, то пакет передается *стандартному шлюзу (default gateway)*.
- *Присвоение адреса (address assignment).* До того как устройство сможет отправить хотя бы один пакет, оно может использовать службы клиента DHCP для получения своего IP-адреса, маски, стандартного шлюза и адреса сервера DNS. Перечисленные параметры также могут быть настроены вручную (т.е. заданы статически) в настройках сети хоста.
- *Преобразование имен (name resolution).* Когда пользователь прямо или косвенно использует имя хоста в каком-либо приложении, рабочая станция отправляет серверу DNS запрос на преобразование имени, чтобы установить IP-адрес нужного хоста. Запрос может и не отправляться, если нужная информация уже есть в кеше.

- *Преобразование IP- в MAC-адрес (IP-to-MAC resolution).* Хост использует протокол ARP, чтобы узнать MAC-адрес устройства-получателя или стандартного шлюза. Запрос может и не отправляться, если нужная информация уже есть в кеше.

Из четырех перечисленных выше механизмов только маршрутизация выполняется для каждого пакета. Функция присвоения адреса обычно используется один раз, сразу же после загрузки системы. Процесс преобразования имен и запросы ARP выполняются по мере необходимости, обычно в ответ на какие-либо действия пользователя.

Чтобы проанализировать, насколько правильно и безошибочно хост использует перечисленные методы, найти и устраниТЬ неисправности, нужно знать несколько команд, связанных с проверкой работы сети для окончной рабочей станции (т.е. хоста). В табл. 21.4 перечислены наиболее важные сетевые команды для операционной системы Microsoft, тем не менее, в других операционных системах существуют аналогичные программы или утилиты. В примере 21.1 проиллюстрирована работа некоторых из перечисленных команд.

Таблица 21.4. Команды проверки сети операционной системы Windows

Команда	Функции команды
ipconfig /all	Выдает подробную информацию об IP-конфигурации всех интерфейсов, в том числе IP-адрес, маску, стандартный шлюз и IP-адрес сервера DNS
ipconfig /release	Освобождает IP-адрес, полученный от сервера DHCP
ipconfig /renew	Отправляет запрос на получение IP-адреса и связанной с ним информации серверу DHCP
nslookup имя	Отправляет запрос DNS для указанного имени хоста
arp -a	Выводит содержимое таблицы ARP хоста
ipconfig /displaydns	Выводит содержимое кеша хоста
ipconfig /flushdns	Удаляет все записи из кеша хоста
arp -d	Очищает (сбрасывает) всю таблицу ARP хоста
netstat -rn	Показывает таблицу маршрутизации хоста

В примере 21.1 показана команда ping www.cisco.com, выполненная на хосте в операционной системе Windows XP, сразу же после того, как кеш ARP и кеш имен были удалены (т.е. очищены). В первой части примера показаны полученные от сервера DHCP IP-адрес и адрес сервера DNS, потом проиллюстрирован процесс очистки кешей, а затем — команда ping www.cisco.com. Выполнение последнего действия приводит к тому, что хост использует сервер DNS для получения IP-адреса веб-сервера компании Cisco, после этого выполняет запрос ARP для обнаружения MAC-адреса стандартного шлюза и только потом пересыпает эхо-запрос протокола ICMP по найденному адресу.

ВНИМАНИЕ!

Команда ping возвращает отрицательный результат в рассматриваемом примере. Такая ситуация вызвана, скорее всего, со списками ACL в маршрутизаторах или брандмауэрах Интернета. Тем не менее команда все же запускает генератор запросов DNS и ARP, как показано в примере 21.1. Кроме того, эти же команды применяются в окне командной строки большинства операционных систем Windows.

**Пример 21.1. Использование команд для проверки сети
в операционной системе рабочей станции**

```
C:\>ipconfig /all
! Часть строк опущена.
Ethernet adapter Local Area Connection:

  Connection-specific DNS Suffix . : cinci.rr.com
  Description . . . . . : Broadcom NetXtreme 57xx
Gigabit Controller
  Physical Address. . . . . : 00-11-11-96-B5-13
  Dhcp Enabled. . . . . : Yes
  Autoconfiguration Enabled . . . . : Yes
    IP Address. . . . . : 192.168.1.102
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1
    DHCP Server . . . . . : 192.168.1.1
    DNS Servers . . . . . : 65.24.7.3
                                65.24.7.6
  Lease Obtained. . . . . : Thursday, March 29, 2007
6:32:59 AM
  Lease Expires . . . . . : Friday, March 30, 2007 6:32:59
AM
! Ниже удаляется кеш ARP и имен.
C:\>arp -d
C:\>ipconfig /flushdns
Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

! В выводе команды ping указан IP-адрес (198.133.219.25),
! что подтверждает работу сервера DNS.
! Тем не менее команда дает отрицательный результат, возможно, из-за
! списков ACL, фильтрующих трафик ICMP.
C:\>ping www.cisco.com

Pinging www.cisco.com [198.133.219.25] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.133.219.25:
  Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
! Ниже мы проверяем кеш ARP и видим запись для стандартного шлюза.
C:\>arp -a
Interface: 192.168.1.102 --- 0x2
  Internet Address      Physical Address          Type
  192.168.1.1           00-13-10-d4-de-08        dynamic
! Теперь проверим кеш имен и убедимся в том, что команда ping
! вызвала обращение к серверу DNS и было получено имя дистанционного
! хоста.
C:\>ipconfig /displaydns
Windows IP Configuration
  www.cisco.com
  -----
  Record Name . . . . . : www.cisco.com
  Record Type . . . . . : 1
```

```

Time To Live . . . . : 26190
Data Length . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 198.133.219.25

```

! Некоторые строки опущены для краткости

ВНИМАНИЕ!

При подготовке к экзаменам CCNA следует сосредоточиться на концепциях, лежащих в основе этих команд, а не на точной формулировке их вывода.

На рис. 21.2 показан пример конфигурирования IP-адреса хоста, маски, стандартного шлюза и сервера DNS вручную (т.е. статическая конфигурация). Те же настройки можно ввести с помощью команд, но большинство пользователей предпочтуют использовать графический интерфейс.

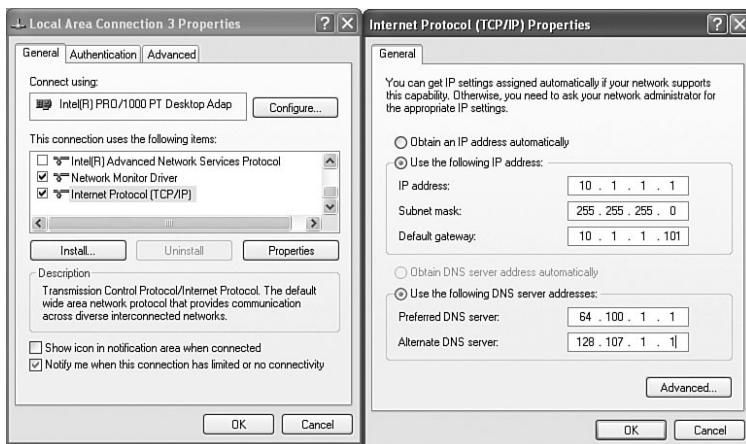


Рис. 21.2. Конфигурирование IP-адреса и параметров сети в операционной системе Windows

Поиск и устранение неисправностей в службах маршрутизации хоста

Поиск и устранение неисправностей в рассматриваемом случае должны следовать алгоритму работы сети в рабочей станции. Первый вопрос, требующий ответа: “Может ли хост успешно отправлять и принимать пакеты эхо-запросов к хостам в той же подсети?” Если такая команда `ping` дает отрицательный результат, то могут быть две причины неработоспособности:

Две наиболее вероятные причины, почему команда `ping` возвращает отрицательный результат для двух хостов



- у двух рабочих станций неправильно настроены IP-адреса и маски, поэтому один из двух хостов полагает, что относится к другой подсети;
- у двух рабочих станций правильно настроены IP-адреса и маски, но на уровне среды Ethernet есть какие-то неисправности.

На экзамене прежде всего изучите IP-адреса и маски хостов, определите адрес подсети и диапазон адресов в ней. Если подсети для всех хостов в сети совпадают, то следует искать неисправности на уровне 1 и 2 в среде Ethernet, как описано в главе 10 и в главе 3 второго тома.

Если рабочая станция успешно отправляет и принимает пакеты эхо-запросов от хоста в той же подсети, следует проверить, проходят ли запросы к IP-адресам из других подсетей, и таким образом проверить следующий этап алгоритма маршрутизации пакетов хостом. Для проверки воспользуйтесь следующими действиями:

- выполните эхо-запросы к IP-адресу стандартного шлюза, чтобы убедиться, что хост может пересыпать пакеты через локальную сеть к стандартному шлюзу и получать ответы;
- выполните эхо-запросы к IP-адресу из другой посети со стандартного шлюза (маршрутизатора), но не к адресу хоста в локальной сети.

Например, как показано на рис. 21.1, на рабочей станции ПК1 можно выполнить команду `ping 172.16.1.253`, чтобы проверить, что она может отправлять и принимать пакеты от стандартного шлюза. Если команда даст положительный результат, на хосте ПК1 можно выполнить команду `ping 172.16.2.253`, благодаря которой рабочая станция будет использовать настройки стандартного шлюза, поскольку для ПК1 адрес 172.16.2.253 находится в другой подсети.

Итак, если проверка с помощью программы `ping` дает положительный результат для хостов в той же подсети и отрицательный — для хостов в других подсетях, то типичные причины такой ошибки могут быть следующими.

 Ключевая тема Три наиболее распространенные причины, почему команда `ping` возвращает положительный результат в той же подсети и отрицательный для хостов из других подсетей

- Есть несоответствие между настройками стандартного шлюза хоста и конфигурацией самого стандартного шлюза или маршрутизатора, выступающего в качестве такового. Проблема может заключаться в несоответствии масок хоста и маршрутизатора, что опять же повлияет на то, как устройства идентифицируют диапазоны адресов подсети, или хост может считать неправильный IP-адрес стандартным шлюзом.
- Если настройки стандартного шлюза правильны, но проверка с помощью программы `ping` шлюза дает отрицательный результат, то в локальной сети есть проблема на первом или втором уровнях (Layer 1 или 2).
- Если настройки стандартного шлюза правильны и проверка с помощью программы `ping` шлюза дает положительный результат, но проверка с помощью программы `ping` одного из интерфейсов маршрутизатора дает отрицательный результат (например, `ping 172.16.2.253`, см. рис. 21.1), то это может свидетельствовать о том, что отказал интерфейс маршрутизатора.

В этом разделе описываются различные сетевые проблемы и методы их обнаружения для рабочих станций, тем не менее следует помнить, что самая основная и часто встречающаяся ошибка — несоответствие IP-адресов и масок хостов в сети. Для успешной сдачи сертификационного экзамена следует уметь быстро находить

IP-адреса и маски и уметь быстро выполнять расчеты, которые описаны в части III, чтобы обнаружить источник проблемы.

Поиск правильного маршрута в маршрутизаторе

В главе 5 был подробно описан процесс маршрутизации пакета. Ключевой момент процесса связан со сравнением IP-адреса получателя пакета с существующей таблицей маршрутизации IP устройства. Маршрут, с которым совпадает IP-адрес получателя, содержит информацию об интерфейсе, через который нужно отправить пакет дальше, и в некоторых случаях IP-адрес следующего транзитного узла на маршруте.

В сети может быть ситуация, когда в таблице маршрутизации конкретного устройства есть больше одного маршрута, соответствующего IP-адресу получателя в пакете. Такое положение дел вполне нормально и часто возникает в реальных сетях, например, если используется метод автоматического суммирования адресов сетей, суммирования вручную, если есть статические маршруты или резервные каналы.

Сертификационный экзамен может проверять знание и понимание теоретических основ маршрутизации, в частности, в нем может быть задание, в котором вопрос стоит так: “Какой маршрут будет выбран для такого-то пакета IP?” Чтобы уверенно отвечать на подобные вопросы, следует помнить перечисленные ниже факты.

Описание процесса поиска соответствия адресу получателя маршрутизатором при маршрутизации



- Если определенному IP-адресу получателя соответствует более одного маршрута в таблице маршрутизации, устройство использует наиболее специфичный маршрут, т.е. маршрут с наибольшей длиной префикса.
- Маршрутизатор использует двоичную математику для сравнения IP-адресов и маршрутов в таблице маршрутизации, однако пользователям удобнее сравнивать числа в десятичном виде. Если указанная для маршрута подсеть создает диапазон адресов, включающий в себя адрес получателя пакета, то считается, что маршрут соответствует пакету.
- Если в задании используется эмулятор сетевого оборудования, найти соответствующий IP-адресу получателя маршрут можно с помощью команды `show ip route адрес`, в выводе которой будет показан маршрут для адреса, указанного в команде.

В примере 21.2 показана типичная таблица маршрутизации маршрутизатора, в которой есть перекрывающиеся маршруты. Внимательно просмотрите информацию в таблице маршрутизации, прежде чем читать объяснения после примера, и укажите, по каким маршрутам будут переданы пакеты, адрес получателя которых равен 172.16.1.1, 172.16.1.2, 172.16.2.2 и 172.16.4.3.

Пример 21.2. Команда `show ip route` показывает перекрывающиеся маршруты в таблице маршрутизации

```
R1#show ip route rip
Codes: C - connected, S - static, 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
```

```
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS
level-2
ia - IS-IS inter area, * - candidate default, U - per-user static
route
o - ODR, P - periodic downloaded static route
```

Gateway of last resort is not set

```
172.16.0.0/16 is variably subnetted, 5 subnets, 4 masks
R      172.16.1.1/32 [120/1] via 172.16.25.2, 00:00:04, Serial0/1/1
R      172.16.1.0/24 [120/2] via 172.16.25.129, 00:00:09, Serial0/1/0
R      172.16.0.0/22 [120/1] via 172.16.25.2, 00:00:04, Serial0/1/1
R      172.16.0.0/16 [120/2] via 172.16.25.129, 00:00:09, Serial0/1/0
R      0.0.0.0/0 [120/3] via 172.16.25.129, 00:00:09, Serial0/1/0
```

R1#show ip route 172.16.4.3

```
Routing entry for 172.16.0.0/16
  Known via "rip", distance 120, metric 2
  Redistributing via rip
  Last update from 172.16.25.129 on Serial0/1/0, 00:00:19 ago
  Routing Descriptor Blocks:
* 172.16.25.129, from 172.16.25.129, 00:00:19 ago, via Serial0/1/0
    Route metric is 2, traffic share count is 1
```

Чтобы найти соответствующий IP-адресу пакета маршрут в таблице маршрутизации, нужно прежде всего определить по маске диапазон адресов для подсети. Далее нужно сравнить адрес получателя с диапазонами адресов всех подсетей и получить таким образом все подходящие маршруты. В том случае, если IP-адрес получателя попадает одновременно в диапазоны адресов для нескольких подсетей, нужно выбрать подсеть с наибольшей длиной префикса. Из информации, представленной в примере 21.2, можно сделать следующие выводы.

- IP-адресу получателя 172.16.1.1 подходят все пять маршрутов, но маршрут к хосту 172.16.1.1 с длиной префикса /32 будет выбран для пересылки пакета, поскольку это наибольшая длина префикса среди всех маршрутов;
- IP-адресу получателя 172.16.1.2 подходят четыре маршрута (за исключением маршрута к хосту 172.16.1.1), наибольшая длина префикса — у маршрута 172.16.1.0/24, следовательно, он будет использоваться для передачи пакета;
- IP-адресу получателя 172.16.2.2 подходят три маршрута, из указанных в таблице маршрутизации устройства R1, но для пересылки пакета будет выбран маршрут 172.16.0.0/22, поскольку у него для такого получателя наибольшая длина префикса;
- IP-адресу получателя 172.16.4.3 подходят последние два маршрута в таблице устройства, а для пересылки пакета будет выбран маршрут 172.16.0.0/16, как маршрут с наибольшей длиной префикса.

Обратите также внимание на вывод команды `show ip route 172.16.4.3` в конце примера 21.2. В ней указан маршрут, который будет использоваться для пересылки пакетов IP-адресу 172.16.4.3. Эта команда очень удобна и пригодится как в практической работе, так и для решения задач сертификационного экзамена. В данном примере пакету, отправленному на IP-адрес 172.16.4.3, будет соответствовать маршрут на классовую сеть класса В 172.16.0.0/16 (выделено в примере).

Команды для поиска неисправностей

Несомненно, наиболее популярной командой для поиска и устранения неисправностей в маршрутизаторах и коммутаторах является команда `ping`. В главе 20 эта команда была достаточно подробно описана как в обычном, так и в расширенном режиме. Фактически команда `ping` просто пересыпает некоторый пакет хосту, а тот создает и пересыпает ответ на него, чтобы проверить, могут ли такие пакеты передаваться между хостами.

В этом разделе представлены еще три команды операционной системы Cisco IOS, которые очень пригодятся для поиска ошибок в работе сети, а именно: `show ip arp`, `traceroute` и `telnet`.

Команда `show ip arp`

Команда `show ip arp` выводит на экран содержимое кеша ARP маршрутизатора. В примере 21.3 показан вывод этой команды для маршрутизатора R1 на рис. 21.1, после того как всем хостам были заданы адреса из подсети с префиксом /24.

Пример 21.3. Пример вывода команды `show ip arp`

```
R1#show ip arp
Protocol Address      Age (min)  Hardware Addr  Type  Interface
Internet 172.16.1.1      8          0013.197b.2f58  ARPA  FastEthernet0/0
Internet 172.16.1.253    -          0013.197b.5004  ARPA  FastEthernet0/0
Internet 172.16.2.253    -          0013.197b.5005  ARPA  FastEthernet0/1
```

Наиболее полезная информация в выводе указанной команды: IP-адрес, MAC-адрес и интерфейс. Когда маршрутизатор пересыпает какой-либо пакет через определенный интерфейс, он использует записи, связанные только с этим интерфейсом. Например, когда устройство R1 пересыпает пакет хосту ПК1 (см. рис. 21.1, адрес 172.16.1.1), оно использует интерфейс Fa0/0, следовательно, поиск будет выполняться только в записях кеша ARP данного порта.

В специальной колонке указан таймер существования записи (`Age`). Если в ней есть какое-то число, оно показывает, сколько минут прошло с того момента, как был получен последний пакет от данного устройства. Например, из таблицы видно, что маршрутизатор R1 получал что-либо от устройства ПК1 8 минут назад, IP-адрес хоста — 172.16.1.1, MAC-адрес отправителя — 0013.197b.2f58. Таймер `Age` не показывает, сколько времени прошло от последнего запроса ARP или ответа, он сбрасывается в ноль каждый раз, когда был получен пакет от соответствующего хоста. Если в поле таймера `Age` стоит прочерк, это означает, что такая запись ARP представляет IP-адрес самого маршрутизатора, например, интерфейсу Fa0/0 с IP-адресом 172.16.1.253 устройства R1 (см. рис. 21.1) соответствует вторая строка в примере 21.3.

Команда `traceroute`

Команда `traceroute` в операционной системе Cisco IOS точно так же, как и команда `ping`, используется для проверки маршрута между маршрутизатором и хостом или между двумя маршрутизаторами. В отличие от последней она выдает также IP-адреса транзитных узлов на маршруте. Например, как показано на рис. 21.3 и в примере 21.4, если в сети из трех маршрутизаторов в устройстве R1 выполнить команду `traceroute 172.16.2.7`, то в результате будет получен маршрут следования пакета. Стрелками на рис. 21.3 показаны три IP-адреса, которые ниже выводятся в команде `traceroute`.

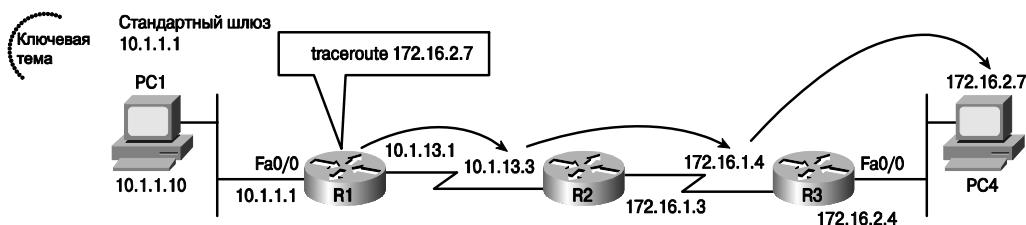


Рис. 21.3. Определение адресов с помощью команды `traceroute` операционной системы Cisco IOS

Пример 21.4. Вывод команды `traceroute`

```
R1#traceroute 172.16.2.7
Type escape sequence to abort.
Tracing the route to 172.16.2.7
```

```
1 10.1.13.3 8 msec 4 msec 4 msec
2 172.16.1.4 24 msec 25 msec 26 msec
3 172.16.2.7 26 msec 26 msec 28 msec
```

В примере показана команда `traceroute`, которая дает положительный результат проверки. Тем не менее, если бы в сети были проблемы с маршрутизацией, вывод команды выглядел бы по-другому. Представим себе ситуацию, в которой у маршрутизатора R1 есть маршрут к адресу 172.16.2.7, т.е. устройство “знает”, куда следует направить пакеты для маршрутизатора R2. А у маршрутизатора R2, например, нет маршрута к получателю 172.16.2.7. В данном случае команда `traceroute` будет выводить строку, описывающую первый транзитный узел на маршруте (см. выделенную строку в примере 21.4). Остальные устройства (т.е. соответствующие им строки) не будут выводиться на экран, и пользователю придется прервать вывод команды (нажав комбинацию клавиш `<Ctrl+Shift+6>`). Тем не менее по выводу команды можно определить, что у хоста с IP-адресом 10.1.13.3 (т.е. маршрутизатора R2) есть проблемы с маршрутизацией. После этого можно подключиться к устройству R2 с помощью команды `telnet` и попытаться установить, почему у него нет маршрута, соответствующего адресу получателя 172.16.2.7.

Следует запомнить, что команда `traceroute` выдает IP-адреса следующего транзитного узла (`next-hop`) на маршруте. Как показано в примере 21.4, IP-адрес в первой строке вывода (R2, 10.1.13.3) представляет собой адрес следующего транзитного узла на маршруте для пакета. Аналогично адрес в следующей строке (R3, 172.16.1.4) представляет собой следующий транзитный узел на маршруте с точки зрения маршрутизатора R2. Как команда `traceroute` обнаруживает маршрут и определяет IP-адреса транзитных узлов, подробно описано во втором томе книги.

ВНИМАНИЕ!

В многих операционных системах есть аналогичная команда, выполняющая те же действия. Например, в операционных системах от корпорации Microsoft есть команда `tracert`.

Запуск и приостановка сессий Telnet

Большинство сетевых инженеров ищут и устраняют ошибки в сетях за своим рабочим столом, а не непосредственно подключаясь к устройству. Чтобы получить дистан-

ционный доступ к маршрутизатору или коммутатору, инженеру нужно воспользоваться клиентом Telnet или SSH на своей рабочей станции и установить один, а чаще всего несколько сеансов дистанционной связи с разными устройствами. В качестве альтернативы инженер может подключиться к одному маршрутизатору или коммутатору при посредничестве сеанса Telnet или SSH, а потом с помощью команд `telnet` или `ssh` операционной системы Cisco IOS подключаться к другим маршрутизаторам или коммутаторам. Указанные команды работают как клиент Telnet или SSH и соответственно предоставляют абсолютно те же возможности, что и аналогичные утилиты в других операционных системах. После завершения работы из сеанса можно выйти, просто введя команду `exit`, чтобы разъединить сеанс Telnet или SSH.

Честно говоря, те специалисты, которые мало занимаются поиском и устранением неисправностей, редко используют все возможности команд `telnet` и `ssh` операционной системы Cisco IOS, им проще запустить несколько сеансов с рабочей станции к разным устройствам. Если же поиском ошибок приходится заниматься достаточно часто, то все возможности рассматриваемых команд помогут быстро переключаться между различными маршрутизаторами и коммутаторами.

Наиболее полезной функцией команд `telnet` и `ssh` в операционной системе IOS является возможность приостановки сеансов. Эта функция позволяет приостановить сеанс и перевести его в фоновый режим работы, не разрывая соединения Telnet или SSH. Следовательно, из одного устройства можно установить несколько сеансов к другим устройствам и быстро и легко переключаться между ними. На рис. 21.4 показана схема сети, которая будет использоваться для демонстрации функции приостановки сеансов.

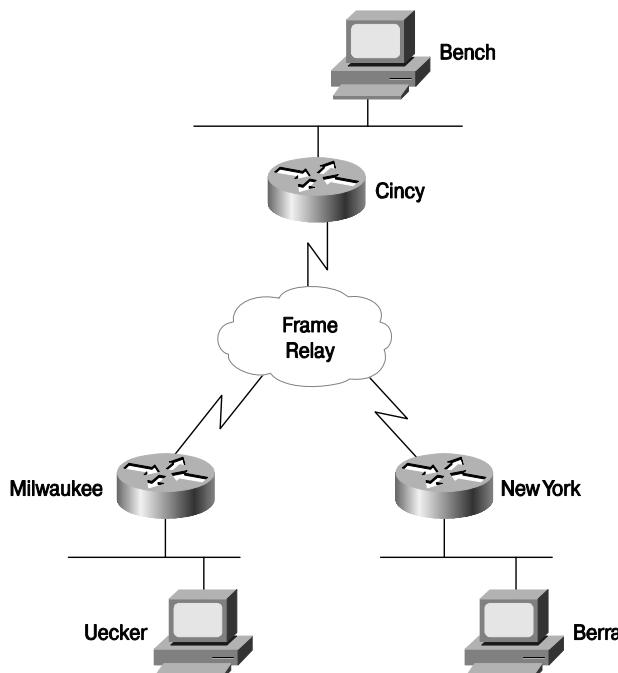


Рис. 21.4. Приостановка сеансов Telnet

Сетевой администратор работает за компьютером Bench и устанавливает сеанс Telnet с маршрутизатором Cincy. Подключившись к интерфейсу командной строки последнего, администратор из него устанавливает сеанс Telnet с маршрутизатором Milwaukee. Работая с устройством Milwaukee, сетевой администратор в некоторый момент времени подавляет сеанс, нажав комбинацию клавиш <Ctrl+Shift+6>, а потом клавишу <x>. (Обратите внимание: комбинация клавиш <Ctrl+Shift+6> посылает символ прерывания, но в некоторых национальных раскладках клавиатуры символ прерывания может быть сопоставлен с другой последовательностью клавиш.) После этого администратор устанавливает сеанс Telnet с маршрутизатором New York и, опять же, приостанавливает сеанс. В конце рассматриваемого примера сетевой администратор с помощью трех сеансов подключен к трем разным маршрутизаторам и может переключаться между ними буквально нажатием нескольких клавиш. В примере 21.5 проиллюстрирован описанный процесс подключения, а также даны некоторые комментарии по выполняемым действиям (справа в скобках).

Пример 21.5. Приостановка сеансов Telnet

```
Cincy#telnet milwaukee
Trying Milwaukee (10.1.4.252) ... Open
```

(Пользователь устанавливает сеанс Telnet с Milwaukee.)

User Access Verification

Password: (Пользователь вводит пароль и может выполнять команды.)

```
Milwaukee>
Milwaukee>
Milwaukee>
```

```
Cincy#telnet NewYork
```

Trying NewYork (10.1.6.253) ... Open

(Пользователь нажимает <Ctrl+Shift+6>, потом <x>.)

(Пользователь снова находится в командной строке маршрутизатора Cincy, поскольку сеанс был приостановлен.)

(Пользователь подключается к маршрутизатору New York, используя команду telnet NewYork.)

User Access Verification

Password:

```
NewYork>
NewYork>
NewYork>
```

(Пользователь может вводить команды в интерфейсе устройства New York)

```
Cincy#show sessions
```

(Пользователь нажимает <Ctrl+Shift+6>, потом <x>.)

(Эта команда показывает приостановленные сеансы Telnet.)

Conn	Host	Address	Byte	Idle	Conn Name
1	Milwaukee	10.1.4.252	0	0	Milwaukee
*	2 NewYork	10.1.6.253	0	0	NewYork

```
Cincy#where
```

(Команда where выводит то же самое, что и show sessions.)

```

Conn Host Address Byte Idle Conn Name
Conn   Host          Address      Byte   Idle   Conn Name
      1 Milwaukee      10.1.4.252    0       0   Milwaukee
*     2 NewYork       10.1.6.253    0       0   NewYork
Cincy#resume 1
[Resuming connection 1 to milwaukee ... ]

Milwaukee>
Milwaukee>
Milwaukee>
!
Cincy#
[Resuming connection 1 to milwaukee ... ]
Milwaukee>
Milwaukee>
Milwaukee>
Cincy#disconnect 1
Closing connection to milwaukee [confirm]
Cincy#
[Resuming connection 2 to NewYork ... ]
NewYork>
NewYork>
NewYork>
Cincy#disconnect 2
Closing connection to NewYork [confirm]
Cincy#

```

(Вернуться к соединению №1 (см. Show session), т.е. к соединению с маршрутизатором Milwaukee.)

(Пользователь может вводить команды в интерфейсе Milwaukee.)

(Пользователь нажимает <Ctrl+Shift+6>, потом <x>, чтобы переключиться обратно на маршрутизатор Cincy.)

(Пользователь просто нажал клавишу <Enter> и переключился к последнему по счету сеансу Telnet.)

(Пользователь нажимает <Ctrl+Shift+6>, потом <x>.)

(Ненужный сеанс с устройством Milwaukee разъединен!)

(Пользователь нажимает клавишу <Enter>, чтобы подтвердить отключение.)

(Пользователь просто нажал клавишу <Enter> и переключился в последний по счету сеанс Telnet.)

(Пользователь нажимает <Ctrl+Shift+6>, потом <x>.)

(Ненужный сеанс с устройством New York разъединен!)

(Пользователь просто нажал клавишу <Enter> и переключился в последний по счету сеанс Telnet.)

Пошаговые комментарии в рассмотренном выше примере объясняют практически все нюансы работы с сеансами. В начале примера 21.5 показано приглашение интерфейса командной строки маршрутизатора Cincy, к которому можно подключиться клиентом Telnet рабочей станции сетевого администратора Bench. После подключения к маршрутизатору Milwaukee сеанс Telnet приостановлен нажатием комбинации клавиш <Ctrl+Shift+6>, а потом <x>. После установки соединения Telnet с маршрутизатором New York сеанс также приостановлен с использованием той же комбинации клавиш.

Два сеанса могут быть приостановлены или возобновлены очень просто: для возобновления сеанса используется команда `resume`. Чтобы восстановить какое-либо конкретное соединение Telnet, в команде `resume` нужно указать идентификатор сеанса, который можно узнать с помощью команды `show sessions` (или с помощью команды `where`). Если же команда `resume` используется без параметров, то будет возобновлен последний по счету приостановленный сеанс Telnet. Вместо команды `resume` можно просто ввести номер нужного сеанса — это эквивалентный вариант. Например, можно ввести цифру 2, и она выполнит то же действие, что и команда `resume 2`.

Есть один интересный и потенциально опасный нюанс в приостановке и возобновлении сеансов Telnet в устройствах. Чтобы перейти к последнему по счету приостановленному сеансу, нужно нажать клавишу `<Enter>`. Это просто и удобно, но многие специалисты замечают, что иногда они нажимают клавишу `<Enter>` несколько раз подряд, чтобы сдвинуть строки интерфейса командной строки и очистить экран от того, что выводит устройство в консольный порт. Если в устройстве есть приостановленный сеанс Telnet, то он будет возобновлен в результате таких действий и специалист попадет в другое устройство. Такая ситуация может быть очень опасной, если выполняются какие-либо существенные изменения в конфигурации или используются потенциально опасные команды операционной системы Cisco IOS, поэтому нужно внимательно следить за тем, с каким устройством вы работаете, если используется приостановка сеансов Telnet.

В выводе команды `show sessions` звездочкой (*) отмечен последний активный сеанс, который был приостановлен, поэтому определить, куда именно переключится интерфейс командной строки после нажатия клавиши `<Enter>`, очень просто.

Кроме команд для приостановки и возобновления сеансов Telnet и SSH, показанных в примере 21.5, на практике пригодятся еще две команды, отображающие информацию о сеансах и подключенных к устройству пользователях. Команда `show users` показывает список подключенных к устройству пользователей. В ее выводе показаны все сеансы, в том числе консольное подключение, сеансы Telnet и SSH и др. Команда `show ssh` выводит ту же информацию, но только для пользователей, подключенных при посредничестве сеансов SSH. Обе указанные команды отличаются от рассматривавшейся выше команды `show sessions`, которая выводит список приостановленных сеансов Telnet и SSH для устройства.

На этом мы заканчиваем первый раздел главы. Во втором разделе основной акцент делается на применение методов и инструментов для поиска и устранения неисправностей, которые были описаны выше.

Сценарий поиска и устранения ошибок в маршрутизации

В этом разделе описан некоторый сценарий, состоящий из трех типичных ситуаций. В каждой ситуации (А, Б и В) есть некоторые схемы, примеры и комментарии, описывающие то, что происходит в сети. Читателю нужно будет завершить выполнение некоторых заданий и ответить на сопровождающие задание вопросы. В каждой из трех частей есть правильные ответы на контрольные вопросы.

Основная цель сценария — продемонстрировать на практике методы поиска и устранения неисправностей, обсуждавшиеся выше. Рассматриваемые ниже ситуации не совпадают полностью с задачами и вопросами, которые могут встретиться в сертификационном экзамене CCNA. Они представляют собой пример того, как

можно применять имеющиеся знания в практической работе, а также помогут подготовиться к решению самых сложных задач сертификационных тестов.

На прилагаемом к книге компакт-диске есть дополнительные задания, которые также можно использовать для подготовки к экзамену и тренировки. Еще больше заданий есть на компакт-диске, прилагаемом ко второму тому книги.

Ситуация А: задачи и вопросы

Наш сценарий начинается с ситуации, в которой есть только что установленная компьютерная сеть, но документация на нее частично отсутствует. Читатель должен изучить существующую документацию (в виде схемы сети), а также использовать различные команды группы `show`. Такая информация позволяет:

- определить IP-адрес, маску подсети (длину префикса) для каждого из интерфейсов маршрутизатора;
- рассчитать адрес подсети для каждого сегмента на схеме сети;
- завершить и усовершенствовать схему сети, указав на ней IP-адрес и длину префиксов, а также адреса подсетей;
- идентифицировать любые проблемы, которые существуют в сети с IP-адресами или подсетями, указанными на схеме сети;
- предложить метод решения для обнаруженных проблем.

В примерах 21.6–21.8 показаны выводы нужных команд для маршрутизаторов R1, R2 и R3; схема сети проиллюстрирована на рис. 21.5. В примере 21.9 показаны команды, которые сначала были набраны в текстовом редакторе, а позже скопированы в конфигурацию маршрутизатора R4.

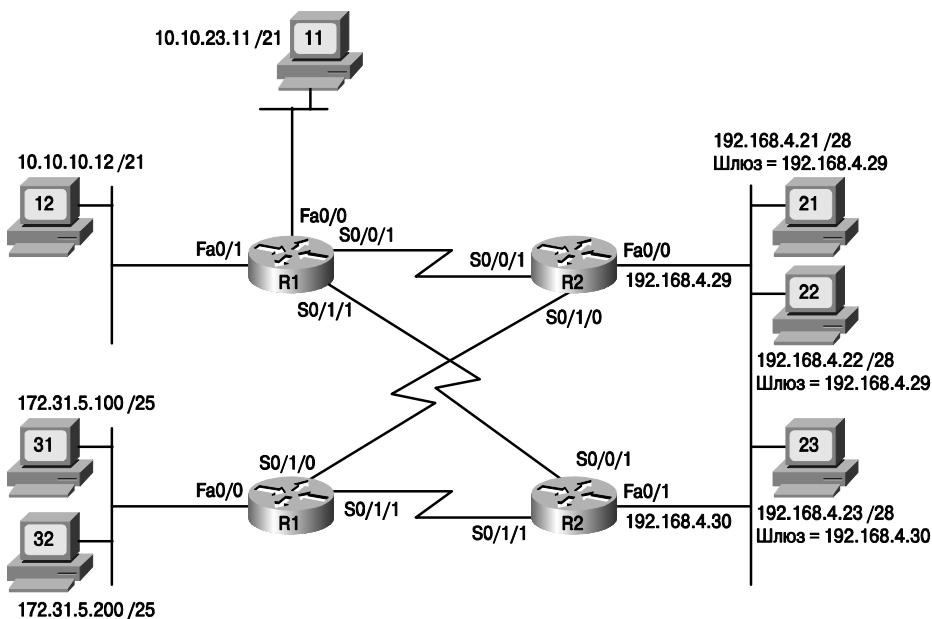


Рис. 21.5. Ситуация А: неполная схема сети

Пример 21.6. Ситуация А: информация о маршрутизаторе R1

```
R1#show ip interface brief
Interface          IP-Address      OK? Method Status          Protocol
FastEthernet0/0    10.10.24.1     YES  NVRAM  up           up
FastEthernet0/1    10.10.15.1     YES  NVRAM  up           up
Serial0/0/0        unassigned     YES  NVRAM  administratively down  down
Serial0/0/1        192.168.1.1   YES  NVRAM  up           up
Serial0/1/0        unassigned     YES  NVRAM  administratively down  down
Serial0/1/1        192.168.1.13  YES  NVRAM  up           up

R1#show protocols
Global values:
  Internet Protocol routing is enabled
FastEthernet0/0 is up, line protocol is up
    Internet address is 10.10.24.1/21
FastEthernet0/1 is up, line protocol is up
    Internet address is 10.10.15.1/21
Serial0/0/0 is administratively down, line protocol is down
Serial0/0/1 is up, line protocol is up
    Internet address is 192.168.1.1/30
Serial0/1/0 is administratively down, line protocol is down
Serial0/1/1 is up, line protocol is up
    Internet address is 192.168.1.13/30
```

Пример 21.7. Ситуация А: информация о маршрутизаторе R2

```
R2#show protocols
Global values:
  Internet Protocol routing is enabled
FastEthernet0/0 is up, line protocol is up
    Internet address is 192.168.4.29/28
FastEthernet0/1 is administratively down, line protocol is down
Serial0/0/0 is administratively down, line protocol is down
Serial0/0/1 is up, line protocol is up
    Internet address is 192.168.1.2/30
Serial0/1/0 is up, line protocol is up
    Internet address is 192.168.1.6/30
Serial0/1/1 is administratively down, line protocol is down
```

Пример 21.8. Ситуация А: информация о маршрутизаторе R3

```
R3#show ip interface brief
Interface          IP-Address      OK? Method Status          Protocol
FastEthernet0/0    172.31.5.1     YES  NVRAM  up           up
FastEthernet0/1    unassigned     YES  NVRAM  administratively down  down
Serial0/0/0        unassigned     YES  NVRAM  administratively down  down
Serial0/0/1        unassigned     YES  NVRAM  administratively down  down
Serial0/1/0        192.168.1.5   YES  NVRAM  up           up
Serial0/1/1        192.168.1.18  YES  NVRAM  up           up

R3#show ip route connected
172.31.0.0/25 is subnetted, 1 subnets
C    172.31.5.0 is directly connected, FastEthernet0/0
     192.168.1.0/24 is variably subnetted, 5 subnets, 2 masks
C      192.168.1.4/30 is directly connected, Serial0/1/0
C      192.168.1.16/30 is directly connected, Serial0/1/1
```

Пример 21.9. Ситуация А: частичная конфигурация маршрутизатора R4

! Команды, указанные ниже, были введены в текстовом редакторе
! и будут скопированы в конфигурацию маршрутизатора R4.

```
interface fa0/1
    ip address 192.168.2.23 255.255.255.240
!
interface serial 0/0/0
    ip address 192.168.1.14 255.255.255.252
!
interface serial 0/1/0
    ip address 192.168.1.19 255.255.255.252
!
! Указанные ниже команды включают протокол RIP версии 2.
router rip
    version 2
    network 192.168.1.0
    network 192.168.4.0
```

Ответы к задачам ситуации А

В примерах 21.6–21.8 указаны IP-адреса всех нужных интерфейсов для маршрутизаторов R1, R2 и R3 соответственно. Тем не менее некоторые из показанных команд не выводят информацию о масках на интерфейсах. В частности, команда `show ip interface brief` очень пригодится специалисту, чтобы быстро просмотреть состояние интерфейсов и их IP-адреса, но в ее выводе не показывается маска интерфейса. Команда `show protocols` выдает ту же информацию, но вместе с масками сетей интерфейсов.

В примере 21.8 (R3) напрямую информация о масках не показана, но ее можно достаточно просто найти. Интерфейсы и их IP-адреса можно увидеть в выводе команды `show ip interface brief`, далее достаточно сравнить полученную информацию со списком маршрутов, который выводится командой `show ip route connected`. В последней команде указана информация о маске и адресе подсети для всех рабочих интерфейсов устройства. Маршрутизатор определяет адрес подсети и маску для каждого напрямую подключенного к устройству сегмента (следовательно, и маршрута) на основе информации, указанной в команде конфигурирования интерфейса `ip address`. Используя две описанные команды, можно достаточно просто определить настройки интерфейсов маршрутизатора R3.

И наконец, в примере 21.9 показаны конфигурационные команды, которые будут использованы в маршрутизаторе R4. В них в явном виде заданы IP-адреса и маски подсетей в нескольких командах `ip address`.

На рис. 21.6 показана схема сети, которая содержит в себе ответы на все задания в ситуации А: IP-адреса, маски всех интерфейсов и адреса подсетей.

Для анализа информации, представленной на схеме сети, читатель может использовать методы и советы, представленные выше в текущей главе, в частности стандартные подходы к анализу IP-адресов и подсетей. В рассматриваемом примере можно увидеть две разные проблемы с адресацией в сети.

Первая проблема состоит в том, что компьютеры 31 и 32 находятся в разных подсетях (в левом нижнем углу рис. 21.6). В рассматриваемой ситуации IP-адрес компьютера с номером 32 равен 172.31.5.200, а длина префикса — /25, следовательно, данное устройство находится в подсети 172.31.5.128/25 с диапазоном адресов от 172.31.5.129 до 172.31.5.254. Компьютер 31 и маршрутизатор R3, которые правильно подключены к тому же сегменту локальной сети, относятся к адресной подсети 172.31.5.0/25, диапазон которой составляет 172.31.5.1 – 172.31.5.126.

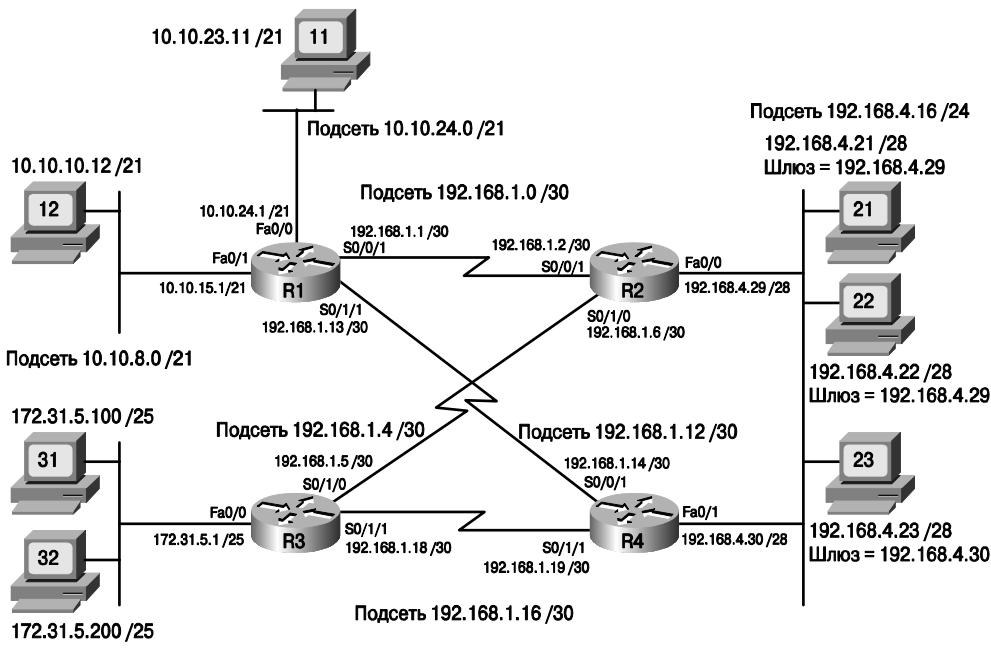


Рис. 21.6. Ситуация A: адреса подсетей и информация IP

Эта проблема препятствует пересылке пакетов маршрутизатором R3 компьютеру 32, поскольку в нем есть маршрут для адреса 172.31.5.0/25, а в реализуемый диапазон адресов не включает адрес компьютера 32, который заканчивается на .200. Таким образом, маршрутизатор R3 просто не имеет маршрутной записи, соответствующей IP-адресу компьютера 32. Аналогично неправилен установленный IP-адрес стандартного шлюза для компьютера 32 (172.31.5.1), поскольку он находится в другой адресной подсети (не совпадающей с подсетью устройства).

Вторая проблема с адресацией в рассматриваемой схеме может быть обнаружена в последовательном канале между маршрутизаторами R3 и R4. У маршрутизатора R4 задан широковещательный адрес подсети (192.168.1.19/30) для подсети 192.168.1.16/30. Эта подсеть имеет диапазон адресов 192.168.1.17–192.168.1.18 с широковещательным адресом подсети 192.168.1.19. Следует отметить, что в рассматриваемом сценарии, если попытаться ввести команды так, как это показано в примере 21.9, т.е. скопировать их из текстового редактора в конфигурацию устройства R4, то это устройство не примет команду `ip address 192.168.1.19 255.255.255.252`, так как она ошибочна — указан широковещательный адрес.

Для решения указанных проблем существует несколько подходов, но самый простой и очевидный — присвоить правильные, но неиспользуемые в других устройствах IP-адреса из нужных подсетей. Для компьютера с номером 32 нужно указать адрес из диапазона 172.31.5.1–172.31.5.126, но он не должен совпадать с используемым компьютером 31 или маршрутизатором R3. Для маршрутизатора R4 следует использовать IP-адрес 192.168.1.17, поскольку это единственный возможный вариант; адрес 192.168.1.18 уже присвоен устройству R3.

Ситуация Б: анализ маршрута пакетов и фреймов

Во втором примере ситуации продолжается рассмотрение сети, показанной на рис. 21.6. Предполагается, что ошибки в IP-адресации все еще присутствуют в сети, других проблем нет. Предполагается также, что все физические соединения корректно работают, а также в маршрутизаторах корректно настроен и запущен протокол RIP-2.

Исходя из указанных выше допущений, следует ответить на перечисленные ниже вопросы. Обратите внимание на то, что для ответа на некоторые вопросы понадобятся MAC-адреса. Они не указаны на схеме, вместо них с каждым устройством связан “псевдофизический” адрес вида R1-Fa0/1-MAC (MAC-адрес для интерфейса Fa0/1 маршрутизатора R1).

1. Компьютер 12 успешно проверяет соединение с компьютером PC21, при этом пакеты передаются по последовательному каналу между маршрутизаторами R1 и R2. Какие записи таблицы ARP будут созданы для обеспечения пересылки пакетов эхо-запросов ICMP?
2. Предположим, что компьютер с номером 12 пересыпает эхо-запросы устройству 23 и они передаются по каналу R1-R4. Какие записи таблиц ARP будут использоваться в устройствах 12, R1, R4?
3. Предположим, компьютер с номером 12 пересыпает эхо-запросы устройству 23 и они передаются по каналу R1-R2. Какие записи таблиц ARP будут использоваться для пересылки ответов (от хоста 23) на такие запросы в устройствах 23, R2, R4, R1?
4. Компьютер 31 пересыпает пакет компьютеру 22. Когда пакет передается в виде фрейма через соединение Ethernet в правой части на схеме сети, какой у него MAC-адрес отправителя и MAC-адрес получателя? Каковы его IP-адреса получателя и отправителя?
5. Компьютер 31 пересыпает пакет компьютеру 22. Когда пакет передается в виде фрейма через последовательный канал между маршрутизаторами R3 и R2, какой у него MAC-адрес отправителя и MAC-адрес получателя? Каковы его IP-адреса получателя и отправителя?
6. Компьютер 21 пересыпает пакет компьютеру 12 через канал между маршрутизаторами R2 и R1. Когда пакет передается в виде фрейма через соединение Ethernet в правой части на схеме сети, какой у него MAC-адрес отправителя и MAC-адрес получателя? Каковы его IP-адреса получателя и отправителя?
7. Компьютер 21 пересыпает пакет компьютеру 12 через канал между маршрутизаторами R2 и R1. Когда пакет передается в виде фрейма через соединение Ethernet в левой части на схеме сети, какой у него MAC-адрес отправителя и MAC-адрес получателя? Каковы его IP-адреса получателя и отправителя?

Ситуация Б: ответы

Задачи второй части сценария требуют знания принципов маршрутизации и коммутации в сетях IP. Теория нужных в данном случае читателю процессов подробно описана в главе 5. В частности, чтобы правильно ответить на перечисленные выше вопросы, необходимо помнить следующие ключевые моменты.



Резюме по MAC- и IP-адресам и их обработке в процессе передачи пакета в сети

- Пакет IP передается от хоста-отправителя к хосту-получателю.
- Заголовок и концевик канального уровня, с помощью которых инкапсулируется пакет третьего уровня, не передаются неизменными на протяжении всего маршрута следования пакета, а, наоборот, в каждом физическом сегменте используются собственные блоки: на участке от хоста до первого маршрутизатора, между двумя маршрутизаторами и т.п.
- Чтобы процесс передачи данных работал корректно, адрес получателя на канальном уровне равен идентификатору следующего транзитного узла.
- В заголовке IP содержатся IP-адреса отправителя и получателя.
- Маршрутизаторы отбрасывают заголовок и концевик для каждого принятого фрейма и добавляют новую информацию канального уровня в соответствии с выходным интерфейсом перед передачей пакета.
- В сегментах локальных сетей хосты и маршрутизаторы используют протокол ARP, чтобы узнать MAC-адреса устройств в сети Ethernet.
- В двухточечных каналах WAN протокол ARP не нужен, поскольку не используется адресация на канальном уровне.

Если у читателя по прочтении указанного списка возникают какие-либо вопросы, следует обратиться к соответствующей главе и освежить в памяти теоретический материал.

Ситуация Б: вопрос 1

В этом вопросе рассматривается маршрут потока пакетов между компьютерами 12 и 21, а также предполагается, что пакеты проходят по каналу между маршрутизаторами R1 и R2. Мы можем предположить, что поток создан с помощью команды ping и представляет собой эхо-запросы протокола ICMP, но такие предположения не повлияют на полученный ответ. Фактически нужно всего лишь указать, какие записи будут использоваться в таблице ARP каждого из устройств на маршруте.

Чтобы правильно ответить на вопрос, нужно помнить, как маршрутизатор или хост выбирает устройство, которому он будет передавать фрейм. Компьютер 12 пересыпает фрейм маршрутизатору R1, потому что IP-адрес получателя относится к другой подсети (не совпадающей с подсетью хоста 12). Маршрутизатор R1 формирует новый фрейм и пересыпает его маршрутизатору R2, последний, в свою очередь, формирует новый фрейм (т.е. добавляет новый заголовок и концевик канального уровня) и пересыпает фрейм компьютеру 21. На рис. 21.7 показаны такие фреймы и указаны MAC- и IP-адреса получателей для них.

Чтобы проанализировать фрейм, отправленный компьютером 12, следует помнить логику пересылки данных хостом — адрес получателя находится в другой подсети, следовательно, фрейм следует переслать стандартному шлюзу. Чтобы осуществить такую операцию, компьютер формирует фрейм так, чтобы он был принят именно маршрутизатором R1, т.е. ему нужно определить MAC-адрес своего стандартного шлюза (10.10.15.1), найдя его в своей таблице или выполнив запрос ARP. Если запись в таблице есть, хост 12 мгновенно формирует фрейм и передает его (первый этап на рис. 21.7), если записи нет, то компьютер рассыпает широковещательное сообщение ARP, получает ответ и создает запись в таблице MAC-адресов.

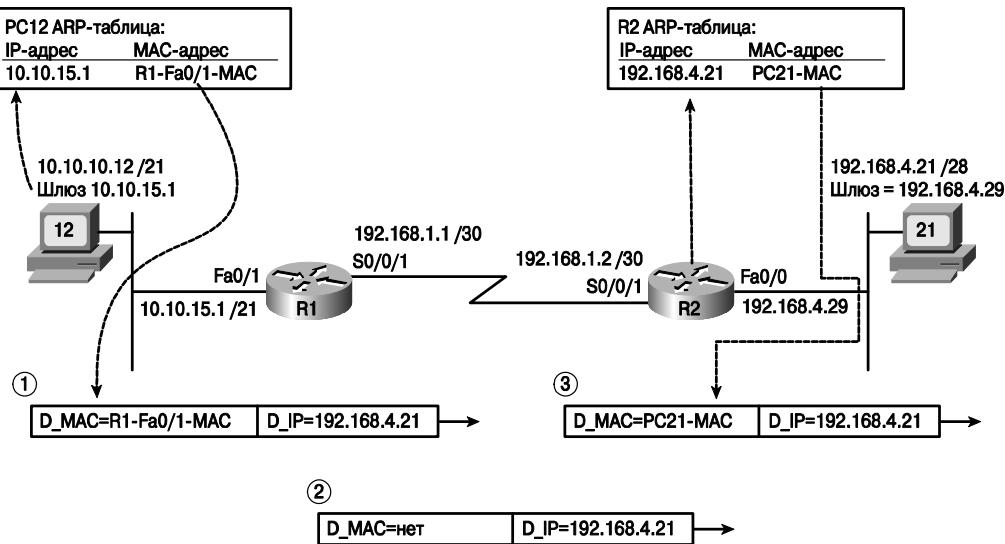


Рис. 21.7. Ситуация Б: ответ на вопрос 1

Следует также помнить, что компьютер 12 не знает MAC-адреса компьютера 21, поскольку он не передает фрейм получателю напрямую. Сначала пакет инкапсулируется во фрейм и передается стандартному шлюзу, поэтому для устройства более важной является информация о его MAC-адресе.

Второй этап (см. рис. 21.7) иллюстрирует передачу фрейма, после того как маршрутизатор R1 отбросил для входного фрейма заголовок и концевик Ethernet и принял решение о пересылке пакета через интерфейс S0/0/1 маршрутизатору R2, поэтому он присоединил к пакету стандартный заголовок канального уровня для последовательных каналов HDLC. IP-адрес получателя пакета (192.168.4.21), вполне очевидно, не изменился. Протокол HDLC применяется только в двухточечных каналах и не использует MAC-адресов, следовательно, протокол ARP в данном случае не нужен. Для этого этапа можно указать, что записи ARP в таблице маршрутизатора R1 для передачи пакета дальше не используются.

И наконец, третий, и последний, этап описывает передачу пакета, после того как маршрутизатор R2 отбросил заголовок и концевик протокола HDLC для входящего фрейма и прикрепил к нему новые блоки канального уровня инкапсуляции Ethernet. Маршрутизатор R2 пересыпает пакет через интерфейс Fa0/0, к которому напрямую подключен компьютер 21, следовательно, в заголовок фрейма он добавляет MAC-адрес хоста 21. Аналогично рассмотренному выше случаю, устройству понадобится запись в таблице ARP для соответствующего устройству IP-адреса (192.168.4.21). Если у маршрутизатора нет записи в таблице MAC-адресов, он отправит запрос ARP (широковещательный), если есть — сразу же сформирует фрейм.

Ситуация Б: вопрос 2

В ответе на второй вопрос используется та же логика и алгоритмы, что и в первой задаче. В данном случае компьютер 12, маршрутизаторы R1 и R4 участвуют в пересылке пакета и делают это в три этапа, описанные ниже.

- Компьютер 12 принимает решение об отправке пакета своему стандартному шлюзу, поскольку IP-адрес получателя (192.168.4.23) относится к другой подсети. Следовательно, хосту 12 понадобится запись в таблице ARP для стандартного шлюза (10.10.15.1 или R1).
- Маршрутизатор R1 получает фрейм, отбрасывает заголовок и концевик канального уровня и пересыпает данные маршрутизатору R4 по последовательному соединению. В канале используется инкапсуляция HDLC, следовательно, устройство R1 не использует протокол ARP.
- Маршрутизатор R1 получает фрейм, отбрасывает заголовок и концевик канального уровня протокола HDLC. Далее он принимает решение об отправке пакета непосредственно компьютеру 23 через интерфейс Fa0/1 и использует для этого запись в таблице ARP для IP-адреса 192.168.4.23 (хоста 23).

На рис. 21.8 показаны записи таблиц ARP, которые будут использоваться при передаче пакета от компьютера 12 до 23. Обратите внимание на то, что на рисунке также показаны соответствующие IP-адреса следующих транзитных узлов (next-hop), их MAC-адреса и MAC-адрес, добавляемый в новый заголовок канального уровня фрейма Ethernet.

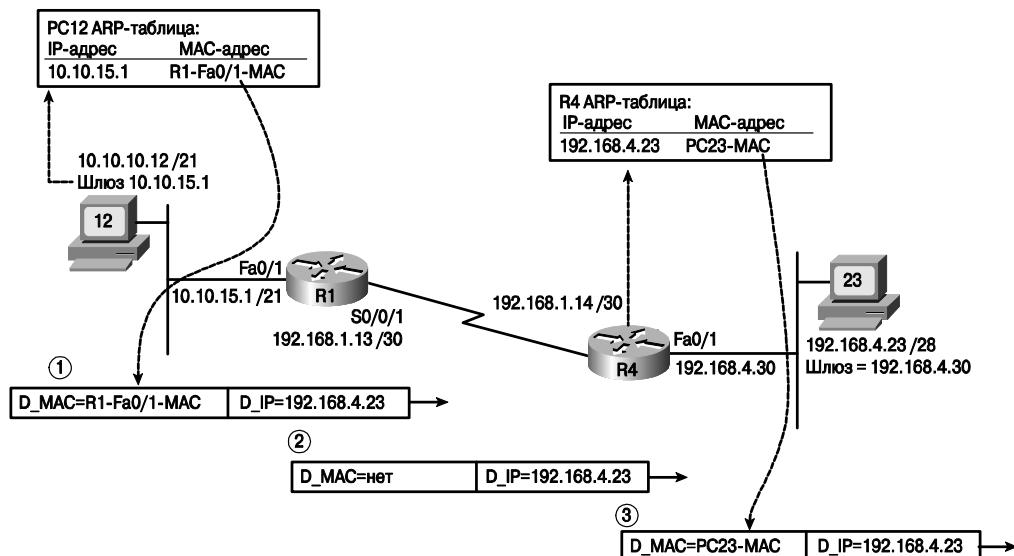


Рис. 21.8. Записи в таблицах ARP: вопрос 2

Ситуация Б: вопрос 3

Коварство этого вопроса заключается в том, что два маршрутизатора подсоединенны к сегменту локальной сети (см. рис. 21.6, справа), следовательно, у компьютера 23 есть два возможных маршрута, и два устройства могут использоваться в качестве стандартного шлюза. В задании предполагается, что пакеты ICMP эхо-запросов от компьютера 12 следуют через маршрутизатор R1, потом через R2 и по локальной сети передаются к компьютеру с номером 23. Узел 23 должен отправить ответы ICMP устройству 12, поэтому, чтобы правильно ответить на вопрос, нужно определить, по

какому маршруту пойдет поток данных, и потом определить, какие записи в таблицах ARP будут использоваться каждым из устройств.

Компьютер 23 использует ту же логику при пересылке пакетов — если получатель находится в другой подсети, устройство должно отправить пакет стандартному шлюзу. В рассматриваемом случае, когда компьютер 23 отправляет пакет ICMP эхо-ответа компьютеру 12, последний находится в другой подсети, следовательно, пересылка будет проходить через транзитный узел с адресом 192.168.4.30 (R4) — стандартный шлюз компьютера 23. Очевидно, что маршрутизатор R4 отправит пакет маршрутизатору R1, который перешлет информацию непосредственно хосту с номером 12.

Записи в таблицах ARP устройств 23, R4, R1 и 12 будут использоваться согласно указанному ниже списку.

1. Компьютер 23 принимает решение о пересылке пакета своему стандартному шлюзу, R4. Следовательно, хосту 23 нужна запись для стандартного шлюза (192.168.4.30) в его таблице ARP, чтобы сформировать фрейм.
2. Маршрутизатор R4 получает фрейм, отбрасывает заголовок и концевик канального уровня и принимает решение о пересылке пакета далее по последовательному каналу к маршрутизатору R1. В этом канале используется протокол HDLC, следовательно, маршрутизатор R4 не использует протокол ARP.
3. Маршрутизатор R1 получает фрейм от устройства R4 и отбрасывает информацию канального уровня протокола HDLC. Далее маршрутизатор принимает решение о пересылке пакета напрямую компьютеру 12 через интерфейс Fa0/1, следовательно, ему нужна запись в таблице ARP для хоста с IP-адресом 10.10.10.12 (компьютера 12).

На рис. 21.9 представлены записи таблицы ARP, необходимые для передачи пакетов с компьютера 23 на компьютер 12. Обратите внимание на то, что рисунок демонстрирует также корреляцию между IP-адресом следующего транзитного узла и MAC-адресом, при последующем добавлении MAC-адреса к новому заголовку канала Ethernet.

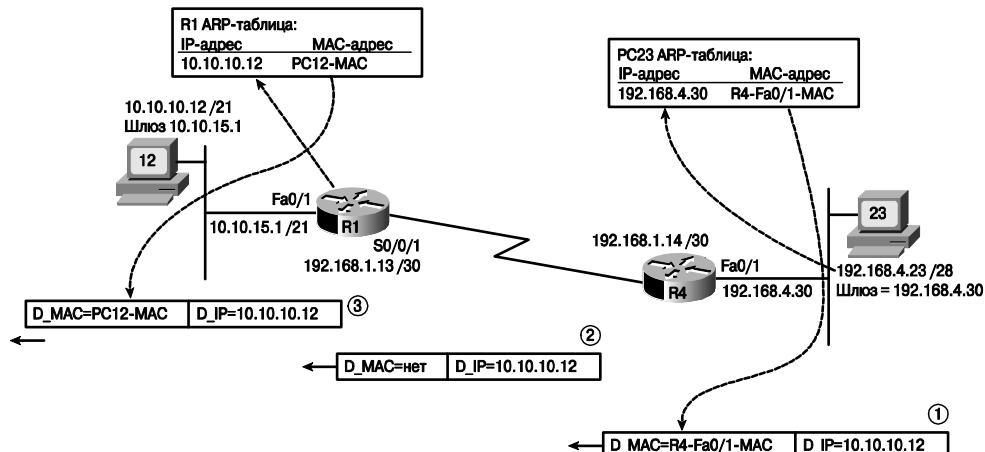


Рис. 21.9. Записи таблиц ARP для вопроса 3

Ситуация Б: вопрос 4

В этом задании рассматривается пакет, пересылаемый компьютером 31 компьютеру 22, но вопрос касается только сегмента локальной сети, который размещен на схеме сети справа (см. рис. 21.6). Чтобы наиболее полно и правильно ответить на вопрос, нужно вспомнить, что IP-адрес отправителя и получателя остаются неизменными при передаче пакета по сети, а адреса отправителя и получателя меняются при прохождении пакета через каждое промежуточное устройство, т.е. каждый маршрутизатор на маршруте убирает старый и добавляет новый заголовок и концевик фрейма. Кроме того, нужно помнить, что последовательный канал между маршрутизаторами R3 и R4 не функционирует из-за ошибочной конфигурации (указанный в конфигурации IP-адрес 192.168.1.19 для маршрутизатора R4 неправильный), следовательно, пакеты IP могут быть переданы только по каналу между маршрутизаторами R3 и R4. В данной ситуации пакет будет передаваться по такому маршруту: компьютер 31 → маршрутизатор R3 → маршрутизатор R2 → компьютер 22.

Итак, рассматриваемый пакет (от компьютера 31 к компьютеру 22) будет передаваться через локальную сеть справа на схеме к стандартному шлюзу, в итоге он попадет в маршрутизатор R2, который передаст его через сегмент локальной сети напрямую компьютеру 22. В данном случае маршрутизатор R2 сформирует новый заголовок Ethernet, в качестве адреса отправителя в котором будет стоять MAC-адрес интерфейса Fa0/0 устройства R2, а в качестве адреса получателя — MAC-адрес компьютера 22. IP-адреса отправителя 172.31.5.100 (31) и получателя 192.168.4.22 (22) не изменятся.

На рис. 21.10 показаны адреса канального и сетевого уровней для всех фреймов и пакетов, пересылаемых от компьютера 31 к устройству 22.

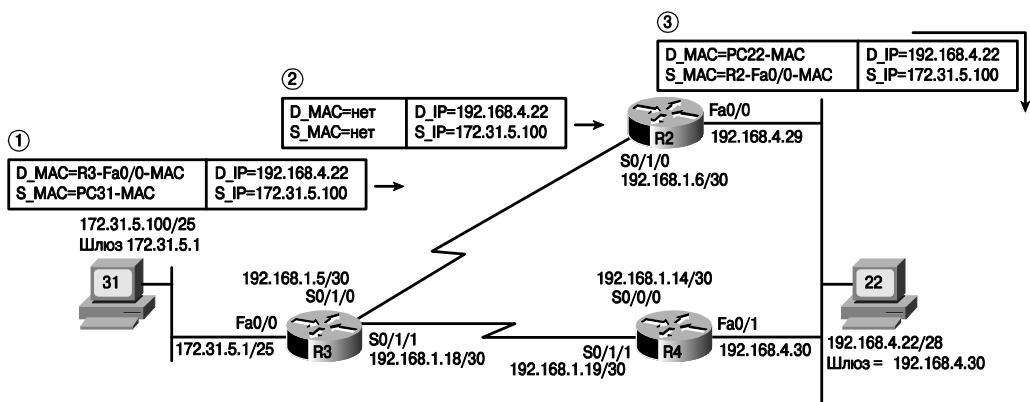


Рис. 21.10. Записи таблиц ARP для вопроса 4

Ситуация Б: вопрос 5

В этом вопросе описан тот же поток данных, что и в вопросе 4, но основное внимание уделяется механизму пересылки фрейма в последовательном канале между маршрутизаторами R3 и R2. На вопрос легко ответить, если читатель помнит, что маршрутизатор отбрасывает заголовки и концевики канального уровня при обработке принятого фрейма и инкапсулирует пакет в новую информацию канального уровня, перед тем как передать его дальше. Заголовок и концевик канального уровня зависят от того интерфейса, через который пересыпается пакет.

В рассматриваемом случае маршрутизаторы используют инкапсуляцию HDLC, которая является стандартным форматом фрейма для двухточечных последовательных каналов в маршрутизаторах Cisco. В заголовках протокола HDLC нет никаких MAC-адресов, фактически адреса второго (канального) уровня там абсолютно излишни, поскольку, если канал двухточечный и, например, маршрутизатор R3 пересыпает фрейм через такой канал, маршрутизатор в любом случае получит такой фрейм, поскольку он является единственным устройством на другом конце канала. В результате в ответе не фигурируют никакие MAC-адреса, так как они не используются, а IP-адреса отправителя 172.31.5.100 (31) и получателя 192.168.4.22 (22) не изменяются. На рис. 21.10 можно почерпнуть всю необходимую информацию для ответа на вопрос и убедиться, что при использовании инкапсуляции HDLC MAC-адреса не используются.

Ситуация Б: вопрос 6

В этом вопросе анализируется пакет, пересылаемый компьютером 21 компьютеру 12, а основное внимание уделяется локальной сети в правой части схемы на рис. 21.6. В вопросе также указано, что пакет пересыпается маршрутизатором 21 маршрутизатору R2, от последнего — маршрутизатору R1, а затем — компьютеру 12.

В данном случае компьютер 21 пересыпает пакет, инкапсулируя его во фрейм Ethernet, маршрутизатору R2. Чтобы сформировать фрейм, MAC-адрес компьютера 21 указывается в качестве адреса канального уровня отправителя, а MAC-адрес интерфейса Fa0/0 маршрутизатора R2 указывается в качестве идентификатора получателя. IP-адреса отправителя 192.168.4.21 (21) и получателя 10.10.10.12 (12) не изменяются на всем маршруте между устройствами 21 и 12. На рис. 21.11 показаны фреймы для текущего и следующего заданий.

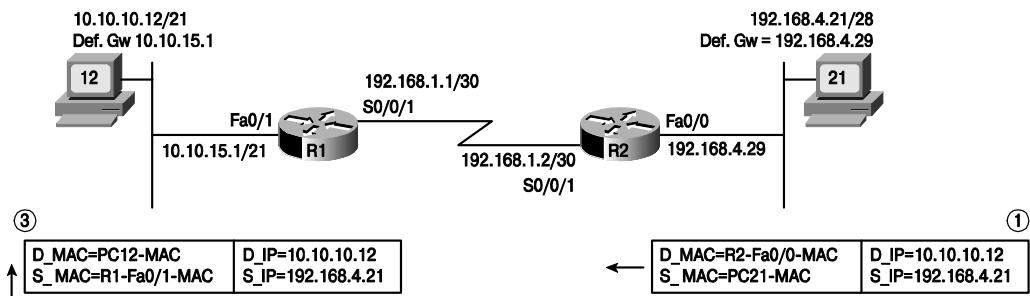


Рис. 21.11. Записи таблиц ARP для вопросов 5 и 6

Ситуация Б: вопрос 7

Этот вопрос фактически является продолжением вопроса 6, в нем исследуется тот же пакет, пересыпаемый между хостами 21 и 12, но основное внимание уделяется участку маршрута, расположенному слева на схеме сети (см. рис. 21.6). Полный маршрут пакета выглядит таким образом: узел 21 пересыпает пакет маршрутизатору R2, устройство R2 — маршрутизатору R1, а последний — хосту 12.

Итак, вначале узел 21 пересыпает пакет IP с адресом отправителя 192.168.4.21 (адрес хоста 21) и адресом получателя 10.10.10.12 (узел 12). Чтобы доставить пакет, компьютер с номером 21 инкапсулирует его во фрейм Ethernet и пересыпает стан-

дартному шлюзу — маршрутизатору R2. Маршрутизатор R2 отбрасывает инкапсуляцию Ethernet и перед отправкой пакета маршрутизатору R1 инкапсулирует его в информацию протокола HDLC. Получив фрейм, маршрутизатор R1 отбрасывает заголовок и концевик протокола HDLC и принимает решение об отправке пакета через интерфейс Fa0/1. Как обычно, IP-адреса отправителя и получателя в процессе пересылки пакета не изменяются.

Перед тем как отправить пакет через интерфейс Fa0/1, маршрутизатор R1 добавляет заголовок Ethernet и соответствующий концевик к пакету. В качестве адреса отправителя в таком фрейме используется MAC-адрес интерфейса Fa0/1 маршрутизатора R1, а в качестве адреса получателя — MAC-адрес хоста 12 из таблицы ARP интерфейса. Процесс передачи показан на рис. 21.10, который также использовался для ответа на предыдущий вопрос.

Ситуация В: анализ маршрутов

В третьем задании рассматриваемого сценария нужно предугадать, какую информацию будет выводить команда `show ip route connected` для маршрутизаторов R4 и R1. Следует помнить, что ошибки, которые были обнаружены и подробно обсуждены в первом задании (ситуация А), *не были исправлены*. Чтобы освежить схему сети в памяти и вспомнить, что происходит в маршрутизации, следует обратиться к рис. 21.6, а также к примерам 21.5–21.9.

Ситуация В: ответы

Маршрутизаторы заносят сети, подключенные к ним напрямую (т.е. указанные на интерфейсах), в свои таблицы маршрутизации в том случае, если:

 **Два основных условия добавления маршрута к напрямую подключеной подсети в таблицу маршрутизации**

- коды состояния интерфейса показывают, что физический и канальный уровни работают (выводится два кода: “up” и “up”);
- IP-адрес интерфейса правильный.

Для каждого интерфейса, соответствующего указанным двум требованиям, маршрутизатор рассчитывает адрес подсети на основе IP-адреса и маски подсети, которые указаны в команде `ip address` в режиме конфигурирования интерфейса. Благодаря информации, полученной в заданиях ситуации А и Б выше, а также согласно схеме сети на рис. 21.5, мы можем сказать, что на всех интерфейсах маршрутизаторов указаны IP-адреса и порты находятся в рабочем состоянии (`up/up`), за исключением интерфейса S0/1/1 маршрутизатора R4. Этому интерфейсу сетевой инженер попытался присвоить адрес, совпадающий с широковещательным адресом подсети, но маршрутизатор не принял соответствующую команду `ip address`. В табл. 21.5 показаны маршруты маршрутизаторов R1 и R4, подключенных напрямую.

Чтобы просмотреть сети, подключенные напрямую, и маршруты на них в маршрутизаторе, следует использовать команду `show ip route connected`. Эта команда просто выдает отфильтрованный список маршрутов по указанному параметру, а именно — только непосредственно подключенные к устройству сети. В примерах 21.10–21.11 показан вывод этой команды для маршрутизаторов R1 и R4 соответственно.

Таблица 21.5. Непосредственно подключенные маршруты маршрутизаторов R1 и R4

Устройство и интерфейс	IP-адрес	Подсеть	Выходной интерфейс
R1 Fa0/0	10.10.24.1/21	10.10.24.0/21	Fa0/0
R1 Fa0/1	10.10.15.1/21	10.10.8.0/21	Fa0/1
R1 S0/0/1	192.168.1.1/30	192.168.1.0/30	S0/0/1
R1 S0/1/1	192.168.1.13/30	192.168.1.12/30	S0/1/1
R4 S0/0/1	192.168.1.14/30	192.168.1.12/30	S0/0/1
R4 Fa0/1	192.168.4.30/28	192.168.4.16/28	Fa0/1

Пример 21.10. Вывод команды show ip route connected для маршрутизатора R1

```
R1#show ip route connected
  10.0.0.0/21 is subnetted, 2 subnets
C      10.10.8.0 is directly connected, FastEthernet0/1
C      10.10.24.0 is directly connected, FastEthernet0/0
  192.168.1.0/24 is variably subnetted, 5 subnets, 2 masks
C      192.168.1.12/30 is directly connected, Serial0/1/1
C      192.168.1.0/30 is directly connected, Serial0/0/1
```

Пример 21.11. Вывод команды show ip route connected для маршрутизатора R4

```
R4#show ip route connected
  192.168.4.0/28 is subnetted, 1 subnets
C      192.168.4.16 is directly connected, FastEthernet0/1
  192.168.1.0/24 is variably subnetted, 5 subnets, 2 masks
C      192.168.1.12/30 is directly connected, Serial0/0/1
```

Если сравнить выделенную в примере 21.11 информацию с командой `ip address 192.168.4.30 255.255.255.240` в примере 21.9, которая была введена в режиме конфигурирования интерфейса Fa0/1 маршрутизатора R4, можно сделать некоторые выводы. Маска из команды `ip address` может быть использована для определения того, как выглядит префиксная запись той же маски — /28. Адрес и маска могут быть использованы для определения адреса подсети — 192.168.4.16. Именно эта информация выделена в выводе команды `show ip route connected` в примере 21.11.

Подготовка к экзамену

Повторите все ключевые темы

Повторите все ключевые темы данной главы, помеченные пиктограммой “Ключевая тема”. Ключевые темы и соответствующие им страницы перечислены в табл. 21.6.

Таблица 21.6. Ключевые темы главы 21

Элемент	Описание	Страница
Список	Зарезервированные значения адресов, которые ни в коем случае не могут быть назначены хостам	561
Табл. 21.2	Как определить, можно ли использовать нулевую и широковещательную подсети	562
Список	Список советов по решению заданий, связанных с IP-адресацией на экзамене	564
Список	Маршрутизация, IP-адресация, преобразование имен и запросы ARP с точки зрения хоста	564
Список	Две наиболее вероятные причины, почему команда ping возвращает отрицательный результат для двух хостов	567
Список	Три наиболее распространенные причины, почему команда ping возвращает положительный результат в той же подсети и отрицательный для хостов из других подсетей	568
Список	Описание процесса поиска соответствия адресу получателя маршрутизатором при маршрутизации	569
Рис. 21.3	Определение адресов с помощью команды traceroute операционной системы Cisco IOS	572
Список	Резюме по MAC- и IP-адресам и их обработке в процессе передачи пакета в сети	582
Список	Два основных условия добавления маршрута к напрямую подключенной подсети в таблицу маршрутизации	588

Заполните таблицы и списки по памяти

Распечатайте приложение M (Appendix L) с компакт-диска или его раздел, относящийся к этой главе, и заполните таблицы и списки по памяти. В приложении N (Appendix M) приведены заполненные таблицы и списки для самоконтроля.

Список команд

В табл. 21.7 описаны команды, используемые в данной главе, и приведено краткое описание функций каждой из них. Следует еще раз повторить команды, выполняемые на конечных хостах, представленные в табл. 21.4. В этой главе нет новых конфигурационных команд.

Таблица 21.7. Команды `show` и `debug` главы 21

Команда	Описание
<code>show sessions</code>	Выводит список приостановленных сеансов Telnet и SSH в устройстве-инициаторе сеансов
<code>where</code>	Является синонимом команды <code>show sessions</code> и выводит ту же информацию
<code>telnet {имя_хоста IP-адрес}</code>	Устанавливает сеанс Telnet с дистанционным устройством
<code>ssh -l имя_пользователя {имя_хоста IP-адрес}</code>	Устанавливает сеанс SSH с дистанционным устройством
<code>disconnect [номер_соединения]</code>	Разъединяет приостановленный сеанс Telnet и SSH, идентифицируя его по указанному в параметре номеру, который может быть получен с помощью команды <code>show sessions</code>
<code>resume [номер_соединения]</code>	Возобновляет приостановленный сеанс Telnet и SSH, идентифицируя его по указанному в параметре номеру, который может быть получен с помощью команды <code>show sessions</code>
<code>traceroute {имя_хоста IP-адрес}</code>	Показывает маршрут к указанному IP-адресу получателя и отображает адреса всех промежуточных узлов на маршруте
<code><Ctrl+Shift+6>, <x></code>	Эта последовательность символов приостанавливает сеанс Telnet или SSH
<code>show ip arp</code>	Выводит содержимое таблицы ARP маршрутизатора
<code>show arp</code>	Выводит содержимое таблицы ARP маршрутизатора
<code>show ssh</code>	Показывает информацию о пользователях, подключенных к маршрутизатору сессиями протокола SSH
<code>show users</code>	Показывает информацию о пользователях, подключенных к маршрутизатору сессиями Telnet или SSH, а также через консольный порт

В этой части рассмотрены следующие темы экзамена Cisco ICND1¹...

Принципы работы сетей передачи данных:

- рассказано, как интерпретировать диаграммы сетей;
- объяснено, как определить маршрут между двумя хостами в сети;
- описаны основные компоненты сети и соединения Интернета;
- рассказано, как правильно определить наиболее распространенные сетевые проблемы на уровнях 1, 2, 3 и 7 с использованием многоуровневого подхода;
- описаны различия локальных (LAN) и распределенных (WAN) сетей и их функций.

Реализация в сети небольшого офиса филиала схемы IP-адресации и служб IP:

- объяснена теория и принцип работы технологии NAT;
- описаны частные и зарегистрированные IP-адреса;
- рассказано, как реализовать технологию NAT в сети с подключением к одному провайдеру с помощью программного обеспечения SDM и проверить ее работоспособность через интерфейс командной строки и с помощью команды ping;

Конфигурирование и проверка каналов WAN:

- описаны различные методы подключения к среде WAN;
- рассказано, как настроить и проверить простое последовательное соединение с сетью WAN;

¹ Текущие темы сертификационного экзамена приведены на сайте <http://www.cisco.com>. — Примеч. авт.

Часть V. Распределенные сети

Глава 22. “Базовые концепции распределенных сетей”

Глава 23. “Конфигурирование соединений WAN”

В этой главе...

- **Технологии WAN.** Рассматриваются несколько дополнительных технологий распределенных сетей, которые не были описаны в главе 4, а именно: модемы, DSL, кабель и ATM.
- **Службы IP для доступа к Интернету.** Рассматривается, как маршрутизатор доступа к Интернету использует функции клиента и сервера DHCP, а также NAT.

ГЛАВА 22

Базовые концепции распределенных сетей

В главе 4 были достаточно подробно рассмотрены две наиболее важные для корпоративных сетей технологии WAN:

- выделенные линии, в которых используется протокол HDLC или PPP;
- технология Frame Relay.

В IV части рассмотрены технологии сетей WAN, которые активно используются для доступа к Интернету. В главе 23 основное внимание уделено реализации и конфигурированию различных функций для сетей WAN, в частности, некоторым службам уровня 3, которые на сегодняшний день наиболее часто используются в типичном подключении к Интернету в *малых и домашних офисах* (Small Office/Home Office — SOHO).

Контрольные вопросы: знаете ли вы уже темы главы

Этот раздел предназначен для того, чтобы читатель мог предварительно оценить свои знания и решить, нужно ли ему читать главу целиком. Если ответы на девять из десяти вопросов даны правильно, можно сразу же перейти к последнему разделу “Подготовка к экзамену”. Основные темы этой главы и предварительных контрольных вопросов перечислены в табл. 22.1. Отвечая на контрольные вопросы и используя таблицу, читатель сможет достаточно точно определить свои знания в той или иной области. Ответы на вопросы приведены в приложении А.

Таблица 22.1. Темы контрольных вопросов

Основная тема	Номера вопросов
Технологии WAN	1–5
Службы IP для доступа к Интернету	6–8

1. Какое из указанных ниже утверждений лучше всего описывает функцию демодуляции модема?
 - а) Кодирует входящий аналоговый сигнал от компьютера в цифровой для передачи по телефонной сети.
 - б) Декодирует входящий цифровой сигнал из телефонной сети в аналоговый сигнал.
 - в) Кодирует набор двоичных цифр в аналоговый электрический сигнал.

- г) Декодирует аналоговый электрический сигнал от телефонной сети в цифровой сигнал.
- д) Кодирует набор двоичных цифр в цифровой электрический сигнал.
2. В каком из указанных ниже стандартов максимальная длина абонентского канала составляет 18 тыс. футов (5,5 км)?
- ADSL.
 - Аналоговый модем.
 - ISDN.
3. Какое из указанных ниже утверждений правильно описывает местоположение и функции мультиплексора DSLAM?
- Обычно используется в домашних и малых офисах для подключения телефонной линии к маршрутизатору DSL.
 - Обычно используется в домашних и малых офисах вместо маршрутизатора DSL.
 - Обычно установлен в АТС оператора связи и обязан предотвратить попадание голосового трафика в маршрутизатор провайдера.
 - Обычно установлен в АТС оператора связи и обязан разделять голосовой трафик и потоки данных.
4. Какие из перечисленных ниже технологий дистанционного доступа поддерживают стандарты, использующие как синхронный (симметричная скорость), так и асинхронный (асимметричная скорость) режим работы? (Выберите несколько ответов.)
- Аналоговые модемы.
 - WWW.
 - DSL.
 - Кабельные модемы.
5. Какая из указанных ниже технологий дистанционного доступа рассматривается как “всегда включенный” канал к Интернету? (Выберите несколько ответов.)
- Аналоговые модемы.
 - DSL.
 - Кабельные модемы.
 - Все указанные ответы верны.
6. Предположим, используется типичный маршрутизатор для подключения к Интернету через кабельный модем или модем DSL. Какую функцию будет выполнять маршрутизатор на интерфейсе, который подключен к локальной сети малого или домашнего офиса?
- Будет работать как сервер DHCP.
 - Будет работать как клиент DHCP.

в) Будет выполнять преобразование NAT/PAT для адреса отправителя в пакетах, выходящих из интерфейса.

г) Будет работать как сервер DNS.

7. Предположим, используется типичный маршрутизатор для подключения к Интернету через кабельный модем или модем DSL. Какую функцию будет выполнять маршрутизатор на интерфейсе, который подключен к Интернету? (Выберите несколько ответов.)

а) Будет работать как сервер DHCP.

б) Будет работать как клиент DHCP.

в) Будет выполнять преобразование NAT/PAT для адреса отправителя в пакетах, выходящих из интерфейса.

г) Будет работать как сервер DNS.

8. Предположим, есть домашняя сеть, в которой установлен компьютер, маршрутизатор DSL и есть подключение к линии DSL. В маршрутизаторе DSL настроены стандартные характеристики и функции. Компьютеру, подключенному к маршрутизатору, задан IP-адрес 10.1.1.1. На компьютере запущен браузер, в котором введен адрес веб-сервера www.cisco.com. Какое из указанных ниже утверждений верно для такого случая? (Выберите несколько ответов.)

а) Веб-сервер может определить, что он взаимодействует с хостом с IP-адресом 10.1.1.1.

б) Компьютер определяет IP-адрес веб-сервера www.cisco.com как открытый и зарегистрированный адрес.

в) Адрес 10.1.1.1 будет внутренним локальным (inside local) IP-адресом.

г) Адрес 10.1.1.1 будет внутренним глобальным (inside global) IP-адресом.

Основные темы

Распределенная сеть (Wide Area Network — WAN) отличается от локальной сети (Local Area Network — LAN) по некоторым ключевым параметрам. Наиболее существенное отличие заключается в том, что сети WAN имеют намного большую протяженность, а каналы таких сетей обычно прокладываются под землей, чтобы защитить кабель от случайного повреждения. Правительственные и государственные службы обычно запрещают среднестатистическому гражданину вести какие-либо раскопки на частной территории, поэтому кабель соединений WAN обычно прокладывается провайдерами, имеющими специальное разрешение или лицензию на выполнение подобного рода работ. После прокладки кабеля провайдер продает службы WAN различным потребителям и организациям. Последнее отличие может быть сформулировано в виде одной короткой фразы: “Локальной сетью вы владеете, распределенную сеть арендуете”.

Эта глава состоит из двух разделов. В первом из них подробно описаны различные варианты соединений WAN, в том числе и среда с коммутацией каналов, линии DSL, подключение к оператору кабельного телевидения, а также сеть ATM. Во втором разделе описаны службы уровня 3, которые понадобятся при подключении к Интернету из малого или домашнего офиса. В ней также объясняется, зачем могут понадобиться службы DHCP и NAT в маршрутизаторах, использующихся при подключении к Интернету, а особое внимание будет уделено технологии преобразования адресов NAT.

Технологии WAN

В этом разделе описаны еще четыре технологии WAN в дополнение к тем двум, которые были описаны в главе 4: выделенные линии и среда Frame Relay. Первая из технологий — соединение с помощью модемов — может быть использована для соединения практически любых двух устройств, а также для подключения к Интернету через какого-либо провайдера. Две следующие технологии — DSL и кабельные сети — используются только для подключения к Интернету. Последняя технология — ATM — похожа на службу с коммутацией пакетов Frame Relay, но используется в крупных сетях и сетях предприятий.

Перед тем как приступить к рассмотрению перечисленных технологий WAN, сначала затронем некоторые детали сети оператора связи, поскольку модемы и технология DSL используют обычные телефонные линии.

Структура телефонной сети

Под термином *открытая коммутируемая телефонная сеть* (Public Switched Telephone Network — PSTN) подразумеваю оборудование и устройства оператора телефонной связи, используемые для предоставления стандартной телефонной услуги. Обычно этим термином описывают комбинированные телефонные сети всей планеты. Слово “открытый” в названии подразумевает, что такая сеть предназначена для публичного использования (за определенную плату), слово “коммутируемый” описывает тот факт, что вызовы могут быть коммутированы между разными абонентами. Несмотря на то что сеть PSTN изначально была предназначена для передачи го-

лосовой информации, две из описываемых ниже технологий напрямую используют ее инфраструктуру для передачи данных. Поэтому знание принципов построения и работы телефонной сети поможет понять, как работают модемы и технология DSL.

Звук представляет собой акустические колебания, которые передаются через какую-либо материальную среду, обычно — воздух. Человеческое ухо слышит звук за счет того, что колебания воздуха передаются барабанной перепонке, которая преобразует их в нервные импульсы, в дальнейшем обрабатываемые человеческим мозгом.

Телефонная сеть не может передавать акустические колебания, зачастую также называемые звуковыми волнами. В телефоне есть микрофон, который преобразует звуковые колебания в аналоговый электрический сигнал. В сети PSTN аналоговый электрический сигнал может быть передан от одного телефонного аппарата другому через замкнутую электрическую цепь. Телефонный аппарат принимающей стороны преобразует аналоговый электрический сигнал в звуковые колебания через динамик телефонного аппарата.

Телефон был изобретен сравнительно давно, в 1870-х годах, Александром Беллом (Alexander Bell), чуть позже была разработана и реализована первая телефонная сеть. В такой телефонной сети, чтобы два абонента могли общаться, нужно было организовать замкнутую электрическую цепь между их телефонными аппаратами. После изобретения цифровых компьютеров, приблизительно в середине 1950-х, телефонные компании начали обновление магистральных каналов и оборудования телефонной сети и стали использовать цифровые сигналы. После перехода на цифровые технологии телефонная сеть получила значительные преимущества в плане скорости, управляемости, качества работы и возможности масштабирования.

Итак, что должна сделать телефонная компания (telco), чтобы домашний телефон абонента заработал? От дома абонента до ближайшей *ATC телефонной компании* (Central Office — CO) должен быть проложен двужильный кабель, называемый *абонентским каналом* (local loop). Один конец кабеля заведен в дом и подключен к телефонным розеткам. Второй конец (возможно, на расстоянии нескольких километров) подключен к гнезду специального устройства в офисе телефонной компании, называемого голосовым коммутатором, или АТС. На рис. 22.1 показана схема подключения и некоторые дополнительные детали.

В абонентской линии передаются аналоговые электрические сигналы голосового вызова. На рис. 22.1 показаны два абонентских канала: один подключен к телефону Энди, второй — к телефону Барни. Энди и Барни живут достаточно далеко друг от друга, поэтому их абонентские каналы подключены к разным АТС.

Когда Энди звонит Барни, происходит телефонный вызов, но сам процесс на сегодняшний день намного сложнее, чем просто создание замкнутой электрической цепи между двумя телефонными аппаратами. Сложность современного телефонного вызова связана с тем, что:

- в телефонах используются аналоговые электрические сигналы;
- голосовые коммутаторы используют цифровые каналы для передачи голосового вызова (в данном случае канал T1);
- голосовой коммутатор должен преобразовывать аналоговый сигнал в цифровой, и наоборот.

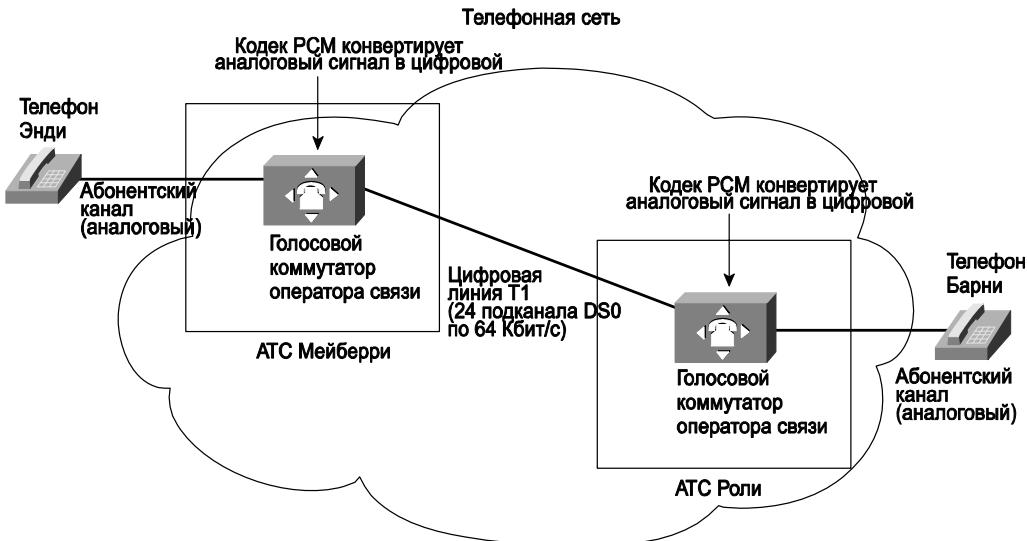


Рис. 22.1. Аналоговые голосовые вызовы через цифровую сеть PSTN

Чтобы телефонный вызов заработал, коммутатор АТС Мейберри телефонной компании выполняет аналого-цифровое преобразование для голосового сигнала от абонента Энди. Коммутатор Роли принимает цифровой сигнал от АТС Мейберри, но перед тем как передать его по абонентскому каналу Барни, эта АТС должна выполнить обратное преобразование — в аналоговый сигнал. Аналоговый сигнал передается по абонентскому каналу Барни точно так же, как сигнал передается по абонентскому каналу Энди на другом конце линии.

Изначальный стандарт для преобразования аналоговой голосовой информации называется *импульсно-кодовой модуляцией* (Pulse-Code Modulation — PCM). В кодировании PCM используется *выборка* (sampling) голосового сигнала 8 тыс. раз в секунду, и для каждого значения используется 8-битовая шкала. Следовательно, для передачи одного голосового вызова нужна скорость передачи в 64 000 бит/с, которая великолепно соответствует одному цифровому подканалу DS0 в 64 Кбит/с из 24-канальной линии T1. (В главе 4 было описано, что в канале T1 есть 24 отдельных подканала DS0 со скоростью 64 Кбит/с, а также 8 Кбит/с используется для сигнализации и служебной информации, таким образом, суммарная пропускная способность канала T1 составляет 1,544 Мбит/с.)

Современные телефонные сети (PSTN) намного сложнее и разнообразнее, чем можно себе представить по краткому описанию выше. Тем не менее несколько последующих страниц посвящено описанию некоторых ключевых моментов современных телекоммуникаций и соединений WAN. Коротко работу телефонных сетей можно описать в виде следующих этапов:

- голосовой коммутатор телефонной компании отвечает за прием и обработку аналогового сигнала в линии (т.е. по *абонентскому каналу*);
- коммутатор телефонной компании преобразует полученный аналоговый сигнал в цифровой с помощью кодека;

- оборудование телефонной компании преобразует цифровой голосовой сигнал в аналоговую форму перед передачей его по абонентскому каналу принимающего абонента;
- голосовой вызов, в том случае если используется кодирование PCM, потребляет 64 Кбит/с в цифровой части сети телефонной компании (при использовании линий T1, E1, T3, E3 и т.п.).

Аналоговые модемы

Аналоговые модемы (analog modem) нужны для передачи через последовательный порт компьютера потока битов через ту же линию, которая используется для передачи голосового вызова между двумя телефонами. Модем подключается к обычной телефонной линии (абонентскому каналу) и не требует внесения изменений как в кабельную систему, так в оборудование и настройки голосового коммутатора АТС телефонной компании. АТС оператора связи рассчитана на прием аналогового сигнала из абонентской линии, поэтому модемы передают и принимают данные в аналоговом виде через сеть PSTN. В аналоговом сигнале закодированы биты потока данных, которые один компьютер передает другому по телефонной сети вместо голосового сигнала. Аналогично тому, как телефонный аппарат преобразует звук в электрический сигнал, модемы преобразуют двоичные цифры компьютерных данных в приемлемый для телефонии аналоговый электрический сигнал.

Чтобы получить определенную битовую скорость передачи данных, модем *модулирует* (изменяет) аналоговый сигнал определенным образом. Например, чтобы получить скорость в 9600 бит/с модем может изменять аналоговый сигнал каждую 1/9600-ю долю секунды. Аналогично принимающий модем должен делать выборку аналогового сигнала каждую 1/9600-ю долю секунды, чтобы правильно интерпретировать принимаемые двоичные 0 и 1. (Процесс обратного преобразования называют *демодуляцией*. Термин *модем* (modem) является сокращением от двух слов: *модуляция* (modulation) и *демодуляция* (demodulation).)

Поскольку модемы передают данные в виде аналогового электрического сигнала, их можно без каких-либо дополнительные изменения в абонентском канале подключить к сети PSTN, запустить соединение, являющееся эквивалентом обычного голосового телефонного вызова, и передать данные. Благодаря такой технологии работы модемы могут быть использованы практически везде, где есть обычные телефонные линии.

В телефонной сети PSTN коммуникационный маршрут между двумя модемами называют *каналом* (circuit). Поскольку модем можно переключить на другого получателя (абонента или телефонный номер), просто разорвав текущее соединение и перезвонив на другой номер, такую разновидность соединений WAN называют *сетью с коммутацией каналов* (switched circuit). На рис. 22.2 показана ситуация, когда Энди и Барни соединяют свои компьютеры по телефонной линии с помощью модемов.

Когда канал установлен, два компьютера соединяются на первом уровне, следовательно, они могут передавать биты друг другу. Тем не менее двум устройствам также нужен некоторый протокол канального уровня в таком соединении для упорядоченной передачи данных, и наиболее популярной инкапсуляцией на сегодняшний день является протокол PPP. Телефонной компании не нужно проверять и интерпретировать передаваемые по каналу данные, в действительности оператору связи абсолютно все равно, что передается через сеть: голос или данные.

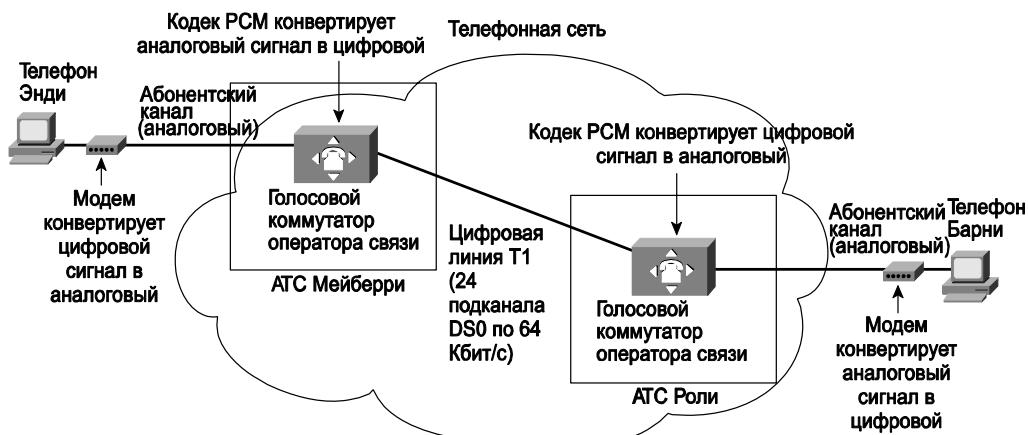


Рис. 22.2. Использование модемов для соединения компьютеров через телефонную сеть

Когда абонент использует рассматриваемую технологию WAN в качестве средства подключения к Интернету, он подключается через modem и телефонную сеть к маршрутизатору провайдера. У компьютера домашнего пользователя обычно есть *встроенный модем* (internal modem) или отдельное устройство — *внешний модем* (external modem), а у провайдера — большой блок модемов. Провайдер обычно публикует телефонный номер своего модемного блока² или указывает его в договоре, а домашний пользователь звонит с помощью модема на такой номер, чтобы через него подключиться к маршрутизатору.

Канал между двумя модемами в некотором роде работает как выделенная линия; тем не менее, два варианта подключения существенно отличаются по методам синхронизации и тактирования соединения. Модули CSU/DSU на концах выделенной линии обеспечивают синхронный режим работы канала, они не только подстраивают скорость работы под оптимальную величину для имеющейся линии, но и согласовывают ее для разных концов линии. С помощью модемов можно также установить асинхронный канал. Под асинхронностью обычно понимается ситуация, когда два модема используют одну скорость для обмена данными, но для входящих и исходящих потоков данных используются разные скорости передачи.

Основное преимущество модемов состоит в том, что такой вариант подключения доступен практически повсеместно, т.е. везде, где есть хоть какая-то телефонная линия. Стоимость модемного подключения относительно невысока, но и скорость передачи данных тоже достаточно мала на сегодняшний день. Даже если в модеме используются какие-либо технологии сжатия потока данных, битовая скорость передачи данных модемом чуть больше 100 Кбит/с. Другим существенным недостатком технологии является тот факт, что нельзя одновременно передавать данные через modem и осуществлять телефонный звонок.

Цифровая абонентская линия

Технология *цифровой абонентский канал* (digital subscriber line — DSL) была разработана во второй половине 1990-х годов для замены низкоскоростных методов

² Модемный блок чаще всего называют модемным пулом. — Примеч. ред.

дистанционного доступа WAN. Так же как и раньше, нужна была технология установки соединения с дистанционным компьютером, но все популярнее и популярнее становился Интернет, поэтому необходим был высокоскоростной доступ к нему. Долгие годы модемы использовались для дистанционного подключения, но рост популярности Интернета привел к тому, что современный человек рассматривает подключение к глобальной сети практически как коммунальную службу, например, как электричество, газ и т.п. Интернет фактически предоставляет подключение к компьютерам в любой точке мира — если есть подключение к Интернету, то можно установить логический канал с любым компьютером.

Итак, технология DSL изначально рассматривалась как средство подключения к Интернету, поэтому ее принцип работы немного отличается от модемного соединения. Фактически технология DSL предназначена прежде всего для организации высокоскоростного подключения домашнего или малого офиса к АТС. Ограничив область применения цифровой абонентской технологии определенными приложениями, разработчики технологии смогли достичь скорости передачи данных выше модемной.

Базовая служба DSL во многом похожа на модемное соединение:



Сравнение подключения DSL и модемов

- в технологии DSL аналоговые голосовые и цифровые сигналы потоков данных передаются по одному и тому же абонентскому каналу одновременно;
- абонентский канал на стороне телефонной компании должен быть подключен к чему-то, что является более современным, чем стандартный голосовой коммутатор АТС; такое устройство называют *мультиплексором доступа DSL* (DSL Access Multiplexer — DSLAM);
- в соединении DSL одновременно могут передаваться голосовой вызов и поток данных;
- в отличие от модемов, служба передачи данных в технологии DSL всегда включена; другими словами, не нужно передавать какие-либо сигналы или званиваться по определенному номеру телефона, чтобы установить канал для передачи данных.

Технология DSL дает несколько очень существенных преимуществ, в частности, можно использовать уже имеющиеся старые телефоны, за абонентом сохраняется его телефонный номер и, как только служба DSL подключена, можно в любой момент воспользоваться соединением Интернета и не нужно предпринимать каких-либо дополнительных действий для этого. На рис. 22.3 показано типичное соединение DSL.

На рисунке показано некоторое условное устройство, обозначенное как “маршрутизатор/модем DSL”, подключенное стандартным телефонным кабелем в разъем настенной телефонной розетки. Существует множество вариантов оборудования для домашнего подключения DSL: может использоваться отдельный маршрутизатор и отдельный модем DSL, оба устройства могут быть скомбинированы в одно, а также маршрутизатор, модем, коммутатор и точка беспроводного доступа могут быть объединены в одно устройство. (На рис. 19.4 и 19.4 главы 19 показано еще несколько вариантов конструкции сети и кабельная система для подключения к Интернету, в которых используются те же аппаратные компоненты.)

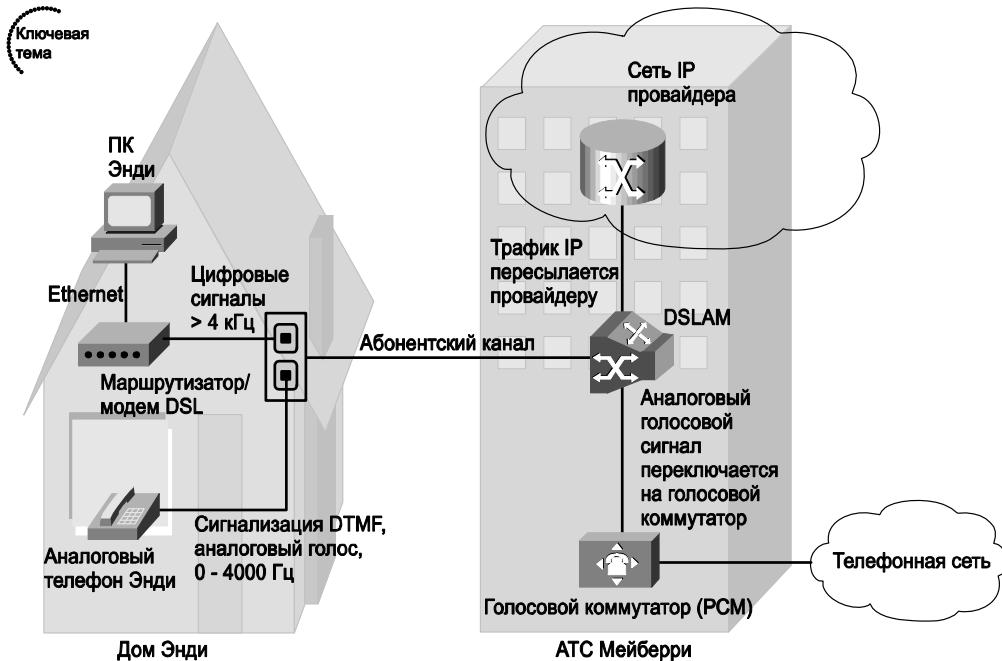


Рис. 22.3. Топология подключения DSL к провайдеру

В домашнем подключении маршрутизатор/модем DSL подключается к обычной телефонной линии (абонентскому каналу — local loop), как показано на рис. 22.3, слева. Обычные старые аналоговые телефоны также могут быть подключены к такой линии с помощью свободных разъемов многоразъемной розетки. В кабеле телефона или модема DSL используются стандартные разъемы RJ-11, которыми подключаются как обычные телефоны, так и модемы.

В технологии DSL поддерживается одновременная передача голосового звонка и потока данных, поэтому, несмотря на то, что соединение DSL с Интернетом всегда включено, параллельно можно осуществлять обычные телефонные звонки. Телефон передает аналоговый сигнал в частотном диапазоне от 0 до 4000 Гц, модем DSL использует частоты выше 4000 Гц, поэтому сигналы между собой не интерферируют. Обычно для устойчивой и качественной работы в линию нужно установить фильтр — устройство размером чуть больше спичечного коробка, которое устанавливается между телефонами, линией и модемом, чтобы предотвратить высокочастотную интерференцию от модема DSL.

Мультиплексор DSLAM местной АТС играет жизненно важную роль в передаче цифровых данных и аналогового голоса дальше. Переводя абонента с обычной голосовой службы на службу передачи голоса и услугу DSL, телефонная компания отключает кабель абонентского канала от голосового коммутатора и переключает его на мультиплексор DSLAM. Оборудование DSLAM коммутирует голосовой сигнал (с частотой от 0 до 4000 Гц) на голосовой коммутатор, а последний обрабатывает его так, как если бы телефонный вызов поступал по обычной телефонной линии. Поток данных, поступающий на мультиплексор DSLAM, устройство коммутирует на маршрутизатор провайдера, предоставляющий соответствующую услугу (см. рис. 22.3).

Схема сети, в которой показан абонентский канал, мультиплексор DSLAM и маршрутизатор провайдера услуг, предполагает бизнес-модель, в которой услуга доступа к Интернету приобретается не от местной телефонной компании, а от независимого поставщика. Местной телефонной компании принадлежит абонентский канал. Тем не менее многие провайдеры не являются одновременно и телефонными компаниями, но предоставляют услугу подключения по технологии DSL. Осуществляется обычно это таким образом, что потребитель платит ежемесячную плату за услугу DSL, а провайдер работает с местной телефонной компанией (т.е. заключает договор) и обеспечивает подключение абонентского канала к мультиплексору DSLAM (вполне возможно, что это будет мультиплексор телефонной компании). Местная телефонная компания конфигурирует свой мультиплексор таким образом, что поток данных от абонентского подключения затем передается маршрутизатору провайдера. Клиент платит провайдеру за высокоскоростное подключение DSL, а провайдер отдает часть платы местной телефонной компании за возможность использования абонентского канала.

Типы, скорость и максимальное расстояние технологии DSL

Существует несколько вариантов технологий DSL, которые работают с разными скоростями и по-разному позиционируются на рынке телекоммуникаций. Современному специалисту нужно знать несколько наиболее распространенных разновидностей и их основные характеристики.

Одна из самых ключевых характеристик, по которой все технологии DSL разделяют на два больших типа, — это принцип работы — симметричный или асимметричный. В *симметричной* (symmetric) технологии DSL скорость исходящего канала равна скорости входящего, а в *асимметричной* (asymmetric) — скорости разные. Давно было замечено, что пользователи домашнего подключения к Интернету обычно больше принимают данных, чем передают. Например, когда пользователь вводит какой-либо адрес URL в окно браузера, провайдеру отправляется несколько сотен байтов запроса на соответствующий веб-сайт, а страница, загруженная по такому запросу, может занимать сотни килобайт и даже мегабайт. В *асимметричной технологии DSL* (Asymmetric DSL — ADSL) входящий поток данных (от Интернета в домашнюю сеть) намного больше исходящего (из домашней сети в Интернет), если сравнивать ее с технологией симметричной передачи. Чтобы лучше соответствовать схеме трафика и обеспечить более широкую полосу пропускания, в соединении ADSL может использоваться 1,5 Мбит/с для исходящего канала и 384 Кбит/с — для восходящего канала передачи данных в Интернет. В табл. 22.2 перечислены наиболее распространенные разновидности технологии DSL и указано, являются ли они симметричными или асимметричными.

Таблица 22.2. Типы технологии DSL

Аббревиатура	Название	Тип
ADSL	Асимметричная технология DSL (Asymmetric DSL)	Асимметричная
CDSL (G.lite)	Пользовательская технология DSL (Consumer DSL)	Асимметричная
VDSL	Сверхвысокоскоростная технология DSL (Very-high-data-rate DSL)	Асимметричная
SDSL	Симметричная технология DSL (Symmetric DSL)	Симметричная
HDSL	Высокоскоростная технология DSL (High-data-rate DSL)	Симметричная
IDS	Технология ISDN DSL	Симметричная

Скорость линии DSL зависит от многих факторов. Спецификации большинства типов DSL улучшались несколько раз. Например, когда вы заказываете и используете линию DSL в Соединенных Штатах, вы, вероятно, используете абонентскую линию ADSL, но это может быть и линия на базе стандартов ADSL2 или ADSL2+. Вне зависимости от фактического стандарта, используемого провайдером на происходящее в реальном соединении между вами и провайдером, влияет несколько перечисленных ниже факторов.



Факторы, влияющие на скорость линии DSL

- Расстояние между АТС и абонентом (чем больше расстояние, тем меньше скорость).
- Качество кабеля абонентского канала (чем хуже кабель, тем меньше скорость).
- Тип технологии DSL (в каждом стандарте своя максимальная теоретическая скорость).
- Конкретный мультиплексор DSLAM, используемый телефонной станцией (более старое оборудование может не обеспечивать высоких скоростей передачи данных или плохо работать с не очень качественными линиями за счет отсутствия новых технологий и усовершенствований).

Например, стандарт ADSL2, последний из стандартов ADSL, заявляет максимальную теоретическую скорость передачи в 12 Мбит/с. Его преемник, стандарт ADSL2Plus, заявляет максимум в 24 Мбит/с. На самом деле на момент написания книги неофициальный отчет по наибольшим провайдерам услуг DSL в США показал типичную максимальную скорость передачи 6 Мбит/с. Независимо от реальной скорости приема и передачи, технология DSL позволяет передавать и принимать данные намного быстрее, чем обычные аналоговые модемы, поэтому она стала очень популярной на рынке высокоскоростного доступа к Интернету.

Технология DSL обычно не работает в линиях, превышающих некоторую стандартную длину, например, подключения ADSL стали популярными потому, что они могут быть организованы в абонентских каналах длиной до 18 тыс. футов (около 5,5 км, или 3 американские мили). Тем не менее, если абонент живет в сельской местности, т.е. далеко от ближайшей АТС, шансы подключиться с помощью какого-либо канала DSL к сети у него невелики.

Резюме по технологии DSL

Технологии DSL используются для организации высокоскоростного домашнего подключения к Интернету. В них одновременно можно передавать данные и голос, при этом можно использовать существующий старый абонентский канал и старые аналоговые телефоны. Служба подключения к Интернету всегда включена, т.е. канал никогда не разрывается и не нужно выполнять какую-либо процедуру вызова телефонного номера или установления соединения. К положительным моментам технологии можно отнести то, что скорость службы DSL не уменьшается при подключении большего количества пользователей к сети.

У технологии DSL, тем не менее, есть вполне очевидные недостатки. Такой вариант подключения может быть недоступен некоторым абонентам, особенно в сель-

ской и малонаселенной местности, особенно в том случае, если расстояние до АТС велико. У местной телефонной компании также должно быть установлено оборудование DSL, чтобы появилась возможность предоставлять услугу высокоскоростного подключения через какого-либо провайдера либо средствами компании. Скорость работы с ресурсами, доступными непосредственно в сети телефонной компании или провайдера услуги, может быть выше, чем с другими веб-сайтами и сетями.

Кабельное подключение к Интернету

Среди всех рассматриваемых в данной главе технологий подключение к Интернету через оператора кабельного телевидения — единственное, не требующее телефонной линии от местного оператора связи в качестве физического канала. Сегодня практически в каждом городском доме есть *кабельное телевидение* (cable TV — CATV), которым обычно заменяют коллективные антенны эфирного вещания. Кабельные модемы предоставляют услугу *постоянного доступа* (always on) к Интернету, при этом одновременно можно бродить просторы сети, смотреть телевизор и разговаривать по телефону по обычной телефонной линии!

ВНИМАНИЕ!

Многие кабельные компании предлагают цифровые голосовые услуги и конкурируют с местными операторами фиксированной телефонной связи. Голосовой трафик при этом также передается через кабель оператора кабельного телевидения.

Кабельные модемы и маршрутизаторы, которые представляют собой обычные маршрутизаторы с интегрированными в них модемами (аналогично технологии DSL), используют некоторую сигнальную емкость кабеля, которая могла бы быть использована для передачи большего количества телевизионных каналов. Фактически же для передачи данных используются определенные частоты вместо новых телевизионных каналов. Иногда в шутку говорят, что подписчик такой услуги получает новый телевизионный канал с названием “Интернет” наряду с каналами CNN, MTV, The Cartoon Network и HTB+.

Чтобы понять, как работают кабельные модемы, нужно сначала обратиться к основам и терминологии кабельного телевидения. Традиционно услуга, предоставляемая оператором кабельного телевидения, односторонняя — кабельная компания передает электрический сигнал телевизионных каналов абонентам. После установки и подключения телевизора все, что нужно сделать, — выбрать, какой канал смотреть. Если пользователь услуги смотрит, например, канал MTV, сигнал телеканала CNN все равно передается по кабелю и доходит до телевизионного приемника, но последний просто игнорирует такие сигналы. Если в квартире есть два телевизора, то можно одновременно смотреть разные каналы на разных телевизорах, поскольку сигнал обоих каналов все равно присутствует в кабеле.

В кабельном телевидении есть собственная терминология, точно так же, как и в любой другой технологии доступа, рассматриваемой в данной главе. На рис. 22.4 приведены некоторые ключевые термины кабельных сетей.

К кабельному модему или маршрутизатору подключен кабель телевидения, который на рисунке показан пунктирной линией. В среднестатистической квартире или частном доме обычно установлено несколько настенных розеток, а кабельный модем или маршрутизатор может быть подключен к одной из них. Точно так же как и в технологии DSL, такой маршрутизатор или модем подключен к компьютеру кабелем Ethernet.

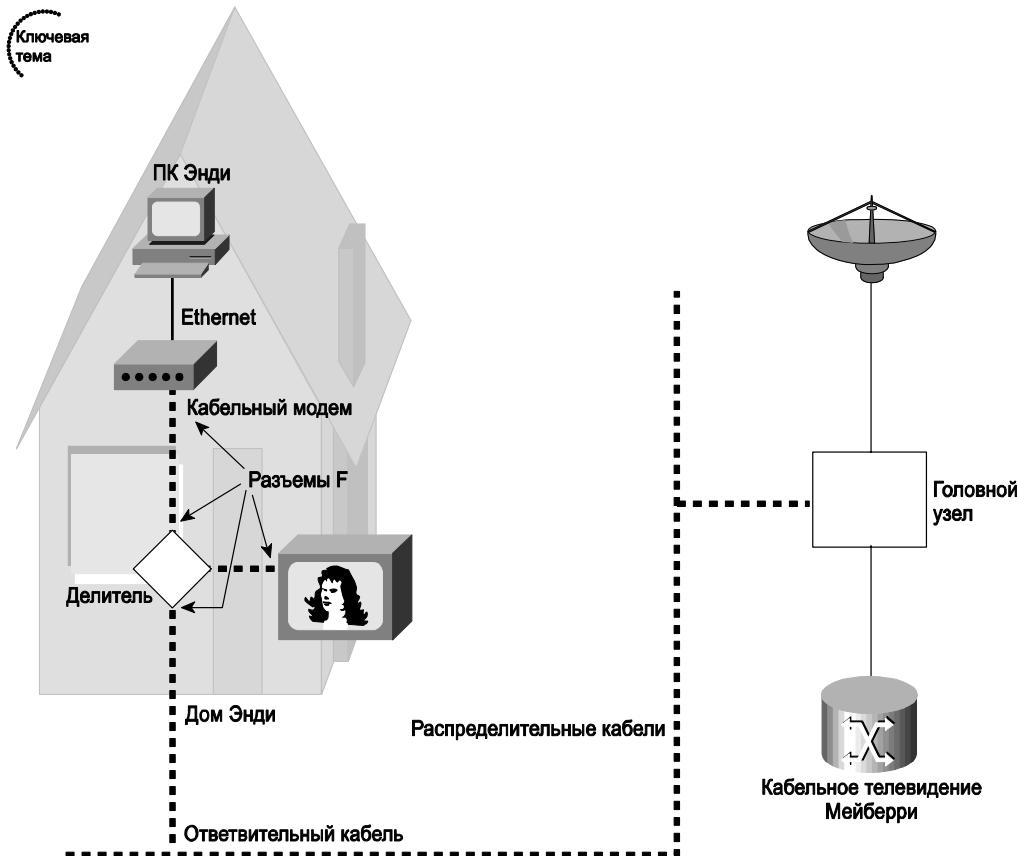


Рис. 22.4. Терминология и топология кабельной сети

Другой конец кабеля подключен к оборудованию в узле компании-поставщика кабельных услуг, который называют *головным узлом* (head-end). Оборудование головного узла перенаправляет канал, используемый для доступа к Интернету, на маршрутизатор провайдера, точно так же, как мультиплексор DSLAM разделяет канал передачи данных и голоса для абонентского канала местной телефонной компании. То же самое оборудование отвечает за прием телевизионных сигналов, обычно через спутниковую антенну, и передачу телеканалов абонентам.

Кабельное подключение к Интернету фактически очень сильно напоминает подключение через технологию DSL. Но как можно догадаться, между ними есть некоторые отличия. Кабельное подключение к Интернету работает быстрее, чем подключение DSL. Скорости кабельного подключения варьируются от сопоставимых со скоростями DSL до предоставляемых многими провайдерами скоростей в 15 и даже в 50 Мбит/с. Как обычно, это могут быть разные устройства или одно комбинированное.

Тем не менее в двух вариантах подключения к сети есть некоторые, вполне очевидные, отличия. Подключение к Интернету через оператора кабельного телевидения работает на более высокой скорости, чем канал DSL, а типичные скорости в 2–5 раз больше, чем указанная выше скорость в 1,5 Мбит/с для технологии DSL. Скорость кабельного

соединения не уменьшается с удалением от регионального узла (т.е. в зависимости от длины абонентского кабеля). Но у кабельного подключения есть существенный недостаток, скорость работы такого канала доступа к сети уменьшается при увеличении трафика, пересылаемого другими пользователями, поскольку кабель в такой системе является разделяемым ресурсом в рамках какого-либо участка кабельной системы, в то время как в технологии DSL нет такой проблемы. Проблему загруженности какого-либо сегмента потоками данных могут решить инженеры оператора кабельной сети и увеличить эффективную полосу пропускания канала для пользователей.

ВНИМАНИЕ!

Точно измерить скорости каналов DSL и кабельных подключений в числах довольно трудно, однако вполне возможно, если воспользоваться некоторыми инструментами проверки соединения. Лично мне нравится измеритель скорости подключения от CNET (<http://reviews.cnet.com/internet-speed-test/>).

Сравнение технологий дистанционного доступа

В этой главе описаны базовые принципы работы обычных и кабельных модемов, а также технологии DSL. Пользователи выбирают, каким вариантом подключения воспользоваться, в зависимости от того, какая именно услуга предоставляется в данном регионе или районе города. Следовательно, сетевые инженеры должны иметь представление обо всех вариантах, поскольку придется сталкиваться со всеми технологиями. В табл. 22.3 перечислены основные характеристики трех основных вариантов подключения к Интернету.

Таблица 22.3. Сравнение модемов, технологии DSL и кабельных модемов



	Аналоговые модемы	DSL	Кабельные модемы
Транспортная среда	Абонентский канал местной телефонной компании	Абонентский канал местной телефонной компании	Кабельная сеть оператора кабельного телевидения
Поддерживает симметричный режим	Да	Да	Нет
Поддерживает асимметричный режим	Да	Да	Да
Типичные скорости работы	До 100 Кбит/с	Нисходящий поток до 6 Мбит/с	Нисходящий поток до 15–20 Мбит/с
Возможна одновременная передача голосового вызова и потока данных	Нет	Да	Да
Доступ к Интернету всегда возможен	Нет	Да	Да
Есть проблемы при большой длине абонентского канала	Нет	Да	Нет
Пропускная способность падает при увеличении числа пользователей услуги	Нет	Нет	Да

Технология ATM

Все перечисленные выше технологии WAN предназначены прежде всего для доступа к Интернету из малого или домашнего офиса. Технология *асинхронной передачи данных* (Asynchronous Transfer Mode — ATM) предназначена для организации магистральных каналов, которые работают по принципу службы с коммутацией пакетов, например, похоже на технологию Frame Relay, или для построения крупных коммутируемых сетей, например, операторов связи и телефонных компаний. В текущем разделе описаны детали технологии ATM с точки зрения службы с коммутацией пакетов.

Чтобы использовать технологию ATM, маршрутизаторы должны быть подключены каналом доступа к коммутатору ATM в сети провайдера услуги; обычно топология сети клиента выглядит аналогично используемой в среде Frame Relay. Если в сети компании есть несколько узлов, то маршрутизатор каждого из них должен быть подключен к среде ATM *виртуальным каналом* (Virtual Circuit — VC), с помощью которого создаются логические каналы между филиалами и центральным офисом компании. В технологии ATM могут использоваться *постоянные виртуальные каналы* (Permanent VC — PVC), аналогичные тем, которые устанавливаются в сети Frame Relay.

Вполне очевидно, что между технологиями ATM и Frame Relay есть существенные различия, но обе выполняют фактически одну и ту же функцию, поэтому нет необходимости использовать обе технологии одновременно. Прежде всего следует отметить, что для сети ATM характерны намного большие скорости в каналах на физическом уровне, в частности, в тех, где используется технология *синхронной оптической сети* (Synchronous Optical Network — SONET³). Второе существенное отличие — в сети ATM передаются не фреймы, а ячейки (cell). Ячейка, как и фрейм, представляет собой некоторый последовательный набор битов, передаваемый по сетевой среде. Ее отличие от фреймов состоит в том, что фреймы могут быть разного размера, а ячейки ATM имеют фиксированную длину — 53 байта.

Ячейка ATM состоит из 48 байтов полезной нагрузки (данных) и 5-байтового заголовка. В заголовке есть два поля, которые выполняют ту же функцию, что и идентификатор DLCI в технологии Frame Relay, — идентифицируют конкретный виртуальный канал (VC). Эти два поля называются *идентификатором виртуального маршрута* (Virtual Path Identifier — VPI) и *идентификатором виртуального канала* (Virtual Channel Identifier — VCI). Точно так же как коммутаторы Frame Relay пересыпают фреймы согласно идентификатору DLCI в заголовке, коммутаторы ATM, размещенные в сети провайдера, пересыпают ячейки по нужному маршруту согласно значению пары идентификаторов VPI/VCI.

Пользователи обычно подключены к сети какими-либо каналами Ethernet, а устройства Ethernet не создают ячеек. Следовательно, чтобы преобразовать фреймы Ethernet в ячейки ATM, нужно использовать некоторый маршрутизатор, который одновременно будет работать как с технологиями локальной, так и распределенной сети. Когда такой маршрутизатор принимает пакет из локальной сети, он декодирует фрейм, в который инкапсулирован пакет, принимает решение об отправке пакета в сеть ATM, а после разбивает пакет на маленькие блоки фиксированной длины — 48-байтовые сегменты. К каждому сегменту добавляется 5-байтовый заголовок, и получившаяся ячейка передается в сеть. На рис. 22.5 проиллюстрирован описанный процесс, выполняемый маршрутизатором R2.

³ Стандарт Bellcore, определяющий скорости, сигналы и интерфейсы для синхронной передачи данных по оптоволоконному кабелю. — Примеч. ред.

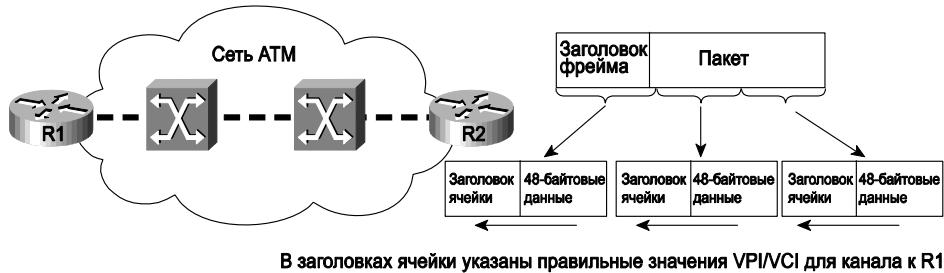


Рис. 22.5. Сегментация и повторная сборка пакета в сети ATM

Маршрутизатор R1 выполняет обратный процесс: получая ячейки, он отбрасывает от них заголовки и собирает целый пакет; такой процесс называют *повторной сборкой* пакета (reassembly). Весь процесс полностью, т.е. сегментация пакета на фиксированные блоки и повторная сборка пакета из ячейки, называется *сегментацией и повторной сборкой* (Segmentation And Reassembly — SAR). В маршрутизаторах компании Cisco для подключения к сети ATM используются специализированные интерфейсы. В таких портах ATM есть специализированные микросхемы для выполнения функции SAR на аппаратном уровне и специализированное аппаратное обеспечение для поддержки каналов SONET.

Сравнение технологии коммутации пакетов и каналов

Большинство технологий WAN по принципу их работы можно отнести к одному из двух классов: службы с *коммутацией каналов* (circuit-switching) и службы с *коммутацией пакетов* (packet-switching). С точки зрения традиционной телефонной терминологии *канал* (circuit) — это некоторая возможность на физическом уровне передать голос или данные через сеть поставщика услуги. Сам термин появился давно и связан с принципом работы старых телефонных станций, когда, для того, чтобы осуществить звонок какому-либо абоненту, нужно было создать замкнутую электрическую цепь между двумя абонентами, т.е. некоторый физический выделенный канал из двух проводников. С такой точки зрения к физическим каналам относятся выделенные линии, которые были описаны в главе 4, поскольку в них используется физическая двухканальная или четырехпроводная линия.

Коммутация пакетов подразумевает, что устройства WAN делают нечто большее, чем просто передают биты или электрический сигнал по физической среде передачи данных от одного устройства к другому. В технологии коммутации пакетов сетевое оборудование провайдера интерпретирует биты, пересылаемые оборудованием пользователя, и обнаруживает в них так называемое адресное поле в заголовке фрейма второго уровня. После этого служба коммутации принимает решение, куда нужно коммутировать соответствующую группу битов — фрейм. В табл. 22.4 описаны ключевые отличия описанных двух технологий сети WAN.

Таблица 22.4. Сравнение коммутации каналов и пакетов

Ключевая тема

Характеристика	Коммутация каналов	Коммутация пакетов
На каком уровне OSI реализуется	1	2
Используется двухточечный (два устройства) или многоточечный канал	Двухточечный	Многоточечный (т.е. больше двух устройств)

Технология Ethernet в качестве среды WAN

Перед тем как приступить к рассмотрению некоторых проблем с доступом к Интернету, следует кратко затронуть одно полезное усовершенствование, которое появилось относительно недавно в сетях WAN: технология Ethernet в качестве среды WAN, или *городские сети Ethernet* (Metropolitan Ethernet — Metro E). В технологии Metro E провайдер предоставляет подключение Ethernet для клиента, причем зачастую используется оптоволоконный кабель, с помощью которого можно создать канал большей протяженности. Потребитель услуги подключает такой кабель к коммутатору или маршрутизатору своей локальной сети.

Провайдер может предоставить клиенту подключение через интерфейс FastEthernet или GigabitEthernet, но, точно так же, как и в технологии Frame Relay, оговорить некоторую гарантированную скорость передачи данных, которая меньше пропускной способности интерфейса. Например, клиенту необходимо только 20 Мбит/с от общей полосы пропускания для соединения своих офисов и филиалов или центров обработки данных в разных районах города. Провайдер подключает такого клиента через порт FastEthernet и заключает договор с клиентом на предоставление скорости в 20 Мбит/с. Клиент конфигурирует свои маршрутизаторы таким образом, чтобы они не передавали данные со скоростью, выше, чем оговоренная в контракте, с помощью технологии, называемой *ограничением скорости* (shaping). В такой конфигурации потребитель получает нужную полосу пропускания, обычно по цене более низкой, чем аналогичная телекоммуникационная линия (T3 или E3).

Существует множество схем построения сетей на технологии Metro E: начиная от простейшего подключения одного клиента одним каналом доступа к узлу провайдера услуги и кончая объединением нескольких филиалов компании через сеть провайдера с использованием нескольких сетей VLAN в одном канале доступа. Тонкости и детали этой технологии выходят за рамки курса CCNA, тем не менее, это очень интересный и быстро развивающийся метод построения сетей, завоеваывающий все большую популярность на рынке телекоммуникаций.

В следующем разделе будут подробно описаны несколько важных функций, которые понадобятся в типичном подключении к Интернету с помощью кабеля или модема DSL.

Службы IP для доступа к Интернету

Кабельные технологии и технологии DSL доступа к Интернету имеют много общего. В частности, в обоих методах нужен маршрутизатор, который отвечает за пересылку пакетов от компьютеров в домашней или офисной сети через соответствующий канал провайдеру услуги и осуществляет прием и перенаправление ответных пакетов. Во второй части данной главы будут достаточно подробно описаны несколько функций IP, выполняемых кабельным маршрутизатором или маршрутизатором DSL, например, пара вариантов использования службы DHCP, а также функция *трансляции сетевых адресов* (Network Address Translation — NAT).

Оборудование, используемое в сети SOHO для подключения к Интернету по кабелю или DSL, может представлять собой как одно интегрированное устройство, так и несколько отдельных устройств (см. рис. 13.4 и 13.5 в главе 13). Чтобы упростить описание нужных технологий IP, в данной главе будут рассматриваться отдельные устройства, например, как в схеме сети, показанной на рис. 22.6.

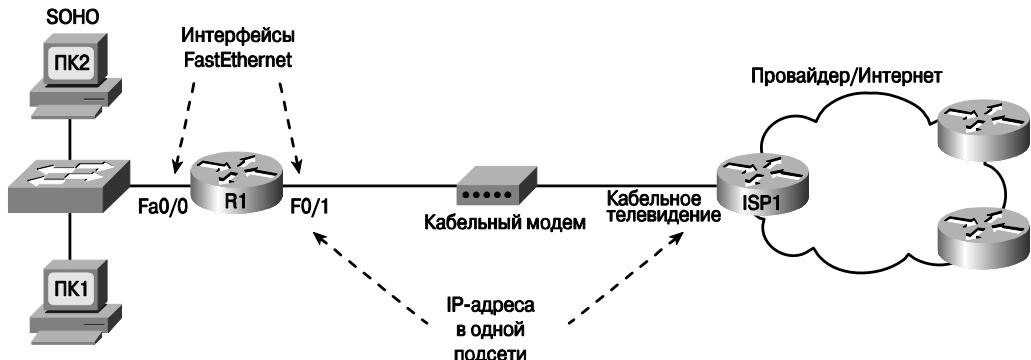


Рис. 22.6. Схема подключения оборудования для доступа к Интернету: отдельные устройства

Если рассматривать поток данных слева направо на схеме, то можно заметить, что компьютер пересыпает свои пакеты стандартному шлюзу, в данном случае — местному маршрутизатору доступа. Коммутатор локальной сети просто пересыпает фреймы маршрутизатору, последний принимает решение о том, что пакет, в свою очередь, нужно перенаправить маршрутизатору провайдера, который выступает в роли следующего транзитного узла на пути следования пакета. Кабельный modem конвертирует фрейм Ethernet, полученный от маршрутизатора, в формат, соответствующий кабельной сети (формат фрейма в кабельной сети выходит за рамки рассмотрения данной книги). В конце концов, в таблице маршрутизации провайдера есть все маршруты Интернета, поэтому он может отправить такой пакет нужному получателю.

Из трех представленных на схеме сети устройств малого офиса только маршрутизатор будет описан более подробно. Кроме стандартной маршрутизации, такое устройство дополнительно выполняет три важные функции, которые описаны ниже: присвоение адресов, обнаружение маршрутов и трансляция адресов (NAT).

Присвоение адресов с помощью маршрутизатора доступа к Интернету

У маршрутизатора доступа к Интернету, показанного на рис. 22.6, есть два интерфейса LAN: один подключен к модему и осуществляет связь с Интернетом, другой — к локальной сети. Как было описано в части III, чтобы устройство могло маршрутизировать пакеты между двумя интерфейсами, на обоих должны быть установлены IP-адреса. Тем не менее вместо выбора и установки адресов вручную с помощью команды конфигурирования интерфейса `ip address` IP-адреса выбираются согласно правилам, перечисленным ниже.

Факторы, влияющие на IP-адресацию маршрутизаторов доступа к Интернету

Ключевая тема

- На интерфейсе маршрутизатора, подключенном к Интернету, необходимо установить зарегистрированный IP-адрес, чтобы маршрутизаторы в глобальной сети знали, куда отправлять соответствующие пакеты.
- Провайдер услуги обычно назначает такой открытый (и глобально маршрутизуемый) IP-адрес с помощью службы DHCP.

- Локальным компьютерам обычно нужно динамически получать свои IP-адреса с помощью службы DHCP, следовательно, маршрутизатор доступа будет выступать в качестве сервера DHCP для локальных хостов.
- У маршрутизатора должен быть статически задан адрес для интерфейса локальной сети, причем такой адрес обычно берется из какой-либо частной сети.
- В локальной сети чаще всего используется адресация из какого-либо диапазона частных сетей.

ВНИМАНИЕ!

В главе 12 подробно описаны зарегистрированные и частные блоки адресов, а также указаны диапазоны, используемые для частных сетей.

На рис. 22.7 показана логическая схема работы службы DHCP при домашнем подключении к Интернету; детали кабельной системы опущены.

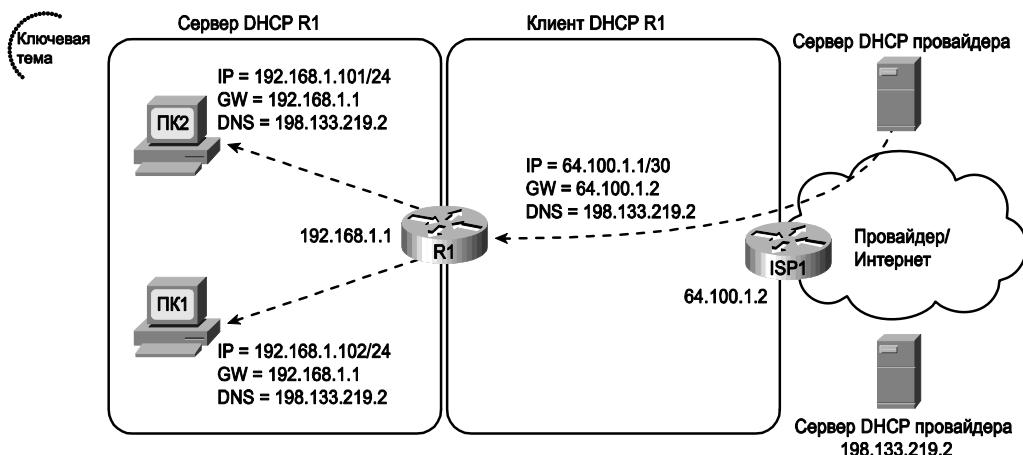


Рис. 22.7. Функции клиента и сервера DHCP в маршрутизаторе доступа к Интернету

В схеме сети, показанной на рис. 22.7, у маршрутизатора доступа (R1) на интерфейсе локальной сети статически установлен IP-адрес и включена функция сервера DHCP на том же самом порту. На интерфейсе, подключенном к Интернету, включена функция клиента DHCP. Маршрутизатор R1 получает IP-адрес интерфейса Интернета от провайдера услуг, в данном случае 64.100.1.1. После того как адрес 192.168.1.1/24 установлен на интерфейсе локальной сети маршрутизатора R1, устройство начинает отвечать на запросы DHCP и присваивать IP-адреса из той же подсети, которая указана на его интерфейсе, компьютерам в локальной сети: ПК1 и ПК2. Обратите внимание на то, что в сообщениях DHCP от маршрутизатора R1 указан IP-адрес сервера DNS (198.133.219.2), который был получен от сервера DHCP провайдера.

Маршрутизация в устройстве доступа к Интернету

Маршрутизатор R1 в рассматриваемой схеме подключения к сети должен маршрутизировать пакеты между Интернетом и локальной сетью. В данной схеме у устройства

есть две напрямую подключенные к нему сети, как обычно. Тем не менее, вместо того, чтобы обнаружить все маршруты Интернета с помощью какого-либо протокола маршрутизации, в маршрутизаторе R1 может быть задан статический *стандартный маршрут* (default route), поскольку у маршрутизатора доступа есть всего один возможный физический канал и физический маршрут к Интернету, а именно — соединение с маршрутизатором провайдера.

Вместо конфигурирования статического маршрута маршрутизатор доступа может получать нужный маршрут через службу DHCP. Например, как показано на рис. 22.7, маршрутизатор R1 получил IP-адрес стандартного шлюза 64.100.1.2, установленный на интерфейсе провайдера (маршрутизатор ISP1), к которому подключено соединение DSL. Маршрутизатор доступа создает стандартный маршрут в такой ситуации и использует *стандартный шлюз* (default gateway) в качестве *следующего транзитного перехода* (next-hop) на маршруте. На рис. 22.8 стрелками показан такой стандартный маршрут и несколько других важных маршрутов.

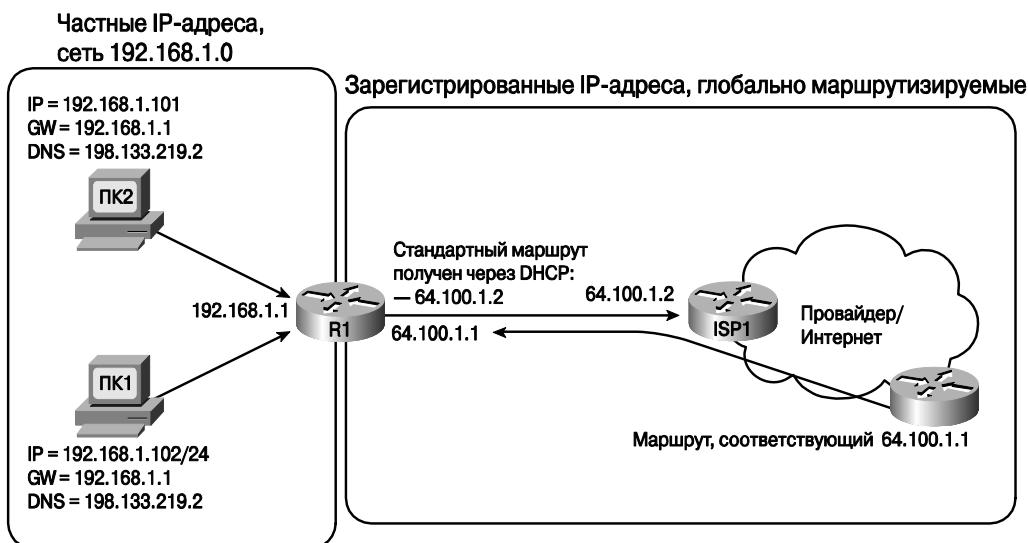


Рис. 22.8. Маршрутизация в устройстве доступа к сети

Указанные настройки стандартного шлюза для компьютеров в локальной сети, вместе со стандартным маршрутом (устройства R1), позволяют рабочим станциям пересыпалать пакеты в Интернет. Маршрутизаторы в Интернете, соответственно, будут маршрутизировать пакеты куда угодно. Тем не менее, пока схема маршрутизации еще не полная, поскольку нужно определиться, куда указывают обратные маршруты из Интернета: в сеть домашнего или малого офиса. IP-адрес интерфейса маршрутизатора R1, подключенный к Интернету, является зарегистрированным открытым адресом (64.100.1.1 на рис. 22.8). Следовательно, все маршрутизаторы в Интернете смогут получить маршрут к нему и переслать пакеты. Маршрутизаторы глобальной сети, тем не менее, никогда не будут владеть информацией о маршрутах к частным адресам, например, к сети 192.168.1.0/24, показанной на рис. 22.8, так как частные адреса предназначены для нумерации в частной сети и не маршрутизируются.

Решение последней проблемы не связано с маршрутизацией, а основывается на отдельной технологии, которая позволяет использовать в локальной сети частные IP-адреса и подключаться к Интернету через какое-то граничное устройство (маршрутизатор R1): технологии NAT и PAT. Хосты в открытом глобальном Интернете пересыпают пакеты открытому зарегистрированному адресу маршрутизатора R1 (64.100.1.1 на рис. 22.8), а маршрутизатор доступа транслирует адреса в таких пакетах, чтобы они соответствовали IP-адресам хостов в локальной сети.

Технологии NAT и PAT

Перед тем как приступить к рассмотрению того, как технология *трансляции сетевых адресов* (Network Address Translation — NAT) и технология *трансляции адресов с использованием портов* (Port Address Translation — PAT) решают проблему доставки возвратных пакетов, обратимся к некоторым вопросам, связанным с оптимальным использованием адресного пространства и его экономией, а также с использованием портов в протоколах TCP и UDP.

Ассоциация по присвоению имен и номеров портов Интернета (Internet Corporation for Assigned Names and Numbers — ICANN) управляет процессом распределения и присвоения открытых IP-адресов в глобальном адресном пространстве IPv4. Следует отметить, что доступные адреса постепенно заканчиваются. Поэтому провайдер, осуществляя кабельное подключение или подключение DSL, старается назначить клиенту как можно меньше открытых зарегистрированных адресов. Кроме того, провайдеры также предпочтитают присваивать адреса динамически, чтобы быстро и легко менять адресацию и выдать адрес другому клиенту в том случае, если он решит подключиться к другому поставщику услуг. Следовательно, в типичном кабельном или соединении DSL с Интернетом провайдер выделяет клиенту один зарегистрированный маршрутизуемый IP-адрес и чаще всего присваивает такой адрес с помощью сервера DHCP, как было показано на рис. 22.7. Провайдер обычно не выделяет несколько публичных зарегистрированных адресов одному клиенту, чтобы последний мог адресовать несколько компьютеров (например, ПК1 и ПК2 на рис. 22.7), поскольку стремится сэкономить свое адресное пространство.

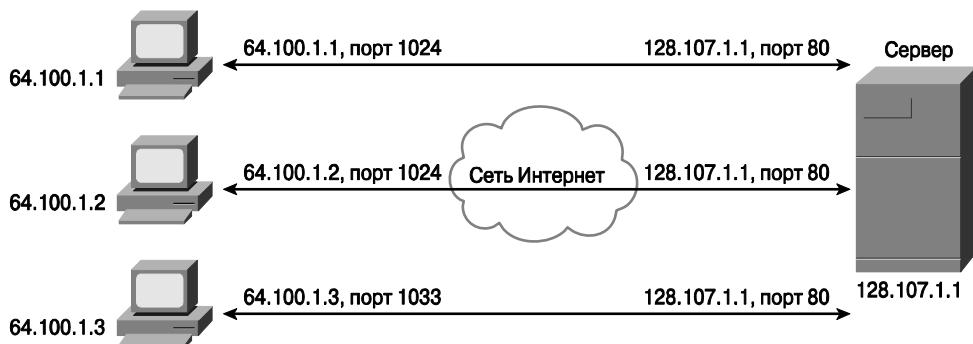
Еще один вопрос, который мы рассмотрим, связан с принципом работы протокола TCP, а именно, как отличаются с точки зрения сервера несколько соединений TCP от одного хоста к серверу и от нескольких хостов. На рис. 22.9 приведен пример, который поможет разобраться в логике работы службы PAT.

В верхней части рисунка показана сеть, в которой три разных хоста устанавливают соединение с веб-сервером, используя протокол TCP. В нижней части показана та же сеть, но все соединения TCP устанавливаются одним хостом. Все шесть соединений устанавливаются с IP-адресом (128.107.1.1) и стандартным портом веб-службы 80. В обоих рассмотренных случаях сервер может различить разные соединения, поскольку у каждого из них уникальна комбинация IP-адреса и номера порта.

Итак, помня о том, что нужно сэкономить IP-адрес и концепцию использования портов, рассмотрим, как технология PAT позволяет локальным хостам использовать частные IP-адреса и установить один зарегистрированный адрес на маршрутизатор доступа. В технологии преобразования адресов PAT используется

особенность работы протокола TCP: с точки зрения сервера абсолютно все равно, осуществляются соединения с тремя разными хостами с разными адресами или соединения устанавливаются с одним хостом на один IP-адрес, но с разными портами. Следовательно, чтобы подключить к Интернету множество хостов небольшого или домашнего офиса с помощью одного только зарегистрированного публичного IP-адреса, служба РАТ транслирует частные адреса локальных хостов в один имеющийся зарегистрированный. Чтобы правильно пересыпать пакеты обратной коммуникации локальным хостам, маршрутизатор хранит у себя таблицу IP-адресов и номеров портов для протоколов TCP и UDP. На рис. 22.10 показан принцип работы рассматриваемой технологии на примере, в котором используется схема сети, представленная на рис. 22.7.

Три соединения от трех ПК



Три соединения от одного ПК

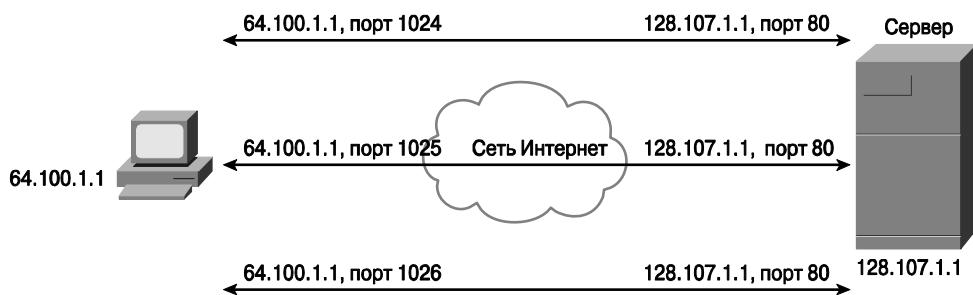


Рис. 22.9. Три соединения TCP от трех разных хостов и от одного хоста

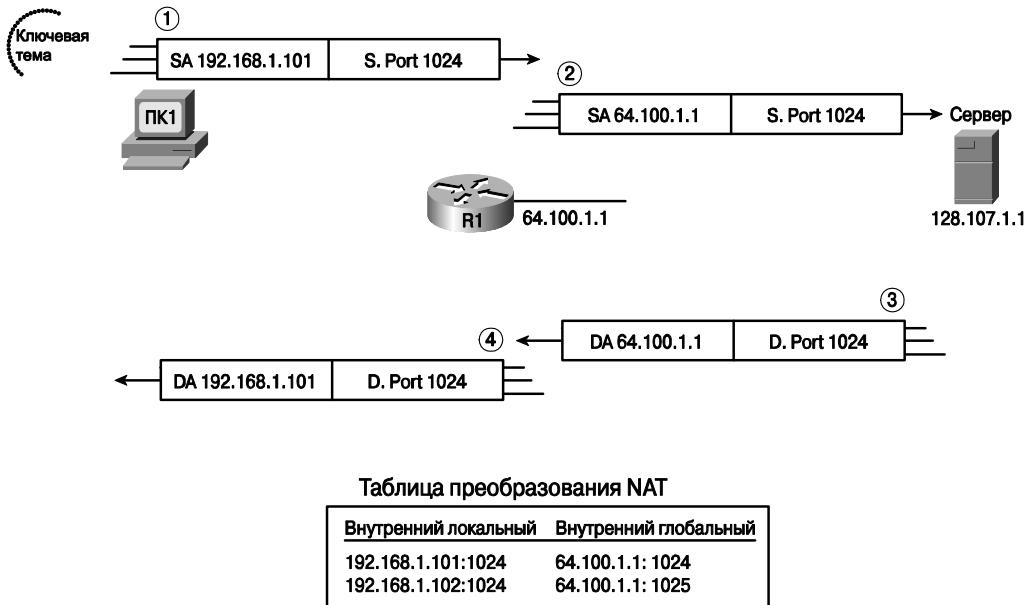


Рис 22.10. Служба PAT маршрутизатора доступа к Интернету

На рис. 22.10 показан пакет, отправленный компьютером ПК1 серверу в Интернете. В верхней части рисунка (этапы 1 и 2) показаны IP-адрес и порт отправителя для такого пакета до того, как устройство R1 выполнит трансляцию с помощью службы PAT. В нижней части (этапы 3 и 4) показан возвратный пакет от сервера, в котором IP-адрес и порт получателя указаны до того, как отработает служба PAT. (Сервер не знает, какие технологии используются в маршрутизаторе доступа, он просто отвечает хосту с теми характеристиками, которые получил в предыдущем пакете.) Этапы, показанные на рис. 22.10, относятся к алгоритму работы службы трансляции адресов, который описан ниже.

- Хост ПК1 передает пакет серверу с IP-адресом 128.107.1.1 и, чтобы доставить его, осуществляет пересылку согласно настройкам своего стандартного шлюза, т.е. передает пакет маршрутизатору R1.
- Маршрутизатор R1 выполняет преобразование PAT согласно таблице трансляций и заменяет IP-адрес локального хоста с частного (используемого в локальной сети) на открытый зарегистрированный (глобально маршрутизуемый), а именно 64.100.1.1 в рассматриваемом примере. Маршрутизатор R1 пересыпает пакет согласно *стандартному маршруту* (default route) в таблице маршрутизации.
- Когда сервер отвечает на пакет, присланный компьютером ПК1, он пересыпает ответный пакет адресу получателя 64.100.1.1 на порт 1024, так как эти значения указаны в полях отправителя входящего пакета на этапе 2. Маршрутизаторы Интернета знают маршрут к такому адресу (устройству R1), поскольку такой получатель представляет собой глобально маршрутизуемый открытый IP-адрес.

4. Маршрутизатор R1 заменяет IP-адрес получателя и порт согласно таблице трансляции PAT, подставляя вместо пары “адрес–порт” 64.100.1.1/1024 значения 192.168.1.101/1024. Устройство знает маршрут к адресу 192.168.1.101, поскольку он принадлежит к подключенной подсети.

Если сформулировать алгоритм работы более общими словами, то можно сказать, что служба PAT в маршрутизации заменяет IP-адрес и порт отправителя для пакетов, покидающих локальную сеть, и заменяет адрес и порт получателя для пакетов, входящих в локальную сеть. С точки зрения всех маршрутизаторов в Интернете все пакеты приходят с одного адреса (или от одного хоста — 64.100.1.1 на рис. 22.10), а у них есть маршрут на такой адрес. Такой подход позволяет провайдеру существенно сэкономить зарегистрированные открытые адреса IPv4.

Термины *внутренний локальный* (inside local) и *внутренний глобальный* (inside global), указанные в таблице трансляции на рис. 22.10, имеют некоторое специфическое значение в технологии трансляции сетевых адресов. Их понимание пригодится больше сетевому инженеру какой-либо компании, чем сетевому администратору провайдера.

Определения ключевых терминов технологии NAT



- *Внутренний хост* (inside host). Хост с частным глобально немаршрутизуемым адресом в корпоративной сети (например, хосты ПК1 и ПК2).
- *Внутренний локальный адрес* (inside local). IP-адрес в заголовке, относящийся к внутреннему хосту, используемый при передаче пакета в локальной сети, но не в Интернете. В рассматриваемом примере адреса 192.168.1.101 и .102 являются внутренними локальными IP-адресами (см. этапы 1 и 4 на рис. 22.10).
- *Внутренний глобальный адрес* (inside global). IP-адрес в заголовке, который получают пакеты внутреннего хоста при передаче по Интернету, вне локальной сети. В рассматриваемом примере адрес 64.100.1.1 является внутренним глобальным и показан на этапах 2 и 3 рис. 22.10.
- *Внутренний интерфейс* (inside interface). Интерфейс маршрутизатора, подключенный к локальной сети, в которой размещены внутренние хосты.
- *Внешний интерфейс* (outside interface). Интерфейс маршрутизатора, подключенный к Интернету.

Итак, после того как мы разобрались в принципе работы технологии PAT, можно дать более точные определения терминам, используемым в службах NAT и PAT. Если нужно дать наиболее четкие определения и представить формальное описание технологии, то можно сказать, что служба трансляции сетевых адресов (NAT) выполняет преобразование адресов сетевого уровня (IP) без замены портов в сессиях. Служба трансляции сетевых адресов с использованием портов (PAT) выполняет преобразование адресной информации как на сетевом, так и на транспортном уровне (заменяет номера портов для протоколов TCP и UDP). С точки зрения более общего подхода технология PAT является частным случаем технологии NAT и фактически представляет собой другой метод конфигурирования службы NAT. Обычно специалисты используют более широкое определение, и, например, когда инженер говорит: “Мы используем службу трансляции адресов для подключения к Интернету

через нашего провайдера”, то в такой сети может использоваться как технология NAT, так и PAT.

В завершение следует отметить, что если вы уже устанавливали, например, в своей домашней сети кабельный маршрутизатор или устройство DSL, то заставить его заработать вам было намного проще, чем автору описать, а читателю понять принцип работы технологий в такой схеме сети. Если клиент покупает кабельный маршрутизатор или маршрутизатор DSL потребительского класса, устройство уже обычно настроено как сервер DHCP, клиент DHCP и в нем запущена служба PAT. (В таком устройстве, особенно если это интегрированный вариант, есть порт, обозначенный как “Internet”. Обычно он работает как клиент DHCP и именно он подключается к открытой глобальной сети.) Следовательно, все описанные функции работают в устройстве, но без какого-либо постороннего вмешательства. Тем не менее, если в сети устанавливается маршрутизатор корпоративного уровня компании Cisco, устройство нужно настроить так, чтобы оно выполняло необходимые действия. В следующей главе описано, как настроить обсуждавшиеся выше службы и проверить их работоспособность.

Подготовка к экзамену

Повторите все ключевые темы

Повторите все ключевые темы данной главы, помеченные пиктограммой “Ключевая тема”. Ключевые темы и соответствующие им страницы перечислены в табл. 22.5.

Таблица 22.5. Ключевые темы главы 22

Элемент	Описание	Страница
Список	Сравнение подключения DSL и модемов	603
Рис. 22.3	Топология подключения DSL к провайдеру	604
Список	Факторы, влияющие на скорость линии DSL	606
Рис. 22.4	Терминология и топология кабельной сети	608
Табл. 22.3	Сравнение модемов, технологии DSL и кабельных модемов	609
Табл. 22.4	Сравнение коммутации каналов и пакетов	611
Список	Факторы, влияющие на IP-адресацию маршрутизаторов доступа к Интернету	613
Рис. 22.7	Функции клиента и сервера DHCP в маршрутизаторе доступа к Интернету	614
Рис. 22.10	Служба PAT маршрутизатора доступа к Интернету	618
Список	Определения ключевых терминов технологии NAT	619

Заполните таблицы и списки по памяти

Распечатайте приложение М (Appendix L) с компакт-диска или его раздел, относящийся к этой главе, и заполните таблицы и списки по памяти. В приложении Н (Appendix M) приведены заполненные таблицы и списки для самоконтроля.

Ключевые термины

Дайте определения перечисленных ниже терминов и проверьте правильность их написания в списке терминов:

технология ADSL (ADSL), асимметричный канал (asymmetric), технология ATM (ATM), технология DSL (DSL), внутренний глобальный адрес (inside global), внутренний локальный адрес (inside local), модем (modem), служба NAT (NAT), служба PAT (PAT), открытая коммутируемая телефонная сеть (Public Switched Telephone Network — PSTN), симметричный канал (symmetric), телефонная компания (telco).

В этой главе...

- **Конфигурирование двухточечных каналов WAN.** Описано, как настроить выделенную линию между двумя маршрутизаторами с использованием протоколов PPP и HDLC.
- **Конфигурирование, поиск и устранение неисправностей для маршрутизаторов доступа к Интернету.** Рассказано, как настроить клиент DHCP, сервер DHCP и функцию PAT в маршрутизаторе доступа к Интернету с помощью программного обеспечения SDM.

Конфигурирование соединений WAN

В этой главе описано конфигурирование сетей WAN, рассмотренных в главах 4 и 22. В первой части главы описано конфигурирование выделенных линий с использованием инкапсуляции *высокоуровневого протокола управления каналом* (High-Level Data Link Control — HDLC) и *протокола двухточечного соединения* (Point-to-Point Protocol — PPP). Во второй части показано, как настроить функции уровня 3 в маршрутизаторе доступа к Интернету, в частности, как настроить *протокол динамического конфигурирования хоста* (Dynamic Host Configuration Protocol — DHCP), а также службу *трансляции сетевых адресов и трансляции адресов с использованием портов* (Network Address Translation/Port Address Translation — NAT/PAT). Во второй части главы практически не используется интерфейс командной строки маршрутизатора, а все настройки осуществляются с помощью веб-приложения, называемого *диспетчером управления устройствами безопасности* (Security Device Manager — SDM).

Контрольные вопросы: знаете ли вы уже темы главы

Этот раздел предназначен для того, чтобы читатель мог предварительно оценить свои знания и решить, нужно ли ему читать главу целиком. Если ответы на девять из десяти вопросов даны правильно, можно сразу же перейти к последнему разделу “Подготовка к экзамену”. Основные темы этой главы и предварительных контрольных вопросов перечислены в табл. 23.1. Отвечая на контрольные вопросы и используя таблицу, читатель сможет достаточно точно определить свои знания в той или иной области. Ответы на вопросы приведены в приложении А “Ответы на контрольные вопросы”.

Таблица 23.1. Темы контрольных вопросов

Основная тема	Номера вопросов
Конфигурирование двухточечных каналов WAN	1–3
Конфигурирование, поиск и устранение неисправностей для маршрутизаторов доступа к Интернету	4–7

- Маршрутизаторы R1 и R2 соединены с помощью выделенной линии через интерфейсы Serial 0/0. В настоящий момент маршрутизаторы успешно пересылают пакеты через такой канал и используют инкапсуляцию HDLC. Какую команду нужно ввести, чтобы использовать протокол PPP?
 - encapsulation ppp.
 - no encapsulation hdlc.

- в) `clock rate 128000.`
- г) `bandwidth 128000.`
2. В лаборатории были установлены маршрутизаторы R1 и R2. Устройства были соединены последовательным кабелем напрямую (back-to-back) интерфейсами Serial 0/0. Какое из указанных ниже утверждений верно для такого соединения?
- Если кабель DCE подключен к маршрутизатору R1, для соответствующего интерфейса маршрутизатора R2 нужно указать команду `clock rate`.
 - Если кабель DTE подключен к маршрутизатору R1, для соответствующего интерфейса маршрутизатора R2 нужно указать команду `clock rate`.
 - Если команда `clock rate 128000` указана в маршрутизаторе R1, то в маршрутизаторе R2 нужно настроить команду `bandwidth 128`.
 - Ни один из перечисленных выше вариантов не верен.
3. Два новых маршрутизатора компании Cisco были куплены некоторой организацией и установлены в разных хостах на расстоянии 100 км друг от друга. Два маршрутизатора соединены выделенной линией с пропускной способностью 768 Кбит/с. Какие из перечисленных ниже команд нужно ввести как минимум в одном из маршрутизаторов, чтобы он смог пересыпать фреймы по выделенной линии, используя протокол PPP в качестве инкапсуляции канального уровня?
- `no encapsulation hdlc.`
 - `encapsulation ppp.`
 - `clock rate 768000.`
 - `bandwidth 768.`
 - `description this is the link.`
4. Если сетевой инженер конфигурирует сервер DHCP в маршрутизаторе доступа к Интернету с помощью программы SDM, какие из настроек обычно он указывает? (Выберите несколько ответов.)
- MAC-адреса компьютеров в локальной сети.
 - IP-адрес маршрутизатора провайдера на общем кабеле или в канале DSL.
 - Диапазон IP-адресов, который будет назначаться хостам в локальной сети.
 - Адреса серверов DNS, которые были получены через протокол DHCP от провайдера услуги.
5. Сетевой инженер конфигурирует маршрутизатор доступа к Интернету с помощью программы SDM и хочет одновременно задать настройки клиента DHCP и службы PAT. Какие утверждения верны для такого процесса?
- Мастер настройки SDM требует, чтобы служба PAT была настроена, если настраивается клиент DHCP.
 - Мастер настройки SDM воспринимает интерфейсы, на которых заданы IP-адреса, как потенциальные внутренние порты для службы PAT.
 - Мастер настройки SDM воспринимает интерфейс, на котором запущена служба клиента DHCP, как внутренний интерфейс для службы трансляции адресов.
 - Ни один из перечисленных выше вариантов не верен.

6. Какое из указанных ниже утверждений верно для процесса конфигурирования устройства программой SDM?
 - а) Для конфигурирования маршрутизатора диспетчер SDM использует соединение SSH через консоль или сеть IP.
 - б) Диспетчер SDM использует веб-интерфейс сети IP или консоль.
 - в) Диспетчер SDM загружает команды в маршрутизатор после окончания работы каждого мастера (после того, как пользователь щелкнет на кнопке) и сохраняет конфигурацию как в текущем (*running-config*), так и в стартовом (*startup-config*) файле.
 - г) Ни один из перечисленных выше вариантов не верен.
7. Какие проблемы наиболее часто встречаются при конфигурировании функций третьего уровня в маршрутизаторе доступа к Интернету? (Выберите несколько ответов.)
 - а) Игнорируется обычно используемая, но необязательная информация от сервера DHCP провайдера, например IP-адреса серверов DNS.
 - б) Установлены неправильные интерфейсы в качестве внутренних и внешних для службы PAT.
 - в) Не настроен точно тот же протокол маршрутизации, который использует провайдер.
 - г) Не включен протокол CDP в интерфейс, подключенный к сети провайдера услуги.

Основные темы

Конфигурирование двухточечных каналов WAN

В текущем относительно небольшом разделе описано, как настроить выделенную линию между двумя маршрутизаторами с использованием протокола HDLC или PPP. Требуемая конфигурация удивительно проста, для протокола HDLC вообще ничего не нужно настраивать, а для протокола PPP нужно ввести всего одну команду в режиме конфигурирования интерфейса (`encapsulation ppp`). Тем не менее ниже будут рассмотрены еще несколько необязательных этапов конфигурирования, которые могут быть полезны, а также объяснено их влияние на работу канала.

ВНИМАНИЕ!

В этой главе подразумевается, что во всех последовательных каналах используются внешние модули CSU/DSU. Конфигурация таких модулей или настройки встроенных интерфейсов CSU/DSU выходят за рамки рассмотрения данной книги.

Конфигурирование инкапсуляции HDLC

Если рассматривать технологию Ethernet с точки зрения трех уровней модели OSI, например, то можно заметить, что для настройки 1 и 2 уровней не требуется каких-либо дополнительных команд, чтобы устройство могло пересыпать пакеты IP. Характеристики уровня 1 являются стандартными, и нужно просто подключить правильный кабель. Операционная система IOS стандартно использует инкапсуляцию Ethernet для всех интерфейсов Ethernet устройства, поэтому не нужны какие-либо команды уровня 2. Чтобы маршрутизатор мог пересыпать пакеты уровня 3, необходимо указать IP-адрес на интерфейсе и зачастую команду `no shutdown`, если в состоянии порта выводится строка “`administratively down`” (административно выключен).

Абсолютно аналогично в последовательных интерфейсах маршрутизаторов компании Cisco стандартно используется протокол HDLC, который не требует дополнительных настроек на 1 и 2 уровнях. Кабели должны быть подключены так, как описано в главах 4 и 22, но для первого уровня эталонной модели не нужны дополнительные команды. Поскольку стандартно используется именно протокол HDLC, то на уровне 2 также не нужны никакие команды для настройки интерфейса. Точно так же как и в интерфейсах Ethernet, нужно указать IP-адрес с помощью команды `ip address`, чтобы устройство могло пересыпать пакеты IP и, возможно, команду `no shutdown`.

Тем не менее в последовательных каналах зачастую требуется указывать некоторые необязательные команды. Ниже описаны некоторые этапы конфигурации, условия, в которых их нужно использовать, и требуемые команды (следует помнить, что они необязательны!).



Обязательные и необязательные этапы конфигурирования последовательного канала между двумя маршрутизаторами

Этап 1 Нужно указать IP-адрес на интерфейсе с помощью команды `ip address`.

Этап 2 Следующие действия нужно выполнять только в том случае, если они явно указаны или указаны соответствующие условия.

- а) если в режиме конфигурирования интерфейса указана команда `encapsulation какой-либо_протокол`, следует заменить ее командой `encapsulation hdlc`, чтобы включить протокол HDLC;
- б) если код состояния интерфейса указывает на то, что интерфейс административно выключен (“`administratively down`”), нужно ввести команду `no shutdown`;
- в) если последовательные интерфейсы соединены кабелем напрямую (back-to-back serial link) в лабораторных условиях или в эмуляторе сети, нужно задать частоту тактовых импульсов с помощью команды в режиме конфигурирования интерфейса `clock rate скорость`. Эту команду нужно вводить только для интерфейса DCE, т.е. порта, к которому подключен кабель DCE (тип интерфейса можно определить с помощью команды `show controllers serial номер`).

Этап 3 Следующие настройки всегда являются необязательными и не влияют на то, как будет передаваться трафик IP и как будет работать линия:

- а) можно указать логическую скорость канала с помощью команды `bandwidth скорость_в_Кбит/с` в режиме конфигурирования интерфейса;
- б) чтобы конфигурация была удобочитаемой, можно указать описание для интерфейса с помощью команды `description текст` в режиме конфигурирования интерфейса.

На практике, когда устанавливается новый маршрутизатор Cisco, т.е. в устройстве нет никакой предварительной конфигурации, а также если используется стандартная схема подключения к линии модулем CSU/DSU, то `ip address` — единственная команда, которую придется внести в конфигурацию интерфейса. На рис. 23.1 показана схема тестовой сети, а в примере 23.1 приведена соответствующая конфигурация. В данном случае последовательный канал был установлен в результате прямого подключения маршрутизаторов друг к другу с помощью кабеля, поэтому кроме настройки этапа 1 (команда `ip address`) пришлось использовать команду этапа 2 в (`clock rate`), а также было указано описание для интерфейса на этапе 3 б (команда `description`).

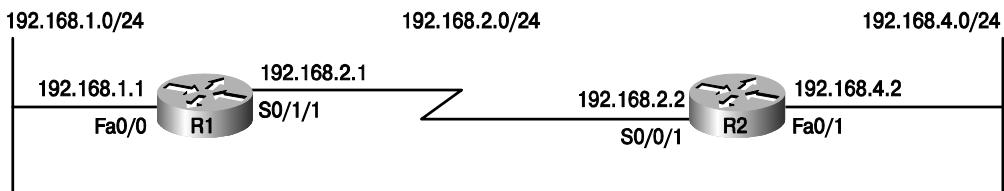


Рис. 23.1. Последовательный канал между двумя маршрутизаторами

Пример 23.1. Конфигурирование инкапсуляции HDLC

R1#show running-config

! Внимание! Показаны только нужные команды конфигурации.

interface FastEthernet0/0

ip address 192.168.1.1 255.255.255.0

```

!
interface Serial0/1/1
    ip address 192.168.2.1 255.255.255.0
    description link to R2
    clockrate 1536000
!
router rip
    version 2
    network 192.168.1.0
    network 192.168.2.0
!
R1#show controllers serial 0/1/1
Interface Serial0/1/1
Hardware is GT96K
DCE V.35, clock rate 1536000
! Часть строк вывода опущена.
R1#show interfaces s0/1/1
Serial0/1/1 is up, line protocol is up
    Hardware is GT96K Serial
    Description: link to R2
    Internet address is 192.168.2.1/24
    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 00:00:06, output 00:00:03, output hang never
    Last clearing of "show interface" counters never
    Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
    Queueing strategy: weighted fair
    Output queue: 0/1000/64/0 (size/max total/threshold/drops)
        Conversations 0/1/256 (active/max active/max total)
        Reserved Conversations 0/0 (allocated/max allocated)
        Available Bandwidth 1158 kilobits/sec
    5 minute input rate 0 bits/sec, 0 packets/sec
    5 minute output rate 0 bits/sec, 0 packets/sec
        70 packets input, 4446 bytes, 0 no buffer
        Received 50 broadcasts, 0 runts, 0 giants, 0 throttles
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        73 packets output, 5280 bytes, 0 underruns
        0 output errors, 0 collisions, 5 interface resets
        0 output buffer failures, 0 output buffers swapped out
        0 carrier transitions
        DCD-up      DSR-up      DTR-up      RTS-up      CTS-up
R1#show ip interface brief
Interface      IP-Address  OK?   Method  Status          Protocol
FastEthernet0/0 192.168.1.1 YES    manual   up           up
FastEthernet0/1 unassigned   YES    NVRAM   administratively down  down
Serial0/0/0     unassigned   YES    NVRAM   administratively down  down
Serial0/0/1     unassigned   YES    manual   administratively down  down
Serial0/1/0     unassigned   YES    manual   administratively down  down
Serial0/1/1     192.168.2.1 YES    manual   up           up
R1#show interfaces description
Interface          Status          Protocol      Description
Fa0/0              up             up
Fa0/1              admin down    down
Se0/0/0            admin down    down
Se0/0/1            admin down    down
Se0/1/0            admin down    down
Se0/1/1            up             up           link to R2

```

Конфигурация маршрутизатора R1 относительно проста. В соответствующей конфигурации интерфейса S0/0/1 маршрутизатора R2 нужно указать всего лишь команду `ip address`, стандартно для интерфейса задана команда `encapsulation hdlc` и понадобится включить соответствующий порт с помощью команды `no shutdown`. Команда `clock rate` не понадобится в маршрутизаторе R2, поскольку кабель DCE включен в маршрутизатор R1, следовательно, в устройстве R2 может быть использован только кабель DTE.

В примере показан вывод нескольких команд `show`. С помощью команды `show controllers` можно убедиться в том, что порт S0/1/1 работает в режиме DCE. Команда `show interfaces S0/1/1` выводит различные настройки, в том числе и стандартную инкапсуляцию на интерфейсе (HDLC), а также стандартное значение полосы пропускания (1544, т.е. 1544 Кбит/с, или 1,544 Мбит/с). В конце примера показан результат выполнения команд `show ip interface brief` и `show interfaces description`, отображающих краткую информацию о состоянии интерфейсов, в частности коды состояния линии и протокола.

Конфигурирование протокола PPP

Настройка простого варианта протокола PPP не менее проста, чем настройка протокола HDLC, за исключением того, что последний является стандартной инкапсуляцией на последовательных интерфейсах и не требует дополнительной конфигурации. Чтобы сменить инкапсуляцию на PPP, нужно ввести только одну команду — `encapsulation ppp`. Все остальные этапы конфигурирования полностью совпадают с необязательными этапами настройки протокола HDLC. В примере 23.2 показана конфигурация последовательных интерфейсов маршрутизаторов R1 и R2 с использованием протокола PPP (см. рис. 23.1).

Пример 23.2. Конфигурирование инкапсуляции PPP

```
! Конфигурация устройства R1.  
R1#show running-config interface s0/1/1  
Building configuration...  
  
Current configuration : 129 bytes  
!  
interface Serial0/1/1  
  description link to R2  
  ip address 192.168.2.1 255.255.255.0  
  encapsulation ppp  
  clockrate 1536000  
end  
! -----  
! Конфигурация устройства R2.  
R2#show run interface s0/0/1  
Building configuration...  
  
Current configuration : 86 bytes  
!  
interface Serial0/0/1  
  ip address 192.168.2.2 255.255.255.0  
  encapsulation ppp  
end
```

В примере выше показан новый вариант команды `show running-config` и выделены команды, относящиеся к протоколу PPP. Команда `show running-config interface S0/1/1` для маршрутизатора R1 выводит конфигурацию интерфейса S0/1/1, и только ее, все остальные настройки не отображаются. Аналогичная команда показана для маршрутизатора R2. Обратите внимание: в обоих устройствах была использована команда `encapsulation ppp` для интерфейсов — важно, чтобы инкапсуляция была одинакова на двух концах канала, иначе он не заработает.

Конфигурирование, поиск и устранение неисправностей для маршрутизаторов доступа к Интернету

Как отмечалось в главе 22, маршрутизатор доступа к Интернету обычно подключен к всемирной сети одним интерфейсом, а второй его порт подключен к локальной сети. Маршрутизаторы потребительского класса для доступа к Интернету обычно поставляются с изначально настроенным клиентом DHCP на порту, подключенным к провайдеру, сервер DHCP запущен на интерфейсе локальной сети и включена служба PAT. В маршрутизаторах корпоративного уровня много больше функций, которые могут понадобиться или не понадобиться в сети компании, они могут не использоваться для доступа к Интернету, а просто выполнять маршрутизацию в корпоративной сети, поэтому эти функции не включены в них стандартно. В этом разделе описано, как настроить перечисленные функции в маршрутизаторах компании Cisco.

Интерфейс командной строки — не единственный метод конфигурирования маршрутизаторов компании Cisco. Чтобы соответствовать экзамену компании Cisco ICND1, в этой главе описано, как настроить разные функции с помощью специализированного программного обеспечения, называемого *диспетчером для управления и безопасностью маршрутизаторов компании Cisco* (Router and Security Device Manager — SDM)¹. Вместо использования сеансов Telnet или SSH пользователь подключается к устройству через веб-браузер. (Для подключения к маршрутизатору через браузер у устройства должен быть задан как минимум один IP-адрес, и такой адрес должен быть доступен с компьютера сетевого инженера.) Приложение SDM позволяет конфигурировать множество функций, в том числе клиент DHCP, сервер DHCP и службу PAT.

ВНИМАНИЕ!

Корпорация Cisco заменила *диспетчер управления устройствами Cisco* (Cisco Device Manager — CDM) новым, но очень похожим инструментом Cisco Configuration Professional (CCP), но в темах экзамена 640-802 все еще упоминается устаревший диспетчер SDM. Однако с точки зрения важности при изучении SDM в этой книге либо при использовании приложений SDM или CCP в ходе подготовки к экзаменам следует сосредоточиться на том, что вы вводите и выбираете в графическом интерфейсе, а фактический экран, на котором вы вводите или выбираете информацию, менее важен.

Следует заметить, что функции, настройка которых с помощью диспетчера SDM показана ниже, можно задать и с помощью интерфейса командной строки.

¹ Вероятно, имелся в виду *диспетчер управления устройствами Cisco* (Cisco Device Manager — CDM) или *диспетчер управления устройствами безопасности Cisco* (Cisco Security Device Manager — SDM). — Примеч. ред.

Маршрутизатор доступа к Интернету: этапы конфигурирования

С помощью программного обеспечения SDM можно настроить клиент DHCP, сервер DHCP и службу PAT, следуя перечисленным ниже этапам.

- Этап 1 Установить связь IP в сети.** Следует спланировать и настроить (из интерфейса командной строки) IP-адреса в локальной сети, чтобы компьютеры имели доступ к интерфейсу маршрутизатора.
- Этап 2 Установить и запустить приложение SDM.** Следует установить диспетчер SDM на маршрутизаторе и рабочей станции, а затем подключиться к маршрутизатору доступа.
- Этап 3 Настроить службы DHCP и PAT.** С помощью диспетчера SDM следует настроить службы клиента DHCP и трансляции адресов PAT.
- Этап 4 Распланировать и настроить параметры службы DHCP.** Необходимо распланировать, какие IP-адреса будут выдаваться маршрутизатором для хостов в локальной сети, какой адрес сервера DNS будет использоваться, доменное имя и какой стандартный шлюз будут анонсироваться.
- Этап 5 Настроить сервер DHCP.** С помощью диспетчера SDM необходимо настроить сервер DHCP в маршрутизаторе доступа к Интернету.

В следующих разделах перечисленные этапы описаны подробно. Конфигурирование выполняется для той же топологии сети, которая была описана в главе 22 и показана в текущей главе на рис. 23.2.

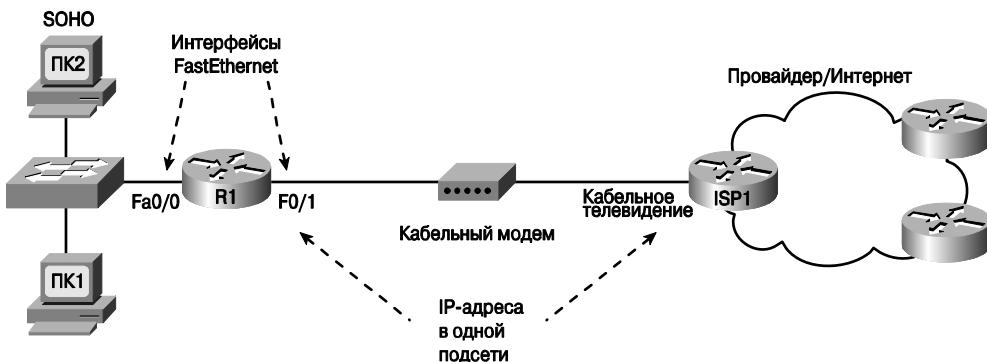


Рис. 23.2. Топология с маршрутизатором доступа к Интернету

Этап 1: установить связь IP в сети

В маршрутизаторах доступа к Интернету используются IP-адреса частных сетей для локальной сети (см. главу 22). Для данного этапа нужно выполнить следующие действия.

Детали процесса планирования и конфигурирования IP-адресов для локальной сети маршрутизатора доступа к Интернету

Ключевая тема

- Этап а** Выбрать произвольную частную сеть.
- Этап б** Выбрать маску, которая дает достаточное количество адресов хостов (стандартной маски соответствующего класса частной сети будет вполне достаточно).
- Этап в** Выбрать IP-адрес для маршрутизатора в такой сети.

На практике абсолютно все равно, какую из частных сетей использовать, поскольку она частная, и внешние маршрутизаторы о ней ничего не знают. Во многих маршрутизаторах потребительского класса используется частная сеть класса С 192.168.1.0, она же будет использоваться в примерах этой главы со стандартной классовой маской. Даже если вы работаете в не очень маленькой компании с несколькими филиалами и каждый из филиалов подключен к Интернету, для каждого филиала можно использовать ту же сеть, поскольку служба NAT/PAT в любом случае будет транслировать адреса.

Этап 2: установка и запуск диспетчера SDM

Чтобы установить диспетчер SDM на маршрутизатор (если он там не установлен) и получить доступ к конфигурационным настройкам устройства через веб-браузер, инженеру понадобится компьютер, подключенный к той же сети IP, что и маршрутизатор. Обычно инженер использует компьютер в локальной сети и устанавливает адрес из той же подсети на интерфейсе маршрутизатора, подключенном к локальной сети (этап 1). Следует помнить, что диспетчер SDM не использует сеансы Telnet или SSH, а компьютер должен быть подключен к маршрутизатору именно через сеть IP, с помощью консоли можно получить доступ только к командной строке устройства.

Сетевому инженеру придется ввести несколько дополнительных команд в маршрутизаторе, чтобы можно было получить к нему доступ и использовать устройство, но такие команды выходят за рамки рассмотрения этой книги. Если читателю нужна дополнительная информация, он может обратиться к веб-сайту компании Cisco <http://www.cisco.com/> и прочитать документацию в разделе “Установка SDM” (“SDM installation”). Этот этап конфигурирования предполагает, что программное обеспечение SDM используется в лабораторных условиях, но нужно помнить, что в реальной сети могут потребоваться дополнительные действия. В конце этого этапа и процесса установки читатель должен получить доступ с помощью веб-браузера к маршрутизатору и увидеть в браузере соответствующую страницу диспетчера SDM, которая показана на рис. 23.3.

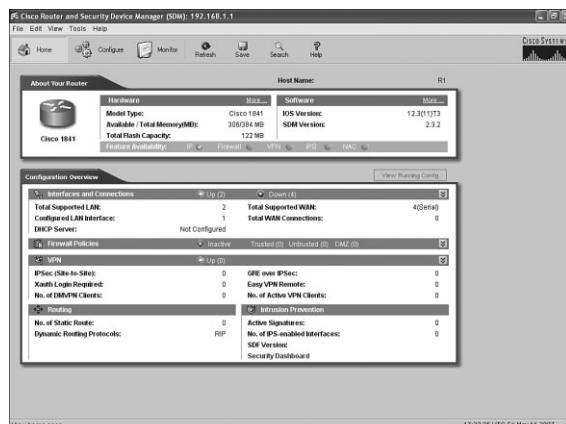


Рис. 23.3. Домашняя страница диспетчера SDM

Этап 3: конфигурирование служб DHCP и PAT

В пользовательском интерфейсе диспетчера SDM есть множество мастеров (wizards) настройки разных служб через интерактивный веб-интерфейс, в котором нужно ответить на вопросы и заполнить нужные поля. По завершении процесса приложение SDM загружает полученную конфигурацию в маршрутизатор.

Один из мастеров диспетчера предназначен для конфигурирования функции клиента DHCP на интерфейсе, подключенном к Интернету, и дополнительно запуска службы PAT. В этом разделе показаны веб-страницы настройки указанных функций для маршрутизатора R1 на схеме сети рис. 23.2.

Чтобы осуществить нужные настройки, в интерфейсе, показанном на рис. 23.3, выполните следующие действия.

1. В верхней части страницы браузера щелкните на кнопке **Configure** (Настроить).
2. Щелкните на кнопке **Interfaces and Connections** (Интерфейсы и соединения) панели **Tasks** (Задания), слева в открывшемся окне.

На рис. 23.4 показано окно конфигурирования интерфейсов (**Interfaces and Connections**), в котором отображается вкладка **Create Connection** (Создать соединение). Обратите внимание: на рисунке описанные выше элементы отмечены стрелками.

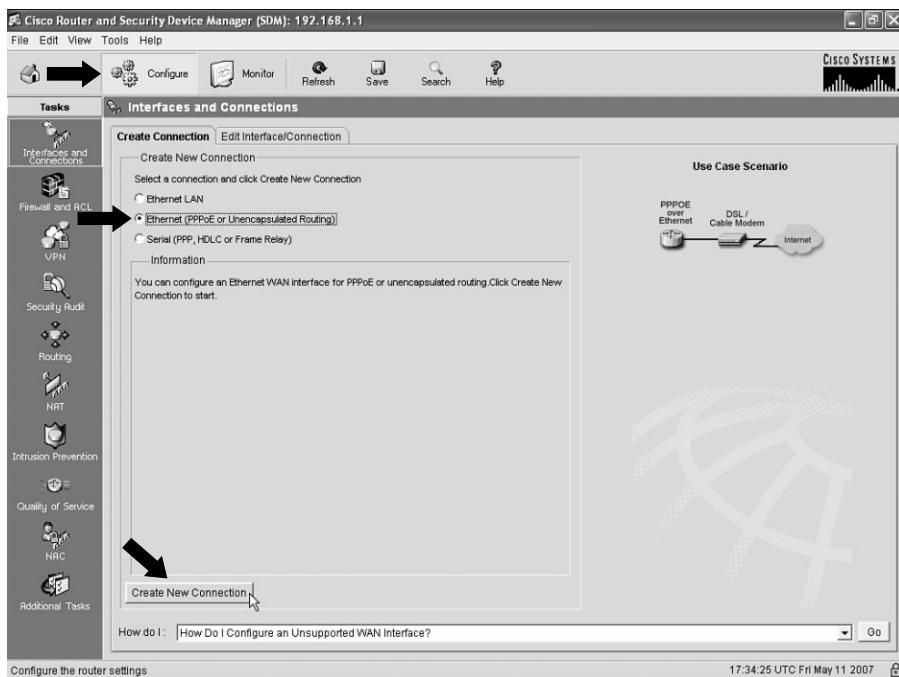


Рис. 23.4. Окно конфигурирования интерфейсов и соединений диспетчера SDM

Топология сети, показанная в правой верхней части окна, выглядит подозрительно знакомой, не правда ли? Она, в общем, совпадает со схемой сети на рис. 23.2, в которой маршрутизатор подключен к каналу через кабельный modem или modem DSL. Во вкладке **Create Connection** (Создать соединение) выполните следующие действия.

- Установите флажок Ethernet (PPPoE or Unencapsulated Routing) (Соединение Ethernet (PPPoE или инкапсулированная маршрутизация)).
- Щелкните на кнопке Create New Connection (Создать новое соединение) в нижней части окна вкладки.

После выполнения указанных действий появится мастер настройки соединения Ethernet интерфейса SDM (SDM Ethernet Wizard), который показан на рис. 23.5. В приведенном окне нет опциональных параметров, которые можно было бы установить, поэтому просто щелкните на кнопке Next (Дальше).

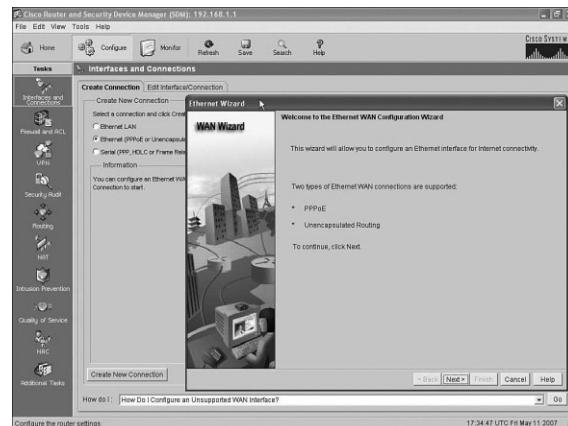


Рис. 23.5. Первая страница мастера настройки Ethernet

В открывшемся окне, показанном на рис 23.6, есть всего один флажок, и если он установлен, то в устройстве включается инкапсуляция *PPP в середине Ethernet* (PPP over Ethernet — PPPoE). Если провайдер использует технологию PPPoE, то флажок нужно установить. Обычно флажок не устанавливается и используется маршрутизация без инкапсуляции, подразумевающая, что маршрутизатор передает фреймы Ethernet, содержащие пакет IP, в интерфейс, как было описано в нескольких главах части III.

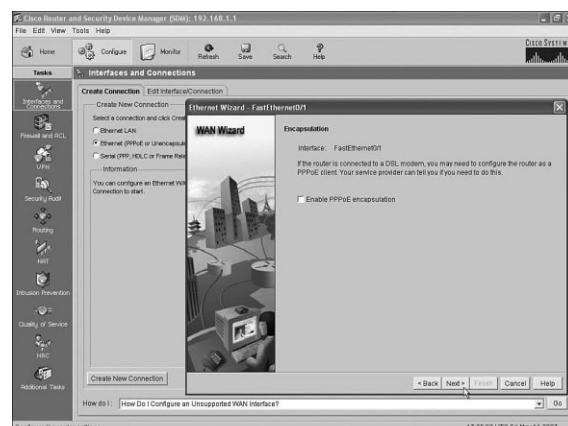


Рис. 23.6. Мастер настройки Ethernet: окно выбора инкапсуляции PPPoE

В верхней части окна на рис. 23.6 в мастере настройки был выбран интерфейс Fast Ethernet, Fa0/1 с целью дальнейшего его конфигурирования. В маршрутизаторе, который используется в рассматриваемом примере, есть два интерфейса локальной сети, одному из которых уже назначен IP-адрес на этапе 1 выше (Fa0/0). Поскольку мастер настройки конфигурирует клиент DHCP в маршрутизаторе, он выбрал интерфейс командной строки, в котором не установлен IP-адрес, а именно Fa0/1. Следует убедиться в том, что мастер настройки устройства выбрал правильный интерфейс, подключенный к модему DSL или кабельному модему, поскольку эта информация жизненно важна для последующего поиска и устранения неисправностей. Этот интерфейс также будет внешним с точки зрения технологии NAT/PAT.

Щелкните на кнопке **Next** (Дальше). На рис. 23.7 показано следующее окно мастера, связанное с настройками IP-адресации. В этом окне можно указать IP-адрес статически, но, как упоминалось в главе 22, практически всегда адрес выдается динамически провайдером — это уникальный глобально маршрутизуемый адрес из блока сетей провайдера. Следовательно, нужно убедиться в том, что установлен флагок **Dynamic (DHCP Client)** (Динамически (клиент DHCP)).

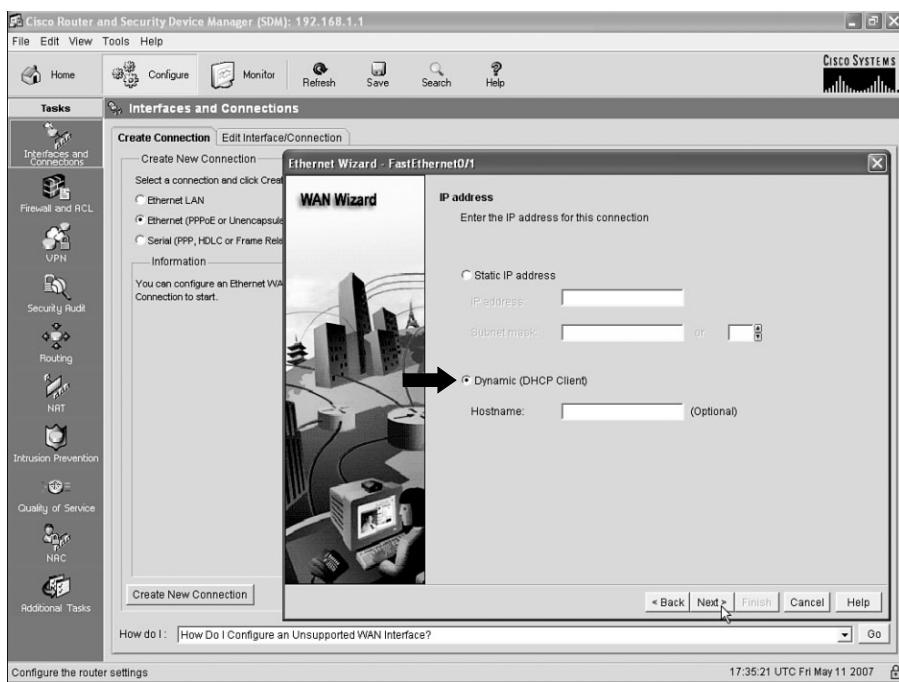


Рис. 23.7. Мастер настройки Ethernet: присвоение адреса через протокол DHCP или статически

Щелкните на кнопке **Next** (Дальше), чтобы перейти к окну **Advanced Options** (Дополнительные параметры), показанному на рис. 23.8. На этом этапе необходимо указать, что будет конфигурироваться трансляция адресов PAT, что также практически всегда выполняется в маршрутизаторах доступа к Интернету. Установите флагок **Port Address Translation** (Трансляция адресов с использованием портов), а если по какой-либо причине транслировать адреса не нужно, сбросьте его.

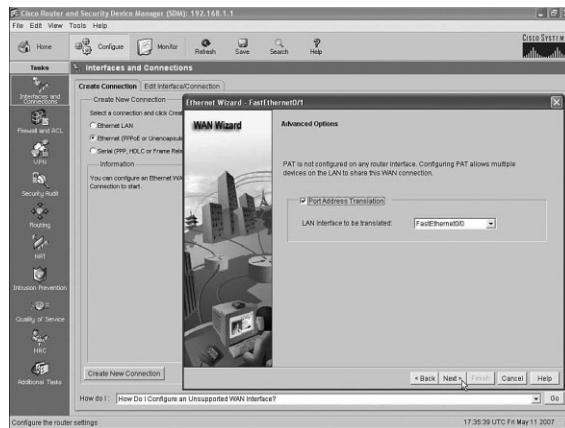


Рис. 23.8. Мастер настройки Ethernet: включение трансляции PAT и выбор внутреннего интерфейса для нее

Обратите внимание на раскрывающийся список LAN Interface to Be Translated (Будет транслироваться интерфейс LAN) в середине окна. В терминологии службы NAT в этом списке указан внутренний интерфейс, т.е. порт, подключенный к локальной сети. В данном примере показан интерфейс FastEthernet0/0, как и предполагалось. Не менее важен тот факт, что интерфейс FastEthernet0/1, который был настроен мастером как клиент DHCP, в данном случае будет внешним интерфейсом для службы NAT, что также правильно.

Щелкните на кнопке Next (Дальше), чтобы перейти к окну Summary (Резюме), показанному на рис. 23.9, в котором показаны параметры, выбранные в процессе конфигурирования рассматриваемых служб. В этом окне показано:

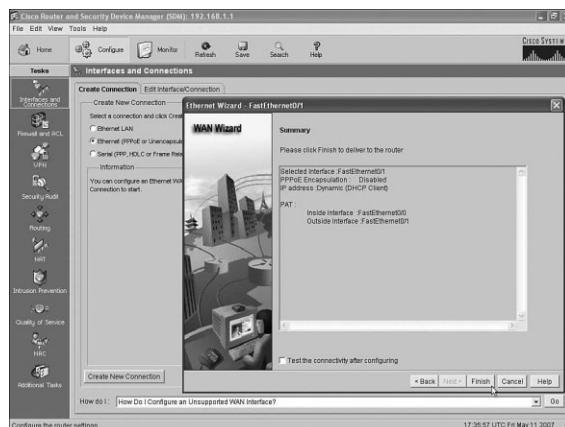


Рис. 23.9. Мастер настройки Ethernet: изменения, которые будут внесены в конфигурацию устройства

- что конфигурировался интерфейс FastEthernet0/1;
- для него будет запущена служба клиента DHCP;

- инкапсуляция PPPoE отключена, следовательно, используется маршрутизация без инкапсуляции;
- служба РАТ включена, интерфейс FastEthernet0/0 используется в качестве внутреннего для нее, а FastEthernet0/1 — внешнего.

Щелкните на кнопке **Finish** (Завершить). Приложение SDM создает конфигурационный файл и копирует его в файл текущей конфигурации устройства (`running-config`). Если нужно сохранить конфигурацию, то следует щелкнуть на кнопке **Save** (Сохранить), чтобы программное обеспечение SDM выполнило команду `copy running-config startup-config`. Без последнего действия настройки будут изменены только в текущем конфигурационном файле.

Итак, клиент DHCP и служба РАТ настроены. Осталось спланировать конфигурацию сервера DHCP для локальной сети и с помощью мастеров диспетчера SDM настроить их.

Этап 4: планирование служб DHCP

Перед тем как запускать функцию сервера DHCP на маршрутизаторе для локальной сети, следует выбрать несколько ключевых параметров настройки сервера. В частности, выбрать подсеть частной сети IP, которая будет использоваться в сегменте локальной сети. Например, в примерах этой главы на этапе 1 была выбрана сеть 192.168.1.0 со стандартной маской 255.255.255.0. Предпочтительнее всего настроить устройство таким образом, чтобы только некоторый блок адресов из такой сети назначался сервером DHCP, а часть адресов была оставлена для назначения вручную статическим образом. Например, интерфейсу Fa0/0 маршрутизатора R1, который подключен к локальной сети, где был назначен IP-адрес 192.168.1.1, следовательно, такой адрес следует исключить из пула адресов, назначаемых сервером.

Ниже перечислены ключевые факты, которые нужно собрать перед тем, как конфигурировать маршрутизатор в качестве сервера DHCP. Первые три параметра относятся к планированию локальной сети, а два последние получены от провайдера и должны быть переданы хостам в локальной сети без искажений.

Планирование конфигурации службы сервера DHCP для локальной сети



1. Вспомните адреса частных сетей и их стандартные маски, которые используются в локальных сетях, и выберите из них сеть, которую будет назначать хостам сервер DHCP.
2. Запомните, какой IP-адрес установлен в соответствующем интерфейсе маршрутизатора, — этот адрес сервер будет выдавать хостам как стандартный шлюз.
3. Определите, какой IP-адрес сервера DNS был получен от провайдера клиентом DHCP маршрутизатора с помощью команды `show dhcp server`. Маршрутизатор впоследствии сможет передавать этот адрес хостам-клиентам локальной сети в настройках.
4. Определите, какое доменное имя было получено от провайдера, с помощью той же команды `show dhcp server`.

ВНИМАНИЕ!

В документации и книгах компании Cisco используется термин *пул DHCP* (DHCP pool) для обозначения блока адресов, присваиваемых сервером DHCP хостам в локальной сети.

В рассматриваемом примере сеть IP 192.168.1.0 с маской /24 уже была выбрана на этапе 1 в процессе конфигурирования устройства. Диапазон 192.168.1.101–192.168.1.254 был зарезервирован для клиентов DHCP в локальной сети, а диапазон 192.168.1.1–192.168.1.100 — для статических адресов. IP-адрес интерфейса маршрутизатора был также установлен на этапе 1 и равен 192.168.1.1, чтобы сетевой инженер мог подключиться к маршрутизатору с помощью диспетчера SDM, следовательно, именно его нужно указать в качестве адреса стандартного шлюза (default gateway).

Для двух последних этапов планирования, определения IP-адреса сервера DNS и доменного имени нужно найти требуемые параметры в выводе команды `show dhcp server`, как показано в примере 23.3. Эта команда выводит информацию о клиенте DHCP, а также параметры, полученные от сервера, когда маршрутизатору динамически назначался IP-адрес. Нужная информация о настройках DHCP выделена в примере 23.3.

Пример 23.3. Определение IP-адреса сервера DNS и доменного имени

```
R1#show dhcp server
DHCP server: ANY (255.255.255.255)
Leases: 8
Offers: 8 Requests: 8 Acknowledgments: 8 Nacks: 0
Declines: 0 Releases: 21 Bad: 0
DNS0: 198.133.219.2, DNS1: 0.0.0.0
Subnet: 255.255.255.252 DNS Domain: example.com
```

Этап 5: конфигурирование сервера DHCP

Чтобы настроить сервер DHCP с помощью приложения SDM, щелкните на кнопке **Configure** (Настроить) верхней панели, а потом на кнопке **Additional Tasks** (Дополнительные задания) панели **Tasks** (Задания). Откроется окно приложения, которое показано на рис. 23.10.

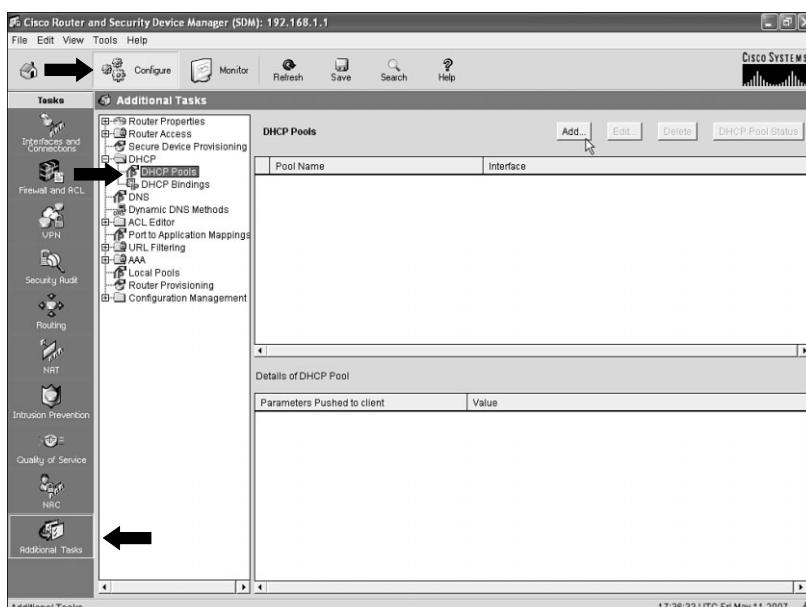


Рис. 23.10. Окно конфигурирования дополнительных настроек диспетчера SDM

Выберите опциональный параметр DHCP Pools (Пулы DHCP) в списке в левой части окна (указана стрелкой) и щелкните на кнопке Add (Добавить), чтобы открыть диалоговое окно пула, показанное на рис. 23.11. В этом диалоговом окне есть поля, в которых нужно указать информацию, собранную на предыдущем этапе, а также дополнительные настройки. На рис. 23.11 продемонстрировано, как настроить маршрутизатор R1 согласно рассматриваемому примеру.

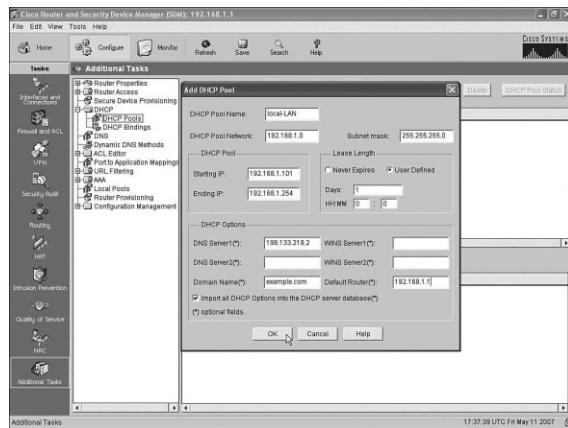


Рис. 23.11. Диалоговое окно пула DHCP в приложении SDM

Все рассмотренные на этапе 4 параметры заносятся в соответствующие поля в окне настроек SDM:

- диапазон адресов сервера DHCP;
- IP-адрес сервера DNS;
- доменное имя;
- настройки стандартного маршрутизатора (шлюза).

В диалоговом окне нужно указать адрес подсети и маску, которые будут использоваться в подсети, предназначенней для динамического присвоения адресов. Создаваемый пул адресов необходимо как-то назвать (в качестве имени можно использовать все, что угодно, но желательно задавать какое-то осмысленное описание, по которому будет понятно, для чего предназначен пул).

Итак, для конфигурирования маршрутизатора доступа к Интернету с помощью приложения SDM понадобилось выполнить несколько этапов, в которых нужно вводить информацию или выбирать из списков в нескольких диалоговых окнах. Тем не менее такой метод конфигурирования несколько проще, чем настройка тех же служб через интерфейс командной строки. В следующем разделе рассмотрено несколько небольших примеров проверки работы настроенных служб, а также поиск и устранение неисправностей в них.

Проверка работы маршрутизатора доступа к Интернету

Конфигурирование служб DHCP и NAT/PAT с помощью диспетчера SDM, а не интерфейса командной строки, имеет как свои преимущества, так и недостатки.

К положительным моментам можно отнести тот факт, что в экзамене ICND1, как в сертификации сугубо начального уровня, рассмотрен базовый набор полезных функций, которые придется настраивать сетевому инженеру в небольших и средних компаниях. Создаваемая приложением конфигурация будет достаточно велика (диспетчер SDM в данном случае создает для рассматриваемого примера порядка 20 конфигурационных команд), а за счет такого интерактивного процесса можно значительно сократить временные затраты на настройку служб и обойтись меньшими усилиями.

К отрицательным моментам метода настройки не через интерфейс командной строки можно отнести сложности с поиском и устранением неисправностей, возникающие из-за того, что конфигурационные команды не были подробно описаны. В результате инженеру в процессе поиска неисправностей придется внимательно проверить, какие значения параметров он ввел в процессе конфигурирования служб в мастерах приложения, и тщательно проверить настройки с помощью самого диспетчера SDM. Показывать все варианты проверки конфигурации с помощью диспетчера SDM достаточно утомительно, поэтому в данном разделе будут просто даны наиболее общие рекомендации по настройке служб DHCP и PAT, а также показано несколько ключевых команд интерфейса командной строки, которые пригодятся в практической работе.

Для простой проверки полученной конфигурации выполните следующие действия.



Что проверить при поиске и устраниении неисправностей в маршрутизаторе доступа к Интернету

- Этап 1** На компьютере в локальной сети запустите веб-браузер и попробуйте зайти на свой любимый сайт в Интернете (например, www.cisco.com). Если веб-страница загружается в окне браузера, значит, маршрутизатор доступа к Интернету правильно работает. Если нет — перейдите к этапу 2.
- Этап 2** Если на компьютере в локальной сети установлена операционная система компании Microsoft, запустите приложение командной строки и выполните команду `ipconfig /all`, чтобы увидеть, получил ли компьютер от сервера DHCP IP-адрес, маску, стандартный шлюз и IP-адрес сервера DNS. И если получил, то проверьте, правильны ли эти параметры. Если настройки не были получены или получены неправильно, используйте команды, перечисленные в главе 21, для поиска и устранения неисправностей.
- Этап 3** Проверьте кабель между маршрутизатором и локальной сетью, а также между маршрутизатором и модемом DSL. Убедитесь в том, что нужные сегменты сети подключены к правильным интерфейсам. Проверьте конфигурацию в приложении SDM, чтобы убедиться, что в службе PAT в качестве внутреннего интерфейса указан порт, подключенный к локальной сети, а в качестве внешнего — к модему DSL или кабельному модему.
- Этап 4** Проверьте работоспособность PAT, передав некий трафик с компьютера в локальной сети на получатель в Интернете (подробнее этот этап описан ниже).

Последний этап обычно проверяется с помощью нескольких команд из интерфейса командной строки. В примере 23.4 показан вывод нескольких команд, связанных с проверкой работоспособности конфигурации маршрутизатора доступа к Интернету, сопровождающихся небольшими комментариями.

Пример 23.4. Полезные команды для проверки работоспособности маршрутизатора доступа к Интернету

```
R1#show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address      Client-ID/Hardware address/User name Lease expiration      Type
```

```
192.168.1.101 0063.6973.636f.2d      May 12 2007 08:24 PM
Automatic
192.168.1.111 0100.1517.1973.2c      May 12 2007 08:26 PM
Automatic
R1#show ip nat translations
Pro Inside global    Inside local        Outside local     Outside global
tcp 64.100.1.1:36486 192.168.1.101:36486 192.168.7.1:80  192.168.7.1:80
udp 64.100.1.1:1027  192.168.1.111:1027  198.133.219.2:53 198.133.219.2:53
R1#clear ip nat translation *
R1#show ip nat translations
R1#
```

Команда `show ip dhcp binding` выводит список IP-адресов, назначенных хостам в локальной сети сервером DHCP. Результат выполнения этой команды следует сравнить с адресами, которые были получены хостами, и убедиться в том, что они совпадают.

С помощью команды `ip nat translations` можно отследить, правильно ли работает служба NAT или PAT. В примере 23.4 команда выводит строку заголовка и две записи для преобразования адресов. Выделенные заглавия столбцов в заголовке относятся к локальному внутреннему (*inside local*) и глобальному внутреннему (*inside global*) адресам записей трансляций. Внутренний локальный адрес всегда должен быть адресом хоста в локальной сети, в данном случае 192.168.1.101. Маршрутизатор транслирует такой адрес в один из открытых маршрутизируемых адресов, в данном случае в IP-адрес 64.100.1.1, полученный маршрутизатором от сервера DHCP провайдера.

Последняя команда в примере, `clear ip nat translation *`, может быть полезна в том случае, когда кажется, что служба NAT должна работать правильно, но она не работает. В такой ситуации можно очистить (сбросить) таблицу преобразований, а когда узел начнет пересыпать данные, запись автоматически создастся заново. Следует помнить, что эта команда может сбросить установленные соединения некоторых приложений.

Подготовка к экзамену

Повторите все ключевые темы

Повторите все ключевые темы данной главы, помеченные пиктограммой “Ключевая тема”. Ключевые темы и соответствующие им страницы перечислены в табл. 23.2.

Таблица 23.2. Ключевые темы главы 23

Элемент	Описание	Страница
Список	Обязательные и необязательные этапы конфигурирования последовательного канала между двумя маршрутизаторами	627
Список	Детали процесса планирования и конфигурирования IP-адресов для локальной сети маршрутизатора доступа к Интернету	631
Список	Планирование конфигурации службы сервера DHCP для локальной сети	637
Список	Что проверить при поиске и устранении неисправностей в маршрутизаторе доступа к Интернету	640

Заполните таблицы и списки по памяти

Распечатайте приложение М (Appendix L) с компакт-диска или его раздел, относящийся к этой главе, и заполните таблицы и списки по памяти. В приложении Н (Appendix M) приведены заполненные таблицы и списки для самоконтроля.

Ключевые термины

Дайте определения перечисленных ниже терминов и проверьте правильность их написания в списке терминов:

диспетчер управления устройствами Cisco (Cisco Device Manager — CDM), диспетчер управления устройствами безопасности Cisco (Cisco Security Device Manager — SDM)

Список команд

Заучивать наизусть информацию в таблицах не нужно, тем не менее, для удобства упоминавшиеся в главе команды конфигурирования перечислены в табл. 23.3, а команды для мониторинга и устранения неисправностей — в табл. 23.4. На практике команды должны запомниться сами собой после выполнения практических лабораторных работ и в процессе подготовки к экзамену. Чтобы потренироваться в их запоминании, следует закрыть левую часть таблицы листком бумаги и по описанию в правом столбце по памяти записать соответствующие команды, а потом проверить, правильно ли был указан ответ.

Таблица 23.3. Команды для конфигурирования устройств

Команда	Описание
encapsulation {hdlc ppp frame-relay}	Команда для конфигурирования последовательного интерфейса маршрутизатора, указывающая, какой протокол (т.е. инкапсуляция) будет использоваться в канальном уровне соединения

Окончание табл. 23.3

Команда	Описание
clock rate <i>скорость</i>	Команда для конфигурирования последовательного интерфейса, задающая скорость в бит/с в том случае, если к интерфейсу подключен кабель DCE
bandwidth <i>скорость_в_Кбит/с</i>	Команда для конфигурирования интерфейса, которая задает логическую, а не физическую скорость канала, т.е. как маршрутизатор будет интерпретировать линию, но не влияет на фактическую скорость передачи. Значение задается в Кбит/с
description <i>текст</i>	Команда для конфигурирования интерфейса, указывающая описание порта

Таблица 23.4. Команды для мониторинга устройств и устранения неисправностей

Команда	Описание
show ip nat translations	Выводит записи в таблице NAT/PAT
show dhcp server	Показывает информацию, полученную от сервера DHCP, когда маршрутизатор (или его интерфейс) работает в качестве клиента DHCP
clear ip nat translation *	Очищает (удаляет) все динамические записи в таблице NAT/PAT
show interfaces	Выводит много полезной информации об интерфейсах, в том числе инкапсуляцию, настройки полосы пропускания, включены ли тестовые пакеты (keepalives), два кода состояния соединения, описание и информацию об IP-адресе и маске
show controllers serial <i>номер</i>	Позволяет определить, подключен ли кабель к интерфейсу и каков тип кабеля: DTE или DCE
show interfaces [<i>тип номер</i>] description	Выводит одну строку информации об интерфейсе (или по строке на каждый интерфейс), в которой указано состояние интерфейса и его описание
show ip interface brief	Выводит одну строку информации на каждый интерфейс, содержащую IP-адрес и описание состояния интерфейса

Часть VI. Подготовка к экзамену

Глава 24. “Подготовка к сертификационному экзамену”

ГЛАВА 24

Подготовка к сертификационному экзамену

В 23 предыдущих главах были достаточно подробно описаны технологии, протоколы, команды и функции, которые понадобятся для практической работы и уверенной сдачи сертификационного экзамена ICND1. Несмотря на то что этих глав вполне достаточно, многим людям необходима дополнительная подготовка, а не просто прочтение теоретического материала. В текущей главе описаны некоторые дополнительные средства и план подготовки к экзамену.

Если читатель планирует сдавать сразу общий экзамен CCNA и читает оба тома книги, то он может заметить, что подобная глава есть также и во втором томе. Тем не менее для подготовки к экзамену достаточно прочитать всего одну из них, поскольку описываемые приложения, утилиты и методы подготовки — одни и те же в обеих главах. То, что относится к общему экзамену CCNA (код экзамена (640-802), а не к сертификационному экзамену ICND1 (640-816), выделено точно так же, как это предложение. Если читатель планирует сдавать для начала только второй экзамен, то соответствующие этапы подготовки он может пока пропустить.

В этой короткой главе есть два раздела: в первом описываются утилиты и программы для подготовки к экзамену, во втором предлагается некоторый план подготовки к сертификации.

ВНИМАНИЕ!

В этой главе есть ссылки на все главы книги и приложения, а также на программы и ресурсы, размещенные на прилагаемом к книге диске. Большая часть приложений к книге также размещена на компакт-диске. Чтобы воспользоваться ими, вставьте диск в соответствующий дисковод и выберите нужный ресурс из открывшегося интерфейса.

Утилиты для подготовки к экзамену

В этом разделе описаны утилиты и инструменты для подготовки к экзамену и рассказывается, как получить доступ к ним.

Программа для тестирования Pearson Cert и вопросы на компакт-диске

На прилагаемом компакт-диске есть программа для тестирования Pearson IT Certification Practice Test — приложение, выводящее набор вопросов, похожих на те, которые будут в сертификационном экзамене, и оценивающее полученный результат. В ней есть вопросы с многовариантным выбором ответа, вопросы с “перетаскиванием” правильных ответов, заполнение бланков и тестлеты. Используя тестовую

программу Pearson IT Certification Practice Test, вы можете либо проходить обучение в режиме Study Mode, либо моделировать экзамен ICND1 или CCNA, подражая реальным условиям экзамена.

Процесс установки приложения для тестирования состоит из двух этапов. На прилагаемом компакт-диске есть свежая версия тестового программного обеспечения Pearson IT Certification Practice Test. Самых вопросов для тестирования (для экзамена ICND1 и CCNA) на диске нет.

Установка программного обеспечения с компакт-диска

Тестовая программа Pearson IT Certification Practice Test — это приложение только для Windows. Вы можете запустить его и на Mac, используя виртуальную машину Windows Virtual Machine, но создана она специально для платформы PC. Минимальные системные требования приведены ниже.

- Операционная система Windows XP (SP3), Windows Vista (SP2) или Windows 7.
- Наличие Microsoft .NET Framework 4.0 Client.
- Наличие Microsoft SQL Server Compact 4.0.
- Процессор класса Pentium 1 ГГц (или эквивалентный).
- Наличие 512 Мбайт RAM.
- 650 Мбайт свободного пространства на диске плюс 50 Мбайт для каждого загруженного экзаменационного теста.

Процесс установки программного обеспечения вполне очевиден и похож на установку других программных продуктов. Если вы уже установили программное обеспечение Pearson IT Certification Practice Test при установке другого продукта от Pearson, нет никакой необходимости устанавливать его повторно. Просто запустите его на своем рабочем столе и перейдите к активации экзаменационных тестов из этой книги, используя код активации, полученный по электронной почте. Установка выполняется согласно следующим этапам.

Этап 1 Вставьте компакт-диск в дисковод своего компьютера.

Этап 2 Автоматически загрузится программное обеспечение компании Cisco Press, в котором можно загрузить программное обеспечение для эмуляции экзамена и приложения к этой книге, имеющиеся только на DVD. Тестовое программное обеспечение можно установить из главного меню (*Install the Exam Engine*).

Этап 3 Введите запрашиваемые параметры, как для любого другого программного обеспечения.

Процесс инсталляции позволит активировать тесты с помощью кода активации, полученного по электронной почте. Этот процесс требует регистрации на веб-сайте Pearson. Регистрация понадобится для активации тестов, поэтому зарегистрируйтесь, пожалуйста, когда попросят. Если регистрация на веб-сайте Pearson уже есть, повторно регистрироваться ненужно, используйте уже существующую регистрацию.

Загрузка и активация практического экзамена

Установив тестовое программное обеспечение, активируйте тесты данной книги следующим образом (если это не было сделано в процессе инсталляции).

-
- Этап 1** Запустите программное обеспечение Pearson IT Certification Practice Test (PCPT) в меню кнопки Пуск или щелчком на соответствующей пиктограмме на рабочем столе.
 - Этап 2** Чтобы загрузить и активировать тест, связанный с этой книгой, щелкните на кнопке **Activate** (Активировать) на вкладке **My Products** (Мои продукты) или **Tools** (Инструменты).
 - Этап 3** На следующем экране введите код активации, полученный вами по электронной почте. После ввода щелкните на кнопке **Activate**.
 - Этап 4** В процессе активации загрузится тест. Щелкните на кнопке **Next** (Далее), а затем на кнопке **Finish** (Готово).

По завершении процесса активации вкладка **My Products** (Мои продукты) будет содержать ваш новый экзамен. Если тест не виден, удостоверьтесь, что перешли на вкладку **My Products** (Мои продукты) в меню. Теперь программное обеспечение и тест готовы к использованию. Выберите тест и щелкните на кнопке **Open Exam** (Открыть тест).

Для обновления определенного теста, который уже активизирован и загружен, достаточно перейти на вкладку **Tools** (Инструменты) и щелкнуть на кнопке **Update Products** (Обновить продукты). Обновление тестов гарантирует наличие последних изменений и обновлений тестовых данных.

Если хотите проверить обновления тестового программного обеспечения Pearson Cert Practice Test, перейдите на вкладку **Tools** (Инструменты) и щелкните на кнопке **Update Application** (Обновить приложение). Это гарантирует наличие последней версии программного обеспечения.

Активизация других экзаменов

Установку и регистрацию тестового программного обеспечения нужно выполнить только один раз. Для каждого последующего варианта экзамена потребуется лишь несколько дополнительных действий. Например, если вы приобрели также второй том этой книги или Pearson IT Certification Cert Guide, запросите новый код активации по электронной почте (сам DVD уже не нужен). Теперь осталось только запустить тестовую программу (если она еще не запущена) и выполнить этапы 2–4 из предыдущего списка.

Издание Premium Edition

В дополнение к бесплатным экзаменационным заданиям, предоставляемым на DVD, можете купить дополнительные тесты с расширенными функциональными возможностями непосредственно у компании Pearson IT Certification. Электронная версия издания Premium Edition и экзаменационные задания для этой книги содержат дополнительно два полных комплекта экзаменационных заданий, а также электронную версию (в форматах PDF и ePub). Кроме того, издание Premium Edition содержит исправления по каждому вопросу, относящемуся к определенной части электронной книги.

Для просмотра страницы издания Premium Edition перейдите по адресу <http://www.pearsonitcertification.com/title/0132903822>.

Учебная сеть Cisco

Компания Cisco предлагает множество инструментов для подготовки к сертификационному экзамену CCNA, которые размещены на веб-сайте компании в разделе

учебная сеть Cisco (Cisco Learning Network — CLN). В этом разделе есть демонстрации интерфейса пользователя на экзамене, примеры вопросов и информационные видеоролики. Но самой большой ценностью является невероятно активный и полезный форум подготовки CCNA, где можно относительно быстро получить ответы на свои вопросы по подготовке.

Чтобы использовать сеть CLN, перейдите на веб-сайт learningnetwork.cisco.com и зарегистрируйтесь. (Это бесплатно.) Затем можно просмотреть весь сайт, но, вероятнее всего, наиболее интересными покажутся ссылки по CCENT и CCNA в левой части страницы. Можно принять участие в работе групп по изучению CCENT и CCNA, получать уведомления о каждом новом сообщении и, вообще, узнать очень много нового.

Учебные средства по подсетям

Умение анализировать IP-адреса протокола IPv4 — не единственный полезный навык, который проверяется в различных сертификационных экзаменах компании Cisco, в том числе и CCNA. В главе 12 описано практически все, что понадобится для решения задач по адресации. В главе 5 второго тома дополнительны описаны маски VLSM.

В этой книге есть несколько дополнительных ресурсов, которые помогут попрактиковаться в расчете подсетей.

- **Полезные советы.** В конце глав 13–18 предоставлено несколько советов по темам экзаменов. Следует быть не только осведомленным, но и быстрым. По завершении изучения книги читатель, вероятно, будет вполне способен создать подсеть. Таблицы, расположенные ближе к концу каждой главы, также помогут подготовиться к вопросам по созданию подсетей.
- **Видеоролики о процессе создания подсетей.** На компакт-диске, прилагаемом к книге, есть несколько видеороликов, демонстрирующих алгоритмы расчета для выполнения заданий по расчету подсетей. Ссылки на такие ролики доступны в простом меню, которое загружается после того, как пользователь вставит диск в дисковод своего компьютера.
- **Задания по расчету подсетей.** В приложениях Г – И, которые доступны только на компакт диске, содержатся дополнительные практические задания по созданию подсетей, кроме заданий в главах 13–18. Эти приложения предоставляют как задания, так и их решения с объяснениями.

Сценарии

Как было сказано во введении к этой книге, в некоторых экзаменационных вопросах задание построено так, что для его выполнения потребуется использовать подход, характерный для стандартных рабочих ситуаций в сетях. Разделы и главы по поиску и устранению неисправностей есть в обоих томах книги, и их основная цель — помочь в подготовке к практической работе и сдаче экзамена.

Альтернативный метод подготовки к решению задач на поиск и устранение неисправностей — проработать несколько практических сценариев, попробовать предсказать и проанализировать, что происходит в том или ином случае, и проверить, работает ли сеть так, как нужно. В приложении К представлены такие сцена-

рии, состоящие из нескольких заданий. Их следует попытаться решить, а потом просмотреть ответы в конце приложения. Читая сценарии и выполняя их задания, читатель сможет приобрести нужные навыки для анализа, поиска и устранения неисправностей в сетях.

План подготовки к экзамену

Чтобы подготовиться к экзамену, нужно использовать все дополнительные ресурсы, которые были перечислены выше. В этом разделе описан некоторый план подготовки к экзамену, который поможет оптимизировать процесс и затратить на него меньше усилий, чем если читатель будет непоследовательно использовать предложенные выше утилиты и ресурсы. Тем не менее этот план является не догмой, а скорее рекомендацией, и читатель может поступать по своему усмотрению.

Если читатель готовится к сдаче экзамена ICND1, он может пропустить выделенные части текста в плане. Если же план используется для подготовки к экзамену CCNA сразу по двум томам книги, на эти рекомендации следует обратить внимание.

В предлагаемом плане подготовки к экзамену все задачи разделены на четыре категории.

- **Повторение теории.** Задания, которые помогут вспомнить и запомнить детали различных технологий из 23 глав книги.
- **Практические задания по расчету подсетей.** Чтобы успешно сдать экзамены ICND1, ICND2 и CCNA, следует уметь быстро и правильно рассчитывать информацию для подсетей. Такие задания помогут развить необходимые навыки.
- **Практика в поиске и устранении неисправностей с помощью сценариев.** Чтобы ответить на некоторые вопросы экзаменов, где описана некая ситуация, читателю потребуется вспомнить теоретические основы технологии, уметь быстро и четко рассчитывать подсети, а также использовать лабораторный эмулятор оборудования. И все это — в одном задании.
- **ПО эмуляции экзамена для практики и тестирования.** Приложение, позволяющее потренироваться на вопросах, подобные которым будут встречаться в экзамене, есть на прилагаемом компакт-диске.

Повторение теории

Как и в большинстве экзаменов, для уверенной сдачи рассматриваемых сертификационных экзаменов нужно помнить множество фактов, концепций и определений. В этом разделе представлено несколько заданий, которые помогут читателю запомнить необходимую информацию.

- Этап 1** **Просмотрите и выполните повторно, если это необходимо, задания в разделе для подготовки к экзамену в каждой главе.** Эти разделы помогут освежить имеющиеся знания. Для подготовки к экзамену CCNA следует выполнить задания в главах 2–17 первого тома и в главах 1–17 — во втором.
- Этап 2** **Просмотрите и повторно ответьте на контрольные вопросы в начале каждой главы.** Несмотря на то что вопросы могут быть уже знакомы, повторное их прочтение поможет вспомнить важнейшие темы каждой главы. Эти вопросы затрагивают важные темы главы, и лишний раз повторить их не помешает.

Практические задания по расчету подсетей

Самое главное, что поможет читателю в успешной сдаче экзаменов ICND1, ICND2 и CCNA, несомненно, — умение быстро, безошибочно и аккуратно рассчитывать подсети. В экзамене CCNA самым критичным ресурсом является время, а больше всего его уходит на задания с эмуляцией командной строки оборудования, симплеты и на вопросы по расчету подсетей. Читателю нужно тренироваться в расчете сетей и подсетей до тех пор, пока он не сможет уверенно рассчитывать ответ за минимальное время.

Перед тем как предлагать метод подготовки к вопросам и заданиям по расчету подсетей, следует отметить, что существует много альтернативных методов поиска правильного ответа. Например, читатель может использовать двоичный метод для всех 32 битов адреса подсети. В качестве альтернативы он может наметанным глазом обнаружить, что 3 из 4 октетов адреса в большинстве вопросов по подсетям не требуют пересчета и их значение может быть предсказано без двоичной математики. Расчеты в таком случае нужно выполнять только для последнего октета. Еще один вариант — запомнить на память и использовать таблицу двоичных и десятичных значений. Таблица не требует проведения никаких расчетов, но ее нужно выучить наизусть. Можно использовать и другие методы, которые читатель мог найти в других книгах или услышать от преподавателя, если он проходил этот курс в очном варианте.

Независимо от того, какой процесс предпочтет читатель, в выбранном методе нужно тренироваться до тех пор, пока поиск ответа не будет занимать минимальное время.

Ниже приведен формальный список некоторой последовательности действий, которая поможет потренироваться в расчете подсетей, независимо от того, какой метод выбрал читатель.

- Этап 1** **Используйте приложения на компакт-диске для практики создания подсетей.** Главы 13–18 представляют математический механизм расчета создания подсетей; Приложения Г–И предоставляют дополнительные практические задания, соответствующие этим главам. Просто выньте компакт-диск из конверта, вставьте его в компьютер и запустите исполняемый файл. Затем ищите в меню приложения Г–И в формате PDF.
- Этап 2** **Просмотрите видеоролики по расчету подсетей на компакт-диске.** В этих видеороликах проиллюстрированы примеры использования нескольких методов расчета подсетей. Для подготовки к экзамену CCNA можно просмотреть видеоролики на компакт-диске только к первому или только ко второму тому книги. Видеоролики идентичны, поэтому нет смысла смотреть их дважды.
- Этап 3** **Практическая игра Cisco Binary Game.** На компакт-диске есть также экземпляр игры Cisco Binary Game, которая поможет овладеть бинарной математикой, включая преобразования двоичных 8-битовых чисел в десятичные, и наоборот. Если захочется осуществлять расчеты подсетей в двоичной форме, то эта игра может оказаться эффективным способом повышения квалификации, а также неплохим развлечением.
- Этап 4** **Используйте дополнительные задания с блога автора.** Вы можете найти ссылки на блоги Уэнделла на его веб-сайте www.certskills.com/blogs. Его блоги CCENT Skills и CCNA Skills содержат разнообразные публикации с дополнительными заданиями по созданию подсетей. В разделе “subnetting speed practice” его блога можно найти большое количество практических задач.
- Этап 5** **Разработайте собственные задания с помощью калькулятора подсетей.** Можете загрузить множество калькуляторов подсетей из Интернета. Или разработайте множество собственных заданий, похожих на те, что представлены в приложениях, посвященных созданию подсетей, а также решите их и проверьте правильность ответа с помощью калькулятора.

Этап 6 Компания Pearson (издатель этой книги) публикует также приложения для iPhone, помогающие изучать подсети. Ищите в хранилище приложений “subnet prep” или посетите сайт www.subnetprep.com.

Практика в поиске и устраниении неисправностей с помощью сценариев

Точно так же как и в реальной жизни, проблемы в сети могут быть вызваны многими причинами — протоколом маршрутизации, поврежденным кабелем, проблемами в протоколе распределенного связующего дерева, неправильными списками контроля доступа и даже ошибками в документации к сети. Поэтому на экзамене придется использовать все свои знания и практический опыт, чтобы ответить на некоторые вопросы. Чтобы улучшить свое умение искать и устранять причину неисправности, читателю следует выполнить следующее задание.

- **Просмотреть и выполнить задания приложения K.** Задания этого приложения оформлены в виде некоторого сценария, в котором приходится устранять проблемы, обсуждавшиеся в нескольких главах книги. Задания требуют более высокого уровня абстрактного мышления для их решения, чем другие примеры вопросов. Для подготовки к экзамену CCNA следует выполнить задания сценариев к обоим томам книги.

Подготовка к экзамену ICND1 640-822 или CCNA 640-802

Экзаменационные задания, прилагаемые к этой книге, позволяют попрактиковаться как в сдаче экзамена ICND1 640-822, так и полного экзамена CCNA 640-802. Вы можете выбрать набор экзаменационных вопросов в верхней части окна параметров, которое открывается при запуске приложения. Если хочется проверить себя только на вопросах экзамена ICND1, можно выбрать любой из наборов тестов ICND1. Обратите внимание: при выборе набора “Book Questions” можно будет получить доступ ко всем вопросам, которые имеются в печатной версии книги. Если задания из книги желательно исключить из проверки, выберите один или несколько других экзаменационных заданий ICND1. Если желательно проверить себя на полном экзамене CCNA (который включает вопросы и по ICND1, и по ICND2), выберите набор заданий CCNA 640-802. Если необходима проверка по полному экзамену CCNA, рекомендуется сбросить все параметры, установленные для экзамена ICND1.

Кроме набора заданий, вопросы из которого будут выбраны случайным образом, можно также настроить проверку так, чтобы сосредоточиться только на определенных темах экзамена. Для этого следует установить или сбросить соответствующие задачи в окне параметров.

Как только набор заданий будет выбран, можно выбрать необходимый режим практики. Для этого в раскрывающемся меню параметров вверху окна выберите режим *Study Mode* (Режим обучения) или *Practice Exam Mode* (Режим экзамена). Режим обучения позволяет задать период времени, отведенный на сдачу экзамена, количество задаваемых вопросов, должны ли вопросы быть упорядочены или следовать в случайному порядке, нужно ли отображать только отмеченные или все вопросы. Можно будет также перебирать вопросы вперед-назад, просматривать ответы и вообще использовать все средства. Этот режим следует использовать при подготовке к экзамену, поскольку он обеспечивает максимальную гибкость в настройке и позволяет немедленно узнать

результат ответа на каждый вопрос. Если выбрать режим экзамена, то параметры будут сразу заданы так, чтобы подражать настоящей экзаменационной системе, поэтому не получится изменить время и объем вопросов, возвращаться к предыдущим вопросам или просматривать ответы на отдельные вопросы. Этот режим следует использовать тогда, когда чувствуешь себя уверенно и готов сдать экзамен, чтобы проверить свою готовность к успешной сдаче фактического экзамена.

Резюме

Все приложения и инструменты, которые были описаны в этой главе, преследуют единственную цель: помочь читателю в подготовке к экзаменам ICND1 и CCNA. Эта книга, а также второй том курса предназначены для того, чтобы дать читателю хорошую теоретическую основу для практической работы и научить применять теоретические знания на практике. Не важно, каков опыт работы читателя с соответствующими технологиями и оборудованием на момент сдачи экзамена. Если читатель прочитает всю книгу, досконально изучит материал и потренируется с помощью предложенных ему методик и утилит, он сможет уверенно сдать экзамен. Автор искренне желает каждому прочитавшему книгу успешно сдать соответствующие сертификационные экзамены.

Часть VII. Приложения (в книге)

Приложение А. “Ответы на контрольные вопросы”

Приложение Б. “Справочные числовые таблицы”

Приложение В. “Обновление экзамена ICND1: версия 1.0”

ПРИЛОЖЕНИЕ А

Ответы на контрольные вопросы

Глава 2

Знаете ли вы уже темы главы

1. г) и е)
2. а) и ж)
3. б) Взаимодействие на смежных уровнях происходит в одном компьютере, когда два расположенных рядом уровня чем-либо обмениваются. Обычно верхний уровень запрашивает какую-либо службу у нижнего, а нижний предоставляет какие-то услуги верхнему.
4. б) Взаимодействие одинаковых уровней происходит между разными компьютерами, поскольку выполняемая функция требует наличия более чем одного участника. Например, передающий узел устанавливает порядковый номер сегмента, а принимающий генерирует для него соответствующий номер подтверждения. Функции и процессы выполняются на одном и том же уровне в рамках какой-либо модели, но реализация такого уровня должна быть одинакова в разных устройствах.
5. а) Инкапсуляция — это процесс добавления заголовка в начале блока данных, полученных от вышестоящего уровня (и, возможно, концевика).
6. г)
7. в)
8. а)
9. е)
10. в) и д) В модели OSI есть транспортный и сетевой уровни, но нет уровня Интернета.

Глава 3

Знаете ли вы уже темы главы

1. г)
2. а)
3. б)
4. б), г) и д) В маршрутизаторах, беспроводных точках доступа и сетевых картах персональных компьютеров контакты 1 и 2 портов Ethernet используются для

передачи данных, а в коммутаторах — контакты 3 и 6. Прямые кабели используются для подключения устройств, в которых используются разные контакты для передачи данных.

5. б)
6. а)
7. а) и в)
8. в) и г)
9. а)
10. б), в) и д)
11. в)

Глава 4

Знаете ли вы уже темы главы

1. б)
2. б) Четырехжильный кабель, предоставляемый телефонной компанией, подключается к устройству, выступающему в роли модуля CSU/DSU. Это может быть внешний модуль CSU/DSU или интегрированный в плату последовательного интерфейса маршрутизатора. У коммутатора LAN нет последовательных интерфейсов, а у последовательных интерфейсов маршрутизатора нет трансиверов.
3. б)
4. а)
5. д)
6. д) В протоколе HDLC есть поле адреса в заголовке, но оно не используется в двухточечных каналах, поскольку есть только один получатель в таком канале.
7. а)
8. б) Одно из основных преимуществ технологии Frame Relay состоит в том, что к маршрутизатору может быть подключен один физический канал, в котором есть множество логических подканалов, каждый из которых может использоваться для пересылки данных разным дистанционным маршрутизаторам. Чтобы идентифицировать разные логические каналы, используются различные идентификаторы канального уровня — DLCI.

Глава 5

Знаете ли вы уже темы главы

1. а) и в) Сетевой уровень задает структуру логической адресации, которая является иерархической в отличие от физической. Логическое упорядоченное построение адресной схемы позволяет легко группировать адреса в блоки и таким образом оптимизировать адресацию. Выбором пути называется процесс поиска оптимального маршрута в сети.
2. в) и д)

3. а)
4. б) 224.1.1.1 — это адрес сети класса D, адрес 223.223.223.255 — широковещательный для подсети класса C с адресом 223.223.223.0, поэтому они не могут быть назначены хостам.
5. г)
6. г) и е) Если не используются подсети, все адреса относятся к сети класса A, 10.0.0.0. Если в сети есть маршрутизатор и хосты находятся в другом сегменте (подключены к другому его порту), они не могут иметь адреса из сети 10.0.0.0.
7. г)
8. е)
9. в)
10. б) и в)
11. а) и в)
12. в)
13. г)

Глава 6

Знаете ли вы уже темы главы

1. г) Компьютер ПК1 интерпретирует отсутствие подтверждения как свидетельство того, что он не знает, получил ли компьютер ПК2 любой из сегментов. В результате компьютер ПК1 снова посыпает все сегменты.
2. г)
3. г) и д)
4. г) и д)
5. в) Протокол TCP, а не UDP использует механизм скользящего окна, восстановление после ошибок и упорядоченную передачу сегментов. Шифрование или маршрутизацию оба протокола транспортного уровня не выполняют.
6. в) и е) Термины *пакет* и *L3PDU* описывают блок данных третьего уровня. Термины *фрейм* и *L2PDU* относятся ко второму уровню эталонной модели.
7. б) Имя хоста — это текст между косыми черточками (// и /). Текст перед символами // описывает используемый протокол уровня приложений, а текст после символа / — название веб-страницы.
8. а) и г) Потоки данных технологии VoIP наиболее чувствительны к задержкам, их флуктуации и потерям пакетов; чем меньше задержки, флуктуации и потери, тем лучше. Тем не менее потоки VoIP обычно требуют меньшей полосы пропускания, чем потоки обычных данных.
9. в) Системы обнаружения вторжений (IDS) выполняют мониторинг пакетов, сравнивая их содержимое с известными комбинациями (т.е. сигнатурами), по которым они могут определить, что происходит атака на сеть.
10. а) Виртуальная частная сеть (VPN) — это технология безопасности, в которой две оконечные точки канала (в том числе и логического) шифруют данные, пе-

ред тем как передать их по какой-либо открытой инфраструктуре, например по Интернету, чтобы обеспечить конфиденциальность и целостность данных.

Глава 7

Знаете ли вы уже темы главы

1. а) Коммутатор сравнивает адрес получателя со своей таблицей МАС-адресов. Если найдена совпадающая запись, коммутатор знает, через какой интерфейс отправить фрейм дальше, если не найдена — лавинно рассыпает через все порты, кроме того, откуда он пришел.
2. в) Коммутатор рассыпает лавинно широковещательные, многоадресатные (если не используется оптимизация многоадресатных потоков) и фреймы с адресом получателя, который устройству неизвестен (т.е. адрес получателя фрейма отсутствует в таблице МАС-адресов коммутатора).
3. а) Коммутатор рассыпает лавинно широковещательные, многоадресатные (если не используется оптимизация многоадресатных потоков) и фреймы с адресом получателя, который устройству неизвестен (т.е. адрес получателя фрейма отсутствует в таблице МАС-адресов коммутатора).
4. б) Коммутатор строит таблицу МАС-адресов, обнаруживая и запоминая адрес отправителя из каждого приходящего фрейма, а также учитывает интерфейс, через который был получен такой фрейм. Таблица МАС-адресов, соответственно, содержит информацию о МАС-адресе и интерфейсе, через который он был принят.
5. а) и б) Когда фрейм, отправленный устройством ПК3, попадает в коммутатор, у последнего есть в таблице только адрес 1111.1111.1111, МАС-адрес ПК1. Фрейм от ПК3 адресован устройству с МАС-адресом 2222.2222.2222, поэтому он рассыпается лавинным образом, т.е. пересыпается через все интерфейсы, кроме того, откуда пришел фрейм.
6. а) Домен коллизий представляет собой совокупность устройств, фреймы которых могут сталкиваться. Мосты, коммутаторы и маршрутизаторы разделяют, или сегментируют, локальную сеть на меньшие по размеру домены коллизий, а концентраторы и повторители — нет.
7. а), б) и в) Широковещательный домен состоит из устройств, широковещательные фреймы которых могут достигать друг друга. Концентраторы, повторители, мосты и коммутаторы не разделяют (сегментируют) локальную сеть на отдельные широковещательные домены, а маршрутизаторы разделяют.
8. б) и г)

Глава 8

Знаете ли вы уже темы главы

1. а) и б)
2. б)
3. б)
4. а)

5. е)
6. г)
7. б) и в)

Глава 9

Знаете ли вы уже темы главы

1. б) Если указаны обе команды, операционная система Cisco IOS использует пароль, указанный в команде `enable secret`.
2. б) и в)
3. б) Первый символ, не являющийся пробелом, после команды `banner login` будет интерпретирован как символ-разделитель. В данном случае это будет буква “t” в слове “this”, а вторая буква “t” встречается в слове “the” и будет интерпретирована как конец сообщения. В результате при подключении к устройству будет выводиться текст, находящийся между двумя буквами “t”, а именно “his is”.
4. а) Стандартная настройка максимального количества MAC-адресов в режиме безопасности — 1, следовательно, команду `switchport port-security maximum` вводить не нужно.
5. а), г) и е) Чтобы разрешить доступ к устройству через протокол Telnet, в коммутаторе должны быть установлены пароли. Минимальное требование — должен быть установлен пароль на линии `vty` с помощью команды `password`. Кроме того, следует настроить IP-адрес в устройстве (в интерфейсе VLAN 1) и указать стандартный шлюз, чтобы коммутатор мог обмениваться пакетами с хостами из других подсетей.
6. е)
7. д)
8. а) Регистр названия сети VLAN учитывается операционной системой, поэтому команда `name MY-VLAN` установит другую сеть VLAN, отличающуюся от показанной в конфигурации. Команда `interface range` не могла быть использована для конфигурирования, поскольку она позволяет ввести в виртуальную сеть интерфейсы Fa0/13, Fa0/14 и Fa0/15, а порт Fa0/14 не входит в показанную сеть VLAN. Чтобы присвоить порту сеть VLAN, должна быть введена команда `switchport access vlan 2`, а команда `switchport vlan 2` — неправильная.

Глава 10

Знаете ли вы уже темы главы

1. д) и е) Протокол CDP собирает информацию о смежных устройствах, а с помощью команды `show cdp` с разными опциональными параметрами можно увидеть более или менее подробную информацию.
2. д) и е)

3. а), б) и г) Если в выводе команды `show interfaces status` указано отключенное состояние интерфейса (`disabled`), то это свидетельствует о том, что порт административно отключен и в выводе команды `show interfaces` будет отображаться строка “`administratively down/down`”. Интерфейс должен быть в подключенном состоянии (`connect`), чтобы устройство могло пересыпать через него фреймы.
4. а) и г) В коммутаторе SW2 была отключена система автоматического согласования параметров интерфейса стандарта IEEE, когда были вручную установлены скорость и дуплексность. Тем не менее коммутаторы компании Cisco могут определить скорость и режим работы дистанционного порта даже при отключенном автосогласовании. Кроме того, согласно стандарту IEEE для скорости передачи 1 Гбит/с используется дуплексный режим, если режим дуплексности не может быть согласован, поэтому соединение в любом случае будет нормально функционировать, поскольку на обоих концах канала используется скорость 1 Гбит/с и дуплексный режим.
5. б) и г) С помощью команды `show interfaces` можно просмотреть текущую скорость работы и режим дуплексности интерфейса, но нельзя сказать, какая скорость была согласована или указана в конфигурации. В выводе команды `show interfaces status` может быть показан префикс `a-` перед значением скорости и режимом дуплексности; он означает, что скорость и режим были автоматически согласованы. В противном случае параметры были заданы вручную в конфигурации.
6. а), б) и г) Для порта Fa0/1 автосогласование должно правильно отработать, и оба коммутатора выберут наибольшую скорость (100) и наилучшие настройки дуплексности (полнодуплексный режим). Автосогласование также отработает в порту Fa0/2 коммутатора SW1, и оба устройства будут использовать скорость в 100 Мбит/с и полнодуплексный режим. В интерфейсе Fa0/2 отключена процедура автосогласования, поскольку скорость и режим заданы вручную. Коммутатор на втором конце канала автоматически обнаружит скорость 100 Мбит/с, но включит полу duplexный режим, и соединение не будет работать.
7. б) Команда вывела только две записи, и обе для виртуальной сети VLAN 1. Команда `show mac address-table` отобразила динамические записи таблицы MAC-адресов для всех сетей VLAN. Таким образом, вы можете установить, что в таблице MAC-адресов нет никаких записей для сети VLAN 2. В результате коммутатор пересыпает фрейм во все порты сети VLAN 2, кроме того порта, с которого поступил фрейм. С точки зрения обучения, поскольку порт Fa0/3 находится в сети VLAN 2, коммутатор, не имея записи в таблице MAC-адресов для адреса 0200.1111.1111 в сети VLAN 2, добавит запись для сети VLAN 2, адреса 0200.1111.1111 и интерфейса Fa0/3.
8. б) и в) Операционная система IOS добавляет MAC-адреса в безопасном режиме порта в виде статических записей, поэтому они не отображаются в выводе команды `show mac address-table dynamic`. Команда `show mac address-table port-security` — неправильная.

Глава 11

Знаете ли вы уже темы главы

1. а) В стандарте 802.11a используется диапазон частот U-NNI (порядка 5,4 ГГц), а в стандарте 802.11b и 802.11g — диапазон ISM (порядка 2,4 ГГц). Стандарт 802.11i — это стандарт безопасности беспроводных сетей.
2. б) В стандарте 802.11a используется только модуляция OFDM, а в 802.11b — только DSSS. В стандарте 802.11g максимальная скорость передачи равна 54 Мбит/с и используется модуляция OFDM.
3. в)
4. а) В расширенном наборе служб (ESS) используется несколько точек доступа и возможен роуминг между ними. В сети BSS используется только одна точка доступа, а в режиме IBSS точек доступа нет вообще. Следовательно, роуминг невозможен в сетях BSS и IBSS.
5. а) и в) В точках доступа должен быть настроен идентификатор SSID, и если точка поддерживает несколько стандартов, то может быть указан используемый стандарт беспроводной сети. Точка доступа всегда пытается использовать максимальную скорость передачи для каждого из устройств в зависимости от уровня сигнала, тем не менее, скорость может отличаться от устройства к устройству. Размер области покрытия точки настроить нельзя, он зависит от типа антенны, ее коэффициента усиления, интерференции и используемого стандарта беспроводной сети.
6. б) Точка доступа подключается к коммутатору локальной сети прямым кабелем, как любое оконечное устройство. Все точки доступа в одной сети ESS также должны входить в одну и ту же сеть VLAN, поскольку все клиенты в такой беспроводной сети должны быть в одной подсети. Как и коммутаторам локальной сети, точкам доступа не нужна конфигурация IP, чтобы пересыпать трафик, но IP-адрес можно настроить для управления точкой. Стандарт или скорость передачи данных в беспроводной сети не влияет на скорость работы порта Ethernet в проводной части сети точки доступа, тем не менее, общая производительность будет выше, если в высокоскоростных беспроводных сетях используется технология Ethernet со скоростью 100 Мбит/с.
7. в) и г) Интерфейсы Ethernet обычно не дают интерференции в беспроводной радиочастотной части, поэтому кабельная сеть не влияет на сеть WLAN. Клиентские устройства обнаруживают точки доступа, прослушивая все каналы, поэтому конфигурирование какого-то определенного канала не помешает клиенту обнаружить точку доступа.
8. б) и г) Это стандарт IEEE 802.11i. Альянс Wi-Fi дал этому стандарту маркетинговое название WPA2.
9. а), в) и г)

Глава 12

Знаете ли вы уже темы главы

1. б) и г). Общее правило, чтобы определить, должны ли интерфейсы двух устройств быть в той же подсети или нет, — это выяснить, отделяются ли два ин-

терфейса друг от друга маршрутизатором. Чтобы предоставить хостам в одной сети VLAN путь для отправки данных хостам вне этой VLAN, интерфейс LAN локального маршрутизатора должен быть подключен к той же сети VLAN, что и хост, а также иметь адрес в той же подсети, что и хосты. Все хосты в той же сети VLAN на том же коммутаторе не будут отделены друг от друга маршрутизатором, поэтому все эти хосты также будут в той же подсети. Однако другой компьютер, подключенный к тому же коммутатору, но находящийся в другой сети VLAN, потребует прохождения своих пакетов через маршрутизатор, чтобы они достигли хоста А. Таким образом, IP-адрес хоста А должен находиться в подсети, отличной от подсети этого нового хоста.

2. г). По определению два адреса в каждой подсети IPv4 не могут использоваться как адреса хостов: первое (самое низкое) числовое значение в подсети — это идентификатор подсети, и последнее (самое высокое) числовое значение в подсети — это широковещательный адрес подсети.
3. б) и в). Необходимо по крайней мере 7 битов подсети, поскольку $2^6 = 64$; всего 6 битов подсети не обеспечит 100 различных подсетей, а 7 битов — вполне, так как $2^7 = 128 \Rightarrow 100$. Аналогично 6 битов хоста недостаточно, поскольку $2^6 - 2 = 62$, но 7 битов хоста вполне достаточно, так как $2^7 - 2 = 126 \Rightarrow 100$. Общее количество битов сети, подсети и хоста должно составлять 32 бита, поэтому один из ответов неправильный. Ответ с 8 битами сети не может быть правильным, поскольку вопрос утверждает, что используется сеть класса В, поэтому количеством битов сети всегда должно быть 16. У двух правильных ответов 16 битов сети (так как в вопросе указана сеть класса В) и по крайней мере 7 битов для подсетей и хостов в каждом.
4. а) и в). Документом RFC 1918 определены следующие частные сети IPv4: сеть класса А 10.0.0.0, 16 сетей класса В (от 172.16.0.0 до 172.31.0.0) и 256 сетей класса С, начинающиеся с 192.168.
5. а), г) и д). Документом RFC 1918 определены следующие частные сети IPv4: сеть класса А 10.0.0.0, 16 сетей класса В (от 172.16.0.0 до 172.31.0.0) и 256 сетей класса С, начинающиеся с 192.168. Три правильных ответа относятся к диапазону открытых сетей IP и не к зарезервированным значениям.
6. а) и в). У сетей класса А, В и С без подсетей есть две части: сети и хоста.
7. б). У сетей класса А, В и С без подсетей есть две части: сети и хоста. Для создания подсетей инженер создает новую часть подсети, заимствуя биты хоста и сокращая их количество. Часть подсети в структуре адреса появляется только после того, как инженер выберет нестандартную маску. Размер части сети останется прежним.
8. в) и г). *Идентификатор подсети* (Subnet ID — сокращение от subnet identifier), *адрес подсети* (subnet address) и *номер подсети* (subnet number) — это синонимы, относящиеся к числу, которое идентифицирует подсеть. Фактическое значение — это разделенное точками десятичное число, поэтому термин *имя подсети* (subnet name) неприменим. Термин *широковещательный адрес подсети* (subnet broadcast) — это синоним термина *широковещательный адрес подсети* (subnet broadcast address). Он относится к последнему (самому высокому) числовому значению в адресе подсети.

Глава 13

Знаете ли вы уже темы главы

1. б) и в). Сетевые идентификаторы сети класса А имеют первый октет в диапазоне 1–126 и нули в последних трех октетах. Адрес 130.0.0.0 — это фактически сеть класса В (диапазон первого октета от 128 до 191 включительно). Все адреса, которые начинаются с 127, зарезервированы, поэтому адрес 127.0.0.0 — это не сеть класса А.
2. д). Все адреса сети класса В начинаются со значения в диапазоне от 128 до 191 включительно в первом октете. В первом октете идентификатора сети может быть любое значение в диапазоне 128–191 и любое значение в диапазоне от 0 до 255 включительно во втором октете, с десятичными нулями в последних двух октетах. Во втором октете двух из ответов находится 255, что вполне приемлемо. Во втором октете двух из ответов находится 0, что также приемлемо.
3. б) и г). Первый октет (172) находится в диапазоне адресов (128–191) сети класса В. В результате идентификатор сети может быть сформирован при копировании первых двух октетов (172.16) и заполнен нулями последних двух октетов (172.16.0.0). Для всех сетей класса В по умолчанию задана маска 255.255.0.0, а количество битов хоста во всех не разделенных на подсети сетях класса В составляет 16.
4. а) и в). Первый октет (192) находится в диапазоне адресов (192–223) сети класса С. В результате идентификатор сети может быть сформирован при копировании первых трех октетов (192.168.6) и заполнен нулями последнего октета (192.168.6.0). Для всех сетей класса С по умолчанию задана маска 255.255.255.0, а количество битов хоста во всех не разделенных на подсети сетях класса С составляет 8.
5. г). Для поиска широковещательного адреса сети выясните сначала ее класс, а затем определите количество октетов хоста. Затем преобразуйте октеты хоста в 255, чтобы получить широковещательный адрес сети. В данном случае адрес 10.1.255.255 находится в сети класса А с тремя последними октетами хоста для широковещательного адреса сети 10.255.255.255. Адрес 192.168.255.1 — это адрес сети класса С с последним октетом как часть хоста для широковещательного адреса сети 192.168.255.255. Адрес 224.1.1.255 принадлежит сети класса D, а следовательно, не находится ни в какой одноадресатной сети IP, поэтому вопрос к нему неприменим. Адрес 172.30.255.255 — это адрес сети класс В с последними двумя октетами хоста. Таким образом, широковещательный адрес этой сети — 172.30.255.255.
6. б). Для поиска идентификатора сети выясните сначала ее класс, а затем определите количество октетов хоста. Затем преобразуйте октеты хоста в нули, чтобы получить идентификатор сети. В данном случае адрес 10.1.0.0 находится в сети класса А, с тремя последними октетами хоста для идентификатора сети 10.0.0.0. Адрес 192.168.1.0 — это адрес сети класса С с последним октетом как часть хоста для идентификатора сети 192.168.1.0. Адрес 127.0.0.0 выглядит как идентификатор сети, но начинается с зарезервированного значения (127), поэтому он не находится ни в какой сети класса А, В, или С. Адрес 172.20.0.1 — это адрес сети класса В с последними двумя октетами хоста, таким образом, идентификатор этой сети — 172.20.0.0.

Глава 14

Знаете ли вы уже темы главы

1. в). Рассмотрим преобразование по одному октету за раз. Каждый из первых двух октетов преобразуется в 8 двоичных единиц. Число 254 преобразуется в 8-битовое двоичное значение 11111110, а десятичное число 0 преобразуется в 8-битовое двоичное число 00000000. В результате полное количество двоичных единиц, определяющих длину префикса, составляет $8+8+7+0 = /23$.
2. б). Рассмотрим преобразование по одному октету за раз. Каждый из первых трех октетов преобразуется в 8 двоичных единиц. Число 240 преобразуется в 8-битовое двоичное значение 11110000. В результате полное количество двоичных единиц, определяющих длину префикса, составляет $8+8+8+4 = /28$.
3. а). Рассмотрим преобразование по одному октету за раз. Каждый из первых двух октетов преобразуется в 8 двоичных единиц. Число 192 преобразуется в 8-битовое двоичное значение 11000000, а десятичное число 0 преобразуется в 8-битовое двоичное число 00000000. В результате полное количество двоичных единиц, определяющих длину префикса, составляет $8+8+2+0 = /18$.
4. в). Значение /24 — это эквивалент маски, содержащей 24 двоичные единицы. Чтобы преобразовать маску в формат DDN, напишите все двоичные единицы (в данном случае 24), а остаток до 32-го разряда дополните двоичным нулями. Затем берите по 8 битов за раз и пересчитайте их из двоичной системы в десятичную (либо запомните девять возможных значений октета маски DDN и их двоичные эквиваленты). Значение маски /24 в двоичном виде составит 11111111 11111111 11111111 00000000. Поскольку каждый из первых трех октетов состоит целиком из двоичных единиц, они преобразуются в 255. Последний октет состоит целиком из двоичных нулей, он преобразуется в десятичное число 0. В результате получится маска DDN 255.255.255.0. Таблица десятично-двоичных преобразований приведена в приложении Б.
5. б). Значение /30 — это эквивалент маски, содержащей 30 двоичных единиц. Чтобы преобразовать маску в формат DDN, напишите все двоичное единицы (в данном случае 30), а остаток до 32-го разряда дополните двоичным нулями. Затем берите по 8 битов за раз и пересчитайте их из двоичной системы в десятичную (либо запомните девять возможных значений октета маски DDN и их двоичные эквиваленты). Значение маски /30 в двоичном виде составит 11111111 11111111 11111111 11111100. Поскольку каждый из первых трех октетов состоит целиком из двоичных единиц, они преобразуются в 255. Последний октет, 11111100, преобразуется в десятичное число 252. В результате получится маска DDN 255.255.255.252. Таблица десятично-двоичных преобразований приведена в приложении Б.
6. б). Значение /21 — это эквивалент маски, содержащей 21 двоичную единицу. Чтобы преобразовать маску в формат DDN, напишите все двоичное единицы (в данном случае 21), а остаток до 32-го разряда дополните двоичным нулями. Затем берите по 8 битов за раз и пересчитайте их из двоичной системы в десятичную (либо запомните девять возможных значений октета маски DDN и их двоичные эквиваленты). Значение маски /21 в двоичном виде составит 11111111 11111111 11111111 11110000 00000000. Поскольку каждый из первых двух октетов состоит целиком из двоичных единиц,

они преобразуются в 255. Третий октет, 11111000, преобразуется в 248. Последний октет состоит целиком из двоичных нулей, он преобразуется в десятичное число 0. В результате получится маска DDN 255.255.248.0. Таблица десятично-двоичных преобразований приведена в приложении Б.

Глава 15

Знаете ли вы уже темы главы

1. в). Размер части сети всегда составляет 8, 16 бит или 24 бита, в зависимости от класса сети А, В или С соответственно. Поскольку адрес класса А — N=8. Маска 255.255.255.0 преобразуется в префикс /24. Количество битов подсети — разница между длиной префикса (24) и N, поэтому в данном случае S=16. Размер части хоста — это число, которое, будучи добавлено к длине префикса (24), даст 32, таким образом, H=8 в данном случае.
2. а). Размер части сети всегда составляет 8, 16 бит или 24 бита, в зависимости от класса сети А, В или С соответственно. Поскольку адрес класса С — N=24. Количество битов подсети — разница между длиной префикса (27) и N, поэтому в данном случае S=3. Размер части хоста — это число, которое, будучи добавлено к длине префикса (27), даст 32, таким образом, H=5 в данном случае.
3. д). Размер части сети всегда составляет 8, 16 бит или 24 бита, в зависимости от класса сети А, В или С соответственно. Поскольку адрес класса В, битов сети будет 16. Маска 255.255.255.128 преобразуется в префикс /25. Количество битов подсети — разница между длиной префикса (25) и N, поэтому в данном случае S=9. Размер части хоста — это число, которое, будучи добавлено к длине префикса (25), даст 32, таким образом, H=7 в данном случае.
4. б) и г). Правила бесклассовой адресации определяют структуру IP-адреса с двумя частями: префикса и хоста. Часть хоста определяется так же, как и при классовой IP-адресации. Длина префикса по правилам бесклассовой адресации — это совместная длина частей сети и подсети при использовании концепции классовой IP-адресации. Математически длина префикса равна количеству двоичных единиц в маске. В данном случае при маске 255.255.255.0 длина префикса составит 24 бита. Длина части хоста — это количество битов, добавленных к 24, чтобы получилось 32, т.е. 8 битов.
5. г). Правила бесклассовой адресации определяют структуру IP-адреса с двумя частями: префикса и хоста. Эта логика игнорирует правила классов А, В и С, она может быть применена к 32-разрядным IPv4-адресам от любого класса. При игнорировании правил класса А, В и С бесклассовая адресация игнорирует любые различия между частями сети IPv4-адреса.
6. а) и б). Маски в двоичном представлении определяют количество двоичных единиц, выделяющих длину части префикса (сеть + подсеть). В сети класса В часть сети составляет 16 битов. Для поддержки 100 подсетей часть подсети должна быть по крайней мере 7 битов длиной. Шесть битов подсети составили бы только $2^6 = 64$ подсетей, а 7 битов подсети составят $2^7 = 128$ подсетей. Ответ: префикс /24 предоставит 8 битов подсети, маска 255.255.255.252 предоставит 14 битов подсети.

Глава 16

Знаете ли вы уже темы главы

1. а). При 50%-ном росте маска должна определять достаточно много битов подсети, чтобы создать 150 подсетей. В результате маска нуждается по крайней мере в 8 битах подсети (7 битов подсети составляет 2^7 , или 128 подсетей, а 8 битов подсети составляет 2^8 , или 256 подсетей). Аналогично потребность в 50%-ном росте размера наибольшей подсети означает, что часть хоста нуждается в достаточном количестве битов для 750 хостов на подсеть. Девяти битов хоста недостаточно ($2^9 - 2 = 510$), а 10 битов хоста обеспечат 1022 хоста на подсеть ($2^{10} - 2 = 1022$). При 16 битах сети, поскольку решено использовать сеть класса В, проект нуждается суммарно в 34 битах маски (16 для сети, 8 для подсети, 10 для хостов), но всего битов только 32, поэтому никакая единая маска не отвечает требованиям.
2. б). У сети класса С размер части сети составит 24 бита адреса, для подсети или хоста остается только 8 битов. При потребности в 12 подсетях 3 битов подсети недостаточно ($2^3 = 8$), но 4 бита подсети предоставят 16 подсетей ($2^4 = 16$). Аналогично 3 бита хоста не обеспечат достаточно хостов на подсеть ($2^3 - 2 = 6$), а 4 бита хоста предоставят 14 хостов на подсеть ($2^4 - 2 = 14$). В сумме 24 бита части сети плюс минимальные размеры частей подсети (4) и хоста (4) составят 32. Требованиям отвечает только одна маска — /28.
3. б). При 20%-ном росте проект должен обеспечить 240 подсетей. Для удовлетворения этой потребности 7 битов подсети недостаточно ($2^7 = 128$), а 8 вполне хватит ($2^8 = 256$). Аналогично минимум битов хоста также 8, поскольку после 20%-ного роста потребуется 144 хоста на подсеть. Для этого нужно 8 битов хоста ($2^8 - 2 = 254$). Это минимальные количества битов хоста и подсети. У правильного ответа, 10.0.0.0/22, есть 8 битов сети (поскольку это сеть класса А), 14 битов подсети (/22 – 8 = 14) и 10 битов хоста ($32 - 22 = 10$). Мaska предоставляет по крайней мере 8 битов подсети и по крайней мере 8 битов хоста. Маски в других ответах не предоставляют либо 8 битов хоста, либо 8 битов подсети.
4. б). Для выбора маски с максимальным количеством хостов используют маску с минимальным количеством битов подсети, что в свою очередь максимизирует количество битов хоста. В данном случае проект требует 1200 подсетей. 10 битов подсети не обеспечат достаточно подсетей ($2^{10} = 1024$), а 11 битов — вполне ($2^{11} = 2048$). Проект использует сеть класса А с 8 битами сети. Префиксная маска /19 (8 сетей плюс как минимум 11 битов подсети) является самой короткой маской, которая отвечает требованиям, оставляя 13 битов хоста для 8190 хостов на подсеть.
5. б). Для обеспечения 1000 подсетей необходимо 10 битов подсети ($2^{10} = 1024$). Проект использует сеть класса В, а значит, 16 битов сети уже занято. Так, самая короткая маска, которая отвечает требованиям, это 255.255.255.192, или /26, состоящая из 16 битов сети плюс 10 битов подсети. Ответ /28 также предоставляет достаточно подсетей, удовлетворяя потребности, но по сравнению с маской /26, маска /28 обеспечивает меньше битов хоста, следовательно, хостов на подсеть будет меньше.
6. д). Для обеспечения 10 подсетей необходимо 4 бита подсети, поскольку $2^3 = 8$, 3 битов недостаточно, а $2^4 = 16$, следовательно, достаточно 4 битов. Проект ис-

пользует сеть класса С, значит, существуют также 24 бита сети. Так, самая короткая маска, которая отвечает требованиям, это 255.255.255.240, или /28, состоящая из 24 битов сети, 4 битов подсети и 4 битов хоста. В ответах нет маски /28, из представленных только у маски 255.255.255.248 (/29) достаточно битов подсети. Другие ответы предоставляют 0 битов подсети (255.255.255.0), 1 бит подсети (/25), 2 бита подсети (255.255.192.0) и 3 бита подсети (/27).

7. г). Для выбора маски с максимальным количеством подсетей используют маску с минимальным количеством битов хоста, что в свою очередь максимизирует количество битов подсети. В данном случае проект требует 200 хостов на подсеть. Семь битов хоста не обеспечат достаточно хостов в подсете ($2^7 - 2 = 126$), а 8 битов — вполне ($2^8 - 2 = 254$). Проект использует сеть класса А с 8 битами сети. Префиксная маска /24 (маска с 8 битами хоста, необходимым минимумом для обеспечения достаточного количества хостов на подсеть) максимизирует размер части подсети, в данном случае предоставляет 16 битов подсети.

Глава 17

Знаете ли вы уже темы главы

1. г). При использовании классовых концепций IP-адресации, описанных в главе 15, у адресов есть три части: сети, подсети и хоста. Для адресов в одной классовой сети часть сети должна быть идентична у всех адресов в той же сети. Для адресов в той же подсете части сети и подсети должны иметь идентичные значения. Часть хоста различных адресов в той же подсете является индивидуальной.
2. б) и г). Идентификатор подсети в любой подсете — это наименьшее число в диапазоне, широковещательный адрес подсети — наибольшее, а пригодные для использования IP-адреса находятся между ними. У всех адресов в подсете идентичные двоичные значения в части префикса (бесклассовое представление), а также частях сети и подсети (классовое представление). Чтобы быть самым младшим номером, у идентификатора подсети должно быть самое низкое возможное двоичное значение (все нули) в части хоста. Чтобы быть самым старшим номером, у широковещательного адреса должно быть максимально возможное двоичное значение (все единицы) в части хоста. Ни идентификатор подсети, ни широковещательный адрес подсети к пригодным для использования адресам не относится, поэтому у адресов в диапазоне, пригодных для использования IP-адресов, никак не может быть всех нулей или единиц в части хоста.
3. в). Мaska преобразуется в 255.255.255.0. При поиске идентификатора подсети для каждого октета маски со значением 255 можно просто скопировать соответствующие значения IP-адреса. Для октетов маски с десятичным числом 0 можно сразу записать нули в соответствующем октете идентификатора подсети. Таким образом, для нахождения идентификатора подсети 10.7.99.0 скопируйте числа 10.7.99, а для 4-го октета напишите 0.
4. В первую очередь, резидентская подсеть (идентификатор той подсети, в которой располагается адрес) в цифровой форме должна быть меньше IP-адреса, что исключает один из ответов. Мaska преобразуется в 255.255.255.252. Поскольку первые три октета маски имеют значения 255, можно скопировать первые три

октета IP-адреса. Для четвертого октета значение идентификатора подсети должно быть кратно 4, поскольку $256 - 252$ (маска) = 4. К кратным числам относятся 96 и 100, а правильный выбор — это самое близкое кратное к значению IP-адреса в этом октете (97) без превышения. Таким образом, правильный идентификатор подсети 192.168.44.96.

5. в). Резидентский идентификатор подсети в данном случае 172.31.77.192. Широковещательный адрес подсети можно найти на основании идентификатора подсети и маски несколькими методами. Маска преобразуется в 255.255.255.224, таким образом, интересен октет 4 с магическим значением $256 - 224 = 32$. Для трех октетов, где маска = 255, скопируйте идентификатор подсети (172.31.77). Для интересующего октета возьмите значение идентификатора подсети (192), добавьте магическое значение (32), вычтите 1, получится 223. Это даст широковещательный адрес подсети 172.31.77.223.
6. в). Чтобы ответить на этот вопрос, необходимо выяснить диапазон адресов в подсети, что, как правило, означает необходимость вычислить идентификатор и широковещательный адрес подсети. При идентификаторе/маске подсети 10.1.4.0/23 маска преобразуется в 255.255.254.0. Для поиска широковещательного адреса после процесса, описанного в данной главе, можно скопировать первые два октета идентификатора подсети, поскольку маска имеет в них значение 255. В четвертом октете запишете 255, поскольку у маски в четвертом октете 0. В интересующем октете 3 добавьте магическое значение (2) к значению идентификатора подсети (4), вычтите 1, чтобы получить значение $2 + 4 - 1 = 5$. (Магическое значение в данном случае вычисляется как $256 - 254 = 2$.) Это дает широковещательный адрес 10.1.5.255. Последний пригодный для использования адрес на единицу меньше: 10.1.5.254. Диапазон, который включает последние 100 адресов: 10.1.5.155 – 10.1.5.254.
7. б). Чтобы ответить на этот вопрос, необходимо вычислить широковещательный адрес подсети, поскольку следует знать нижний конец диапазона адресов в подсети. Первый IP-адрес в подсети на единицу больше идентификатора подсети, или 192.168.9.97. Первые 20 адресов составляют диапазон 192.168.9.97–192.168.9.116.

Глава 18

Знаете ли вы уже темы главы

1. б) и в). Идентификаторы подсети: 10.0.0.0, 10.16.0.0, 10.32.0.0 и так далее, считая по 16 во втором октете, до 10.240.0.0.
2. в) и г). Маска преобразуется в 255.255.252.0, таким образом, разница между последующими идентификаторами подсети (в этой книге называемое магическим числом) составляет $256 - 252 = 4$. Так, список идентификаторов подсети начинается с 172.30.0.0, далее 172.30.4.0, 172.30.8.0 и так далее, при добавлении 4 к третьему октету. Маска, используемая с сетью класса В, подразумевает 6 битов подсети, всего для 64 идентификаторов подсети. Последний из них, 172.30.252.0, может быть выявлен как частный случай, поскольку у его третьего октета, где находятся биты подсети, то же значение, что и у маски в том же третьем октете.

3. а). Первый (в цифровом виде самый нижний) идентификатор подсети совпадает с номером классовой сети 192.168.9.0. Остальные идентификаторы подсети, каждый на восемь больше предыдущего, составляют последовательность 192.168.9.8, 192.168.9.16, 192.168.9.24, 192.168.9.32 и так далее до 192.168.9.248.
4. а). Чтобы решить эту проблему, можно найти все идентификаторы подсети сети 172.20.0.0, используя каждую из масок в ответах, и сравнить каждый список с идентификаторами подсети, перечисленными в вопросе. Если список всех идентификаторов подсети для данной маски включает все значения вопроса, то эта маска и применяется. Для правильного ответа, с маской 255.255.252.0, магическое число на основании третьего октета составляет 4. (Магическое число — $256 - 252 = 4$.) Список идентификаторов подсети при использовании этой маски: 172.20.0.0, 172.20.4.0, 172.20.8.0 и так далее, на 4 больше в третьем октете у каждого. Из трех номеров, перечисленных в тексте вопроса, значения третьих октетов (80, 128 и 192) кратны 4. При маске 255.255.192.0 магическое число — $256 - 192 = 64$, следовательно, третий октет всех идентификаторов подсети должен был бы быть кратен 64. В данном случае один из идентификаторов подсети в вопросе (172.20.80.0) не является кратным 64. Точно так же с маской 255.255.224.0: инкремент идентификаторов подсети 32 и 80 не является кратным 32. И наконец, маска 255.255.0.0 является заданной по умолчанию для сетей класса В. При ней никаких подсетей не существует вообще, и ни один из идентификаторов подсети, перечисленных в вопросе, не может существовать.
5. г). При маске /24 (255.255.255.0) идентификаторы подсети увеличиваются на единицу в третьем октете. Дело в том, что у сети класса В 16 битов в части сети, а с маской /24 следующие 8 битов принадлежат подсети. Таким образом, весь третий октет содержит биты подсети. У всех идентификаторов подсети последний октет будет 0, поскольку весь четвертый октет состоит из битов хоста. Обратите внимание: 172.19.0.0 — нулевая подсеть, 172.19.255.0 — широковещательный адрес подсети, может, и они выглядят странно, но являются вполне допустимыми идентификаторами подсети.
6. б). Маска /27 преобразуется в 255.255.255.224. Поскольку сеть имеет класс В, формат адресов подразумевает 16 битов сети и 11 битов подсети. Биты подсети занимают весь третий октет и первые 3 бита четвертого октета. Магическое число ($256 - 224 = 32$) применяется в четвертом октете как инкремент, который, будучи добавлен к значению в четвертом октете, дает следующий идентификатор подсети. В результате получим идентификаторы подсети: 172.19.0.0, 172.19.0.32, 172.19.0.64 ... 172.19.0.224, 172.19.1.0, 172.19.1.32 ... 172.19.1.224, 172.19.2.0, 172.19.2.32 ... до 172.19.255.224. Обратите внимание: в четвертом октете значение всегда кратно 32. Неправильный ответ содержит значение 16, которое не является кратным 32.
7. г). Согласно процессам, описанным в этой главе, сеть класса А и маска /25 определяют 8 битов сети (по классу) и 17 битов подсети (октеты 2 и 3 целиком плюс 1 бит подсети в октете 4). Магическое число применяется в 4-м октете для поиска значения, добавление которого к предыдущему идентификатору подсети дает следующий идентификатор подсети. Магическое число в данном случае — $256 - 128 = 128$. В результате четвертый октет будет или 0, или 128. Октеты 2 и 3 могли быть любым значением от 0 до 255 включительно. Только один ответ (10.1.1.192) не соответствует значениям этого диапазона.

Глава 19

Знаете ли вы уже темы главы

1. б) и д). В маршрутизаторах компании Cisco есть выключатель питания, в коммутаторах — обычно нет.
2. б) и в). Маршрутизаторы SOHO предназначены для подключения пользователей к Интернету, поэтому в них используется клиент DHCP для получения IP-адреса от провайдера услуги, а служба сервера DHCP назначает адреса хостам в сети малого офиса.
3. а) И в маршрутизаторах, и в коммутаторах используются IP-адреса, поэтому обе команды, `ip address маска` и `ip address dhcp`, могут использоваться в коммутаторах и маршрутизаторах. Команда `interface vlan 1` встречается только в коммутаторах.
4. б) и г) Чтобы маршрутизировать пакеты, у интерфейса маршрутизатора должен быть IP-адрес и его состояние должно быть “`up`” и “`up`”. В последовательных каналах в лабораторном стенде, когда не используются модули CSU/DSU, на одном конце канала в интерфейсе должна стоять команда `clock rate`, которая в данном случае будет задавать скорость линии. Команды `bandwidth` и `description` не влияют на работоспособность канала.
5. в). Если первый код состояния интерфейса равен “`down`”, значит, есть проблема на уровне 1 (например, кабель не подключен к интерфейсу).
6. в) и д).
7. б) и в). В маршрутизаторе каждый рабочий интерфейс должен иметь IP-адрес, а в коммутаторе есть только один адрес, который используется сугубо для доступа к устройству. В диалоге начального конфигурирования устройства таким образом задаются немного отличающиеся параметры, в частности, для маршрутизатора можно указать адреса всех интерфейсов.
8. г) и е). Процедура начальной загрузки маршрутизатора сначала считывает 4 младших бита конфигурационного регистра, называемых загрузочным полем, и проверяет, есть ли в глобальной конфигурации команды `boot system`. Данные настройки позволяют инженеру указать, какую операционную систему IOS следует загружать при инициализации устройства.
9. а).

Глава 20

Знаете ли вы уже темы главы

1. а) и в). Маршрутизатор добавит статический маршрут в таблицу маршрутизации, если выходной интерфейс работает или информация о следующем транзитном узле правильна.
2. а).
3. а) и б).
4. д) и е).

5. б), г), д) и е).
6. г), д) и е).
7. а), г), д) и з). Конфигурация состоит из команд `router rip, version 2, network 10.0.0.0` и `network 11.0.0.0`. Команда `network` использует в качестве параметра адрес классовой сети, а команда `version 2` нужна для включения второй версии протокола RIP. Маршрутизатору №2 не нужна команда `network 9.0.0.0`, поскольку в конфигурации следует вводить команду `network` только для тех сетей, которые подключены непосредственно к устройству.
8. а). В команде `network` в качестве параметра используются классовые адреса сетей, установленных на интерфейсах маршрутизатора. В параметре должен быть указан адрес сети полностью, а не только октеты части сети.
9. б).
10. б) и в). В квадратных скобках указано административное расстояние (первое число) протокола и метрика (второе число) маршрута. Счетчик времени (00:00:13) указывает время, прошедшее от последнего обновления маршрута. Счетчик сбрасывается в значение 00:00:00 при получении обновления маршрутной информации.

Глава 21

Знаете ли вы уже темы главы

1. в) и г). Адреса, начинающиеся с 225, являются многоадресатными и относятся к классу D, следовательно, они не могут быть назначены интерфейсам. Адрес 10.43.53.63 с маской 255.255.255.192 — это широковещательный адрес подсети 10.43.53.0 с маской 255.255.255.192.
2. б).
3. в). Символ звездочки (*) около соединения с номером 2 указывает на последнее активное соединение, в которое команда `resume` переключит пользователя, если в ней не указать параметров.
4. а) и г). Хосты в локальной сети используют протокол ARP, чтобы найти MAC-адреса в той же подсети. Компьютер ПК1 считает, что адрес 10.1.1.130 размещен в той же подсети, поэтому он будет использовать указанный механизм. Компьютер ПК3 не будет использовать протокол ARP для адреса 10.1.1.10, поскольку его подсеть и маска равны 10.1.1.128/25, а диапазон адресов — 10.1.1.129–10.1.1.254. У маршрутизатора R1 есть маршрут к подсети 10.1.1.0/24 с диапазоном 10.1.1.1–10.1.1.254, поэтому устройство будет использовать протокол ARP для обнаружения MAC-адреса хоста с IP-адресом 10.1.1.130.
5. а). Тестирование с помощью утилиты `ping` своего собственного адреса не покажет, работает ли локальная сеть, поскольку пакет через сеть не передается. Необходимо пересыпалать пакеты эхо-запросов от устройства ПК1 через стандартный шлюз (R1), чтобы проверить работоспособность сети, по крайней мере, на участке от хоста до шлюза. Единственный ответ, в котором указано, что пакеты будут проходить искомый участок сети (между ПК1 и R1), — `ping 10.1.1.1`, даже несмотря на то, что такое тестирование дает отрицательный результат.

6. а), в) и д). Команда `tracert` в операционных системах компании Microsoft и команда `traceroute` в операционной системе Cisco IOS выводят список IP-адресов промежуточных маршрутизаторов и адрес хоста-получателя. Первой записью в выводе команды будет адрес ближайшего маршрутизатора к хосту — шлюза.
7. б) и в). Узел ПК1 использует протокол ARP для обнаружения MAC-адресов хостов в том же самом сегменте сети. Компьютеру ПК1 нужен MAC-адрес стандартного шлюза, R1, а шлюзу, аналогично, нужно знать MAC-адрес хоста ПК1.
8. а) и г). Хосты используют протокол ARP для обнаружения MAC-адресов хостов в том же самом сегменте сети. Тем не менее хост также может узнать адрес из пришедшего запроса ARP. Компьютер ПК1 отправит широковещательный запрос на IP-адрес 10.1.1.1 маршрутизатора R1, в результате хост ПК1 узнает MAC-адрес маршрутизатора, а маршрутизатор узнает адрес хоста. Аналогично, поскольку первый пакет пришел от хоста ПК1 к хосту ПК2, маршрутизатору R2 нужно определить MAC-адрес последнего с помощью протокола ARP, и он отправит запрос. Из такого запроса хост ПК2 узнает MAC-адрес маршрутизатора R2, а маршрутизатор узнает адрес хоста ПК2, поэтому устройству ПК2 не нужно пересыпать широковещательный запрос ARP, чтобы узнать адрес шлюза.
9. а), в) и д). В IP-заголовке указан адрес отправителя 10.1.1.10, а адрес получателя 172.16.2.7 — для пакетов, передаваемых в схеме сети слева направо. В ответных пакетах эхо-запросов эти адреса поменялись местами (т.е. в пакетах справа налево). MAC-адреса всегда описывают устройства в данной локальной сети, также нужно помнить, что в протоколе HDLC не используются MAC-адреса.

Глава 22

Знаете ли вы уже темы главы

1. г). Модемы демодулируют аналоговый сигнал из телефонной сети в цифровой и предназначены для декодирования битов, пересылаемых модемом на другом конце линии. Следовательно, демодуляция представляет собой преобразование аналогового сигнала в цифровой, т.е. биты.
2. а). Из рассмотренных в этой книге технологий доступа к Интернету только у DSL есть ограничение на длину абонентского канала.
3. г). Мультиплексор DSLAM разделяет, или мультиплексирует, голосовой трафик и потоки данных, перенаправляет голосовой поток в голосовой коммутатор, а потоки данных — в маршрутизатор.
4. а) и в). Кабельная технология доступа к Интернету поддерживает только асимметричные скорости каналов.
5. б) и в).
6. а). Маршрутизатор выполняет функцию сервера DHCP в локальной сети, а на его интерфейсе IP-адрес назначен статически. Устройство также выполняет преобразование NAT/PAT, заменяя IP-адреса отправителей пакетов. Маршрутизатор не может быть сервером DNS, хотя его служба DHCP передает информацию о серверах разрешения имен клиентским хостам.

7. б) и в). Маршрутизатор выполняет функцию сервера DHCP в локальной сети и работает как клиент DHCP в интерфейсе, подключенном к провайдеру. Он выполняет преобразование NAT/PAT, т.е. заменяет адреса отправителей пакетов, но не работает как сервер DNS.
8. б) и в). В типичной схеме подключения маршрутизатор преобразует адреса (выполняет трансляцию NAT/PAT), следовательно, сервер получит пакет с открытым маршрутизуемым адресом, а не частным — 10.1.1.1. Компьютер воспользуется обычной службой DNS, чтобы определить IP-адрес сайта www.cisco.com, который представляет собой также зарегистрированный адрес в Интернете. В терминологии NAT внутренний локальный адрес представляет собой частный адрес во внутренней сети, а внутренний глобальный — открытый адрес в Интернете, в который преобразуются адреса отправителей с помощью технологии NAT или PAT.

Глава 23

Знаете ли вы уже темы главы

1. а). Команда `encapsulation` сбрасывает инкапсуляцию (настройка канального уровня), поэтому нужно вводить только команду `encapsulation ppp`. Команда `clock rate` имеет смысл только в лабораторном подключении устройств (т.е. когда они соединены напрямую), и если канал уже работает, значит, частота синхронизации линии уже введена. Команда `bandwidth` не влияет на работу канала.
2. б). При лабораторном последовательном подключении устройств необходимо ввести команду `clock rate` в интерфейсе устройства, к которому подключен кабель DCE. Если к маршрутизатору R1 подключен кабель DTE, то к маршрутизатору R2 должен быть подключен кабель DCE и команду нужно ввести в маршрутизаторе R2. Команда `bandwidth` не влияет на работоспособность интерфейса, она нужна для других целей, например, для управления метриками протоколов маршрутизации EIGRP и OSPF.
3. б). Команда `clock rate` нужна только при лабораторном подключении устройств, а в данном случае используется выделенная линия от оператора телефонной связи. Команду `bandwidth` можно использовать, но для работы канала она не нужна. Поскольку маршрутизаторы новые и не были ранее настроены, в последовательных интерфейсах обычно используется инкапсуляция HDLC, поэтому нужно ввести команду `encapsulation ppp` в интерфейсах обоих устройств.
4. в) и г). К дополнительным параметрам относятся: стандартный шлюз службы DHCP, который представляет собой IP-адрес маршрутизатора доступа; адрес подсети и маска подсети.
5. б). Мастер конфигурирования устройства SDM позволяет настроить клиентскую службу DHCP с опциональным включением службы PAT. Конфигурация службы PAT предполагает, что все интерфейсы, в которых установлены IP-адреса, являются потенциально внутренними, а интерфейс, в котором запущен клиент DHCP, — внешним.

-
6. г). Для доступа к диспетчеру SDM нужен веб-браузер на компьютере, а на маршрутизаторе должна быть запущена служба веб-сервера, чтобы пользователь мог подключиться через сеть IP, а не консольный порт. В программном обеспечении служба SSH не используется. Диспетчер SDM загружает конфигурацию в маршрутизатор только после того, как пользователь щелкнет на кнопке **Finish** (Завершить) в любом из мастеров настройки, но конфигурация добавляется только в текущий конфигурационный файл (*running-config*).
 7. а) и б). Чтобы можно было вводить имена вместо IP-адресов для доступа к Интернету, в сервере DHCP нужно сделать несколько дополнительных настроек, в том числе IP-адрес сервера DNS провайдера. Путаница с тем, какие интерфейсы являются внутренними, а какие внешними при трансляции адресов — обычное дело. Два последних ответа вообще не имеют никакого отношения к постановке вопроса.

ПРИЛОЖЕНИЕ Б

Справочные числовые таблицы

Это приложение содержит несколько полезных справочных таблиц, в которых приведены числа, используемые всюду в этой книге. Например, табл. Б.1 полезна при преобразовании десятичных чисел в двоичные, и наоборот.

Таблица Б.1. Десятичные и двоичные числа в диапазоне от 0 до 255

Десятичное число	Двоичное число						
0	00000000	32	00100000	64	01000000	96	01100000
1	00000001	33	00100001	65	01000001	97	01100001
2	00000010	34	00100010	66	01000010	98	01100010
3	00000011	35	00100011	67	01000011	99	01100011
4	00000100	36	00100100	68	01000100	100	01100100
5	00000101	37	00100101	69	01000101	101	01100101
6	00000110	38	00100110	70	01000110	102	01100110
7	00000111	39	00100111	71	01000111	103	01100111
8	00001000	40	00101000	72	01001000	104	01101000
9	00001001	41	00101001	73	01001001	105	01101001
10	00001010	42	00101010	74	01001010	106	01101010
11	00001011	43	00101011	75	01001011	107	01101011
12	00001100	44	00101100	76	01001100	108	01101100
13	00001101	45	00101101	77	01001101	109	01101101
14	00001110	46	00101110	78	01001110	110	01101110
15	00001111	47	00101111	79	01001111	111	01101111
16	00010000	48	00110000	80	01010000	112	01110000
17	00010001	49	00110001	81	01010001	113	01110001
18	00010010	50	00110010	82	01010010	114	01110010
19	00010011	51	00110011	83	01010011	115	01110011
20	00010100	52	00110100	84	01010100	116	01110100
21	00010101	53	00110101	85	01010101	117	01110101
22	00010110	54	00110110	86	01010110	118	01110110
23	00010111	55	00110111	87	01010111	119	01110111
24	00011000	56	00111000	88	01011000	120	01111000
25	00011001	57	00111001	89	01011001	121	01111001
26	00011010	58	00111010	90	01011010	122	01111010
27	00011011	59	00111011	91	01011011	123	01111011

Окончание табл. Б.1

Десятичное число	Двоичное число						
28	00011100	60	00111100	92	01011100	124	01111100
29	00011101	61	00111101	93	01011101	125	01111101
30	00011110	62	00111110	94	01011110	126	01111110
31	00011111	63	00111111	95	01011111	127	01111111
128	10000000	160	10100000	192	11000000	224	11100000
129	10000001	161	10100001	193	11000001	225	11100001
130	10000010	162	10100010	194	11000010	226	11100010
131	10000011	163	10100011	195	11000011	227	11100011
132	10000100	164	10100100	196	11000100	228	11100100
133	10000101	165	10100101	197	11000101	229	11100101
134	10000110	166	10100110	198	11000110	230	11100110
135	10000111	167	10100111	199	11000111	231	11100111
136	10001000	168	10101000	200	11001000	232	11101000
137	10001001	169	10101001	201	11001001	233	11101001
138	10001010	170	10101010	202	11001010	234	11101010
139	10001011	171	10101011	203	11001011	235	11101011
140	10001100	172	10101100	204	11001100	236	11101100
141	10001101	173	10101101	205	11001101	237	11101101
142	10001110	174	10101110	206	11001110	238	11101110
143	10001111	175	10101111	207	11001111	239	11101111
144	10010000	176	10110000	208	11010000	240	11110000
145	10010001	177	10110001	209	11010001	241	11110001
146	10010010	178	10110010	210	11010010	242	11110010
147	10010011	179	10110011	211	11010011	243	11110011
148	10010100	180	10110100	212	11010100	244	11110100
149	10010101	181	10110101	213	11010101	245	11110101
150	10010110	182	10110110	214	11010110	246	11110110
151	10010111	183	10110111	215	11010111	247	11110111
152	10011000	184	10111000	216	11011000	248	11111000
153	10011001	185	10111001	217	11011001	249	11111001
154	10011010	186	10111010	218	11011010	250	11111010
155	10011011	187	10111011	219	11011011	251	11111011
156	10011100	188	10111100	220	11011100	252	11111100
157	10011101	189	10111101	221	11011101	253	11111101
158	10011110	190	10111110	222	11011110	254	11111110
159	10011111	191	10111111	223	11011111	255	11111111

В табл. Б.2 приведены шестнадцатеричные и двоичные числа. Она полезна при преобразовании шестнадцатеричных чисел в двоичные, и наоборот.

Таблица Б.2. Шестнадцатеричные и двоичные числа

Шестнадцатеричное число	Четырехзначное двоичное число
0	0000
1	0001
2	0010
3	0011
4	0100
5	0101
6	0110
7	0111
8	1000
9	1001
A	1010
B	1011
C	1100
D	1101
E	1110
F	1111

Табл. Б.3 содержит степени числа 2, от 2^1 до 2^{32} .

Таблица Б.3. Степени числа 2

X	2^x	X	2^x
1	2	17	131 072
2	4	18	262 144
3	8	19	524 288
4	16	20	1 048 576
5	32	21	2 097 152
6	64	22	4 194 304
7	128	23	8 388 608
8	256	24	16 777 216
9	512	25	33 554 432
10	1 024	26	67 108 864
11	2 048	27	134 217 728
12	4 096	28	268 435 456
13	8 192	29	536 870 912
14	16 384	30	1 073 741 824
15	32 768	31	2 147 483 648
16	65 536	32	4 294 967 296

В табл. Б.4 приведены все 33 возможные маски подсетей, во всех трех форматах.

Таблица Б.4. Все маски подсетей

Десятичная	Префикс	Двоичная
0.0.0.0	/0	00000000 00000000 00000000 00000000
128.0.0.0	/1	10000000 00000000 00000000 00000000
192.0.0.0	/2	11000000 00000000 00000000 00000000
224.0.0.0	/3	11100000 00000000 00000000 00000000
240.0.0.0	/4	11110000 00000000 00000000 00000000
248.0.0.0	/5	11111000 00000000 00000000 00000000
252.0.0.0	/6	11111100 00000000 00000000 00000000
254.0.0.0	/7	11111110 00000000 00000000 00000000
255.0.0.0	/8	11111111 00000000 00000000 00000000
255.128.0.0	/9	11111111 10000000 00000000 00000000
255.192.0.0	/10	11111111 11000000 00000000 00000000
255.224.0.0	/11	11111111 11100000 00000000 00000000
255.240.0.0	/12	11111111 11110000 00000000 00000000
255.248.0.0	/13	11111111 11111000 00000000 00000000
255.252.0.0	/14	11111111 11111100 00000000 00000000
255.254.0.0	/15	11111111 11111110 00000000 00000000
255.255.0.0	/16	11111111 11111111 00000000 00000000
255.255.128.0	/17	11111111 11111111 10000000 00000000
255.255.192.0	/18	11111111 11111111 11000000 00000000
255.255.224.0	/19	11111111 11111111 11100000 00000000
255.255.240.0	/20	11111111 11111111 11110000 00000000
255.255.248.0	/21	11111111 11111111 11111000 00000000
255.255.252.0	/22	11111111 11111111 11111100 00000000
255.255.254.0	/23	11111111 11111111 11111110 00000000
255.255.255.0	/24	11111111 11111111 11111111 00000000
255.255.255.128	/25	11111111 11111111 11111111 10000000
255.255.255.192	/26	11111111 11111111 11111111 11000000
255.255.255.224	/27	11111111 11111111 11111111 11100000
255.255.255.240	/28	11111111 11111111 11111111 11110000
255.255.255.248	/29	11111111 11111111 11111111 11111000
255.255.255.252	/30	11111111 11111111 11111111 11111100
255.255.255.254	/31	11111111 11111111 11111111 11111110
255.255.255.255	/32	11111111 11111111 11111111 11111111

ПРИЛОЖЕНИЕ В

Обновление экзамена ICND1: версия 1.0

Отзывы читателей помогают издательству Cisco Press определить, какие именно темы вызывают наибольшие сложности на сертификационном экзамене. Более того, компания Cisco может постепенно вносить небольшие изменения в темы экзаменов и по-другому расставлять акценты и приоритеты в технологиях передачи данных. Чтобы помочь читателю в работе над изменившимися темами, автор книги публикует дополнительные материалы, в которых объясняются трудные моменты каких-либо технологий и новых тем экзамена. Как было указано во введении к книге, дополнительные материалы для сдачи сертификационного экзамена размещены на веб-сайте по адресу <http://www.ciscopress.com/title/1587204258> в формате PDF. Там же размещена обновленная версия приложения, которое вы сейчас читаете.

В этом приложении содержится новая информация для сертификационного экзамена, которая была доступна на момент издания книги. Чтобы убедиться в том, что у вас есть наиболее актуальная версия приложения, перейдите по ссылке, указанной выше, и посмотрите, какая версия доступна. Версия данного приложения — 1.0.

Данное приложение призвано заполнить некоторые пробелы, которые возникают в процессе издания практически любой книги. В частности, в нем представлена следующая информация:

- несколько технических терминов, которые нигде в книге не описаны и не упомянуты;
- новые темы, которые компания Cisco внесла в экзамены ICND1 и CCNA;
- самые свежие данные по сертификационному экзамену.

Получите самые свежие материалы на веб-сайте

Сейчас вы читаете версию приложения, которая была доступной и актуальной на момент издания книги. Тем не менее всегда лучше владеть самой новой и актуальной информацией, поэтому следует получить обновленную версию с веб-сайта издательства. Чтобы загрузить новую версию, выполните следующие действия.

1. В поле адреса браузера введите <http://www.ciscopress.com/title/1587204258> и зайдите на сайт.
2. Выберите ссылку Downloads (Загрузки) во вкладке More Information (Дополнительная информация).
3. Загрузите документ *ICND1 Appendix C* (Приложение В книги ICND1).

ВНИМАНИЕ!

Загруженный вами документ имеет собственный номер версии. Если версия загруженного документа совпадает с той, которая указана в текущем приложении, значит, у вас есть самый новый вариант приложения и книги, поэтому нет необходимости загружать обновленную версию ICND1.

Техническая информация

В текущей версии приложения нет дополнительной технической информации. Задача этого приложения (версии 1.0) — просто предоставить читателю инструкцию о том, как и где проверить и загрузить свежую версию приложения.

Словарь терминов

1000BASE-T. Спецификация широкополосной технологии Gigabit Ethernet со скоростью передачи 1000 Мбит/с, в которой используются четыре пары кабеля UTP категории 5; максимальная длина сегмента составляет 100 м (328 футов).

100BASE-TX. Спецификация узкополосной технологии Fast Ethernet со скоростью передачи данных 100 Мбит/с, в которой используются две пары кабелей UTP или STP. Первая пара используется для приема данных, вторая — для передачи. Для нормальной синхронизации сигнала в 100BASE-TX соединение не должно превышать 100 м (328 футов). Описывается стандартом IEEE 802.3.

10BASE-T. Спецификация узкополосной технологии Ethernet со скоростью передачи данных 10 Мбит/с, в которой используются две пары кабеля типа “витая пара” (категории 3, 4, 5): одна пара — для передачи данных, другая — для приема. Она является частью стандарта IEEE 802.3; максимальная длина сегмента равна 100 м (328 футов).

802.11a. Стандарт IEEE для беспроводных сетей с использованием спектра U-NII, с модуляцией OFDM и скоростью до 54 Мбит/с.

802.11b. Стандарт IEEE для беспроводных сетей с использованием спектра ISM, с модуляцией DSSS и скоростью до 11 Мбит/с.

802.11g. Стандарт IEEE для беспроводных сетей с использованием спектра ISM, с модуляцией DSSS и скоростью до 54 Мбит/с.

802.11i. Стандарт IEEE безопасности беспроводных сетей, включающий в себя аутентификацию и шифрование.

802.11n. Стандарт IEEE для беспроводных локальных сетей с использованием спектра ISM, модуляцией OFDM и нескольких антенн для одиночного потока со скоростью до 150 Мбит/с.

802.1Q. Стандарт IEEE для магистральных каналов сетей VLAN.

Anti-X. Термин, используемый компанией Cisco для описания многих средств сетевой безопасности, предотвращающих различные атаки, включая антивирус, антифишинг и антиспам.

E1. Цифровой канал передачи данных с полосой 2,048 Мбит/с, состоящий из 32 подканалов по 64 Кбит/с, из которых один зарезервирован для фреймирования и служебных данных. Используется в Европе и является аналогом американского стандарта T1.

IP-адрес (IP address). Это 32-битовый адрес, назначаемый хосту при использовании протокола TCP/IP. Каждый адрес состоит из адреса сети, необязательного адреса подсети и адреса хоста. Адреса сети и подсети совместно используются для маршрутизации, а адрес хоста необходим для доставки информации определенному сетевому хосту в сети или подсети. Маска подсети используется для извлечения из IP-адреса информации о сети и подсети.

L4PDU. Блок данных, сформированный протоколом уровня 4, содержащий заголовок четвертого уровня и инкапсулированные данные верхних уровней, но не информацию нижних.

MAC-адрес (MAC address). Стандартизованный адрес канального уровня, необходимый каждому устройству, подключенному к локальной сети. Все устройства используют MAC-адреса, чтобы найти определенные устройства в сети, а также для создания и обновления таблиц коммутации и структур данных. Длина MAC-адресов составляет 6 байтов, контролируются они Институтом инженеров по электротехнике и электронике (Institute of Electrical and Electronics Engineers — IEEE). Этот тип адреса также называют *аппаратным адресом* (hardware address), *адресом уровня MAC* (MAC-layer address) и *физическим адресом* (physical address).

RFC (Request For Comments). Серия документов IETF с описаниями набора протоколов Интернета и дополнительной информацией. Некоторые документы RFC приняты Советом по архитектуре Интернета (Internet Architecture Board — IAB) как стандарты Интернета. Большинство документов RFC определяют такие протоколы, как Telnet и FTP, но некоторые носят юмористический или исторический характер. Документы RFC доступны на многих веб-сайтах.

RJ-45. Восьмиконтактный разъем, которым обычно заканчивается кабель типа “витая пара” в сети Ethernet. Он похож на телефонный разъем RJ-11, который очень распространен в США и Европе.

ROMMON. Сокращенное название режима ROM Monitor, представляющего собой низкоуровневую операционную систему, загружаемую маршрутизаторами компании Cisco в редких случаях для восстановления паролей или операционной системы IOS во флеш-памяти.

RxBoot. Вариант операционной системы Cisco IOS с ограниченными функциями, хранящийся в памяти ROM в старых моделях маршрутизаторов. Эта версия системы иногда используется для некоторых низкоуровневых функций, например, загрузки новой версии системы IOS во флеш-память или восстановления системы из-за отказа памяти.

T1. Цифровой канал передачи данных по распределенной сети. В линии T1 данные передаются в формате DS-1 со скоростью 1,544 Мбит/с в виде 24 отдельных подканалов по 64 Кбит/с (DS0) и управляющего канала для служебных данных со скоростью 8 Кбит/с.

Telco. Общепринятое англоязычное сокращение от слов “телефонная компания”.

Traceroute (сокращенный вариант — trace). Программа, которая прослеживает путь пакета до пункта назначения. Используется главным образом для отладки процесса маршрутизации между хостами. Существует также протокол отслеживания, определенный в документе RFC 1393. Эта программа имеется во многих операционных системах.

Абонентский канал (local loop). Телефонная линия или телекоммуникационный канал от оборудования абонента до АТС оператора местной телефонной связи.

Автономная система (autonomous system). Отдельная сеть или набор сетей, находящихся под единым административным контролем какой-либо компании, государственной организации. В автономной системе обычно используется *протокол маршрутизации внутреннего шлюза* (Interior Gateway Protocol — IGP).

Авторизация (authorization). В технологиях безопасности проверка прав определенного пользователя или устройства. См. AAA.

Административное расстояние (Administrative Distance — AD). Величина, характеризующая надежность источника информации о маршрутизации. Она выражается числом в диапазоне от 0 до 255. Чем больше ее значение, тем менее доверительна полученная информация.

Адрес подсети (subnet number или subnet address). В протоколе IP v4 — это четырехбайтовое число, записываемое в десятичной форме с точками между байтами, которое описывает все адреса в подсети. В числовом выражении — это наименьший адрес в подсети, который является зарезервированным и не может быть назначен хосту.

Адрес хоста (host address). IP-адрес, присвоенный сетевой карте компьютера.

Альянс Wi-Fi (Wi-Fi Alliance). Организация, сформированная множеством компаний, производящих оборудование для беспроводных сетей (т.е. промышленная ассоциация), основная задача которой — сформировать рынок совместимых между собой устройств от разных производителей. Эта организация занимается выпуском стандартов и ускоряет процесс стандартизации в международных организациях.

Анонс маршрутизации (routing update). Сообщения, рассылаемые между маршрутизаторами объединенной сети, в которых содержится информация о достижимости сети и соответствующая оценка маршрута. Обновления маршрутизации обычно рассылаются с постоянными интервалами, а также в случае изменений в сетевой топологии.

Асимметричный цифровой абонентский канал (Asymmetric Digital Subscriber Line — ADSL). Одна из четырех технологий DSL, предназначенная для высокоскоростной передачи данных в направлении основного трафика (от центрального офиса к пользователю), а не в обратном направлении. Канал ADSL функционирует на расстоянии до 18 000 футов (5488 метров) по одиночной электрической витой паре.

Асимметрия (asymmetric). Свойство многих технологий доступа к Интернету, в том числе и DSL, предполагающее, что скорость входящего потока данных намного больше, чем исходящего.

Асинхронность (asynchronous). Отсутствие временных меток в потоке битов. На практике оба конца канала согласовывают одинаковую скорость передачи данных, но в дальнейшем подстройка или проверка того факта, что скорости передачи немного отличаются, отсутствует. Тем не менее, поскольку данные пересыпаются по-битово, небольшая рассинхронизация не является проблемой.

Аутентификация (authentication). В технологиях безопасности — проверка идентификатора пользователя или процесса.

Аутентификация, авторизация и учет (Authentication, Authorization, And Accounting — AAA). Произносится как “triple a”. С помощью аутентификации идентифицируют пользователя или устройство. Авторизация определяет права на выполнение чего-либо пользователем, а учет записывает информацию о попытках доступа.

Базовый набор служб (Basic Service Set — BSS). Беспроводная сеть с единственной точкой доступа к сети.

Без контроля ошибок (error disabled). Специальное состояние интерфейса в коммутаторе локальной сети, в которое он переходит из-за различных нарушений режима безопасности.

Бесклассовый протокол маршрутизации (classless routing protocol). Более новый протокол маршрутизации, пересылающий в своих анонсах таблиц маршрутизации адрес подсети и маску. Такой протокол маршрутизации не ориентирован на класс сети и поддерживает маски VLSM и суммирование маршрутов вручную.

Блок данных протокола (Protocol Data Unit — PDU). Термин в модели OSI, опи- сывающий сгруппированную определенным образом информацию какого-либо конкретного уровня модели. Обычно аббревиатурой L_xPDU обозначают блок уровня x (Layer x).

Брандмауэр (firewall). Одно или несколько сетевых устройств, таких как маршрутизаторы или серверы доступа, предназначенных для создания буферной зоны между открытыми и частными сетями. Для обеспечения безопасности частных сетей в брандмауэре используются списки управления доступом и другие методы.

Булево “И” (Boolean AND). Математическая операция для однобитового двоичного числа. В результате получается однобитовое число. 1 “И” 1 = 1, все остальные комбинации битов дают в результате 0.

Веб-сервер (web server). Программное обеспечение, запущенное на некотором компьютере, позволяющее хранить веб-страницы и передавать их клиентскому программному обеспечению — браузеру.

Взаимодействие на равноправном уровне (same-layer interaction). Коммуникация между двумя устройствами с использованием функций определенного уровня сетевой модели. Коммуникация осуществляется с использованием заголовков конкретного уровня. Например, устройство заполняет определенные поля в заголовках, пересыпает заголовки и инкапсулированные данные, а принимающая сторона интерпретирует информацию в заголовках и выполняет соответствующие действия.

Взаимодействие на смежных уровнях (adjacent-layer interaction). Общий термин, описывающий, как два смежных уровня одного компьютера взаимодействуют в рамках сетевой модели. Нижний уровень предоставляет некоторую службу верхнему уровню.

Виртуальная локальная сеть (Virtual LAN — VLAN). Группа устройств, принадлежащих одной или нескольким локальным сетям и настроенных таким образом (с помощью управляющего программного обеспечения), что обмен данными между ними происходит так, как будто они подключены к одному кабелю, хотя на самом деле находятся в разных сегментах сети LAN. Поскольку сети VLAN основаны на логическом, а не на физическом соединении, они необычайно гибки.

Виртуальная частная сеть (Virtual Private Network — VPN). Частная сеть, создаваемая в открытой сетевой инфраструктуре, такой, например, как глобальный Интернет. В сетях VPN пакеты шифруются, поэтому обеспечивается конфиденциальность передаваемых данных, а оконечные точки сети аутентифицируются, что обеспечивает их идентичность.

Виртуальный канал (virtual circuit). Логический канал, обеспечивающий надежное соединение между двумя сетевыми устройствами. Виртуальные каналы применяются в сетях Frame Relay, X.25 и ATM, обеспечивая те же функции, что и выделенная линия, но без выделенного физического соединения.

Витая пара (twisted pair). Среда передачи данных, представляющая собой два свитых медных провода в пластиковой оболочке без металлизированного экрана. За счет того, что проводники перекручены, интерференция и перекрестные помехи существенно уменьшаются. Широко используется в различных сетях.

Внутренний глобальный адрес (inside global). Заменяет существующий адрес в заголовках пакетов, передающихся из локальной сети (т.е. из-за устройства NAT) и использующийся для маршрутизации таких пакетов в глобальном (открытом) Интернете.

Внутренний локальный адрес (inside local). Адрес в заголовках пакетов, находящихся за устройством NAT в локальной корпоративной (т.е. частной) сети, подлежащий замене при передаче в открытую сеть.

Вспомогательный порт (auxiliary port). Физический разъем маршрутизатора, предназначенный для подключения дистанционного терминала, например, компьютера с запущенной программой эмуляции терминала, соединяющегося с маршрутизатором через модем.

Выделенная линия (leased line). Разновидность последовательного канала связи между двумя точками без коммутации, зарезервированный поставщиком услуги, обычно — местной телефонной компанией, исключительно для использования заказчиком. Поскольку оператор связи или телефонная компания обычно не выделяет физический кабель между двумя площадками, а предоставляет виртуальный канал, стоимость такой линии может быть ниже.

Высокоуровневый протокол управления каналом (High-Level Data Link Control — HDLC). Бит-ориентированный синхронный протокол канального уровня, разработанный ISO. Основан на протоколе SDLC и определяет метод инкапсуляции данных в синхронных последовательных каналах с помощью символов кадрирования и контрольных сумм.

Головной узел (head end). Вышестоящий узел абонентского канала кабельного телевидения для доступа к Интернету.

Декапсуляция (decapsulation), или *деинкапсуляция* (de-encapsulation). Процесс интерпретации и удаления заголовков нижних уровней по мере продвижения блока данных снизу вверх по уровням в компьютере. Этот процесс на каждом уровне распаковывает модуль передачи данных для вышестоящего уровня.

Диалог начальной настройки (setup mode). Окно операционной системы Cisco IOS в маршрутизаторах и коммутаторах, позволяющее настроить базовые параметры устройства в режиме интерактивного диалога и создать файл текущей и стартовой конфигурации.

Диспетчер управления безопасностью маршрутизаторов компании Cisco (Router Security Device Manager). Веб-интерфейс для управления маршрутизатором, который позволяет конфигурировать и контролировать функции маршрутизатора, в том числе, например, службы DHCP и NAT/PAT.

Дистанционно-векторный протокол маршрутизации (distance vector routing protocol). Относится к классу алгоритмов маршрутизации, последовательно анализирующих переходы на маршруте для построения связующего дерева кратчайшего пути. В дистанционно-векторных протоколах требуется, чтобы каждый маршрутизатор при каждом обновлении маршрутизации рассыпал полностью свою таблицу маршрутизации, но только своим соседям. Алгоритмы дистанционно-векторной маршрутизации подвержены проблеме образования кольцевых маршрутов, однако в вычислительном отношении они проще алгоритмов маршрутизации по состоянию канала. Такие алгоритмы также называют алгоритмами маршрутизации Беллмана–Форда (Bellman-Ford).

Домен коллизий (collision domain). В сетях Ethernet область сети, в которой распространяются столкнувшиеся и поврежденные фреймы. Повторители и концентраторы не отфильтровывают такие поврежденные фреймы, в то время как коммутаторы локальных сетей LAN, мосты и маршрутизаторы их не пропускают.

Дуплексная передача (full duplex). Возможность одновременной передачи данных между отправляющей и принимающей станциями в двух направлениях.

Enable-режим (enable mode). Привилегированный режим доступа к интерфейсу операционной системы Cisco IOS, в котором пользователь может вводить наиболее сложные и “опасные” для маршрутизатора или коммутатора команды, а также выполнять конфигурирование устройства.

Загрузочное поле (boot field). Четыре младших бита конфигурационного регистра маршрутизатора Cisco. Значение в загрузочном поле указывает маршрутизатору, из какого источника загружать операционную систему Cisco IOS.

Запись CIDR. См. префиксная запись.

Зарезервированные порты (well-known ports). Определены документом RFC 1700, зарезервированы и в протоколе TCP, и в протоколе UDP. Зарезервированные порты могут определять приложения, выполняемые над протоколами транспортного уровня.

Защищенный беспроводной доступ (Wi-Fi Protected Access — WPA). Маркетинговое название, присвоенное Альянсом Wi-Fi спецификациям по безопасности, которые предшествовали стандарту IEEE 802.11i.

Защищенный беспроводной доступ версии 2 (Wi-Fi Protected Access 2 — WPA2). Маркетинговое название, присвоенное Альянсом Wi-Fi спецификациям по безопасности, описанным в стандарте IEEE 802.11i.

Звездообразная топология (star topology). Наиболее часто используемая физическая топология локальных сетей Ethernet. Сеть со звездообразной топологией имеет центральную точку соединений, которая может быть концентратором, коммутатором или маршрутизатором; в этой точке сходятся все кабельные сегменты.

Идентификатор набора служб (Service Set Identifier — SSID). Текстовая строка, используемая в беспроводных сетях для идентификации сети.

Изоляция проблемы (problem isolation). Этап процесса поиска и устранения неисправностей, на котором сетевой инженер пытается выделить основные причины отказа.

Импульсно-кодовая модуляция (Pulse Code Modulation — PCM). Передача аналоговой информации в цифровой форме за счет дискретизации и преобразования в коды с фиксированным количеством битов. Аналоговый голосовой поток кодируется в цифровой с пропускной способностью 64 Кбит/с за счет использования 8 битов для уровней сигнала и выборки 8000 раз в секунду.

Инкапсуляция (encapsulation). Упаковка данных в заголовок некоторого конкретного протокола. Например, данные протоколов высокого уровня перед передачей помещаются в заголовок Ethernet. Аналогичным образом при мостовом соединении разнородных сетей весь фрейм из одной сети может быть помещен после заголовка, используемого протоколом канального уровня другой сети.

Институт инженеров по электротехнике и электронике (Institute of Electrical and Electronic Engineers — IEEE). Профессиональная организация, деятельность которой включает в себя разработку коммуникационных и сетевых стандартов. Стандарты для сетей LAN, разработанные IEEE, в настоящее время являются преобладающими при проектировании и эксплуатации сетей.

Интерфейс базового уровня (Basic Rate Interface — BRI). Интерфейс сети ISDN, состоящий из двух каналов B (по 64 Кбит/с) и одного канала D (16 Кбит/с) в сети с коммутацией каналов для передача голоса по сети.

Интерфейс доступа (access interface). Термин, относящийся к дизайну локальных сетей; описывает интерфейс коммутатора, к которому подключены устройства конечных пользователей.

Интерфейс командной строки (Command-Line Interface — CLI). Интерфейс, который позволяет пользователям взаимодействовать с операционной системой за счет ввода специализированных команд и их аргументов.

Интерфейс основного уровня (Primary Rate Interface — PRI). Интерфейс сети ISDN для доступа на основной скорости передачи. Доступ на основной скорости по одному каналу D со скоростью 64 Кбит/с плюс 23 канала (T1) или 30 (E1) каналов B для передачи голоса или данных.

Исправление ошибок (error recovery). Процесс, позволяющий обнаружить, что данные были переданы с ошибками, и отвечающий за повторную пересылку недостающих или ошибочных блоков.

Источник синхронизации (clock source). Устройство, с которым другие устройства в линии синхронизируют свою скорость в синхронных линиях.

Канал связи (access link). В технологии Frame Relay — физический последовательный канал, соединяющий устройство DTE среды Frame Relay, обычно маршрутизатор, с коммутатором Frame Relay. В таком канале используются те же стандарты физического уровня, что и в двухточечных выделенных линиях.

Классовая сеть (classful network). Сеть класса A, B или C протокола IPv4. Называется классовой потому, что подчиняется правилам классовой адресации.

Классовый протокол маршрутизации (classful routing protocol). Протокол, не передающий маску подсети в обновлениях совместно с адресом подсети и, следовательно, ориентирующийся на класс сети — A, B или C. Не поддерживает маски VLSM.

Клиент WLAN (WLAN client). Беспроводное устройство, пытающееся подключиться к беспроводной сети через точку доступа.

Кодек (codec), *кодер-декодер* (coder-decoder). Устройство в виде интегральной схемы для преобразования аналоговых сигналов в цифровой поток битов и обратного преобразования цифровых сигналов в аналоговые сигналы, обычно с помощью кодово-импульсной модуляции.

Коммутатор (switch). Устройство, соединяющее сегменты локальной сети LAN и использующее таблицу MAC-адресов для определения сегментов, в которые следует переслать фреймы. Такой принцип работы позволяет существенно уменьшить объем нецелесообразно рассылаемых данных. Коммутаторы работают с гораздо большими скоростями, чем мосты. Коммутаторы работают на канальном уровне эталонной модели OSI.

Коммутация без буферизации пакетов (cut-through switching). Устройства, использующие этот метод коммутации, читают, обрабатывают и пересылают фреймы сразу после того, как будет прочитан адрес получателя и определен порт назначения. См. также *режим коммутации с промежуточным хранением*.

Коммутация каналов (circuit switching). Технология, в которой во время сеанса связи должен существовать физический канал между отправителем и получателем. Широко используется в сетях телефонных компаний. С точки зрения коммутацию каналов можно рассматривать как противоположность коммутации пакетов и сообщений, а с точки зрения методов доступа — как противоположность методу конкуренции и передачи маркеров. Примером сетевой технологии с коммутацией каналов является ISDN.

Коммутация пакетов (packet switching). Сетевая технология, в которой разные хосты обмениваются пакетами данных по одному разделяемому каналу связи.

Коммутируемая сеть Ethernet (switched Ethernet). Сеть Ethernet, в которой используется коммутатор, но не концентратор, поэтому устройства в сети не конкурируют за среду передачи данных и ее полосу пропускания. Этот термин является антонимом термина *разделяемая сеть Ethernet*, который предполагает использование сети в режиме, в котором устройства конкурируют за среду передачи и полосу пропускания. Коммутируемый вариант сети позволяет наиболее оптимально использовать полосу пропускания и фактически выделить свою собственную полосу каждому устройству.

Конвергенция (convergence). Способность группы устройств объединенной сети, использующих конкретный протокол маршрутизации, согласовать друг с другом информацию о топологии сети после того, как в ней произошли изменения. Требуемое для этого время определяет скорость конвергенции.

Консольный порт (console port). Физический разъем в маршрутизаторе или коммутаторе, к которому кабелем может быть подключен компьютер. Этот порт используется для доступа к интерфейсу командной строки устройства и его конфигурированию с помощью программ эмуляции терминала.

Конфигурационный регистр (configuration register). 16-битовый конфигурируемый параметр в маршрутизаторах компании Cisco, который определяет, как работает маршрутизатор в процессе инициализации. Значение регистра устанавливается программными средствами в шестнадцатеричной системе с помощью специализированных команд.

Концентратор (hub). Общая точка соединений устройств сети. Обычно концентраторы используются для подключения отдельных сегментов к локальной сети. Концентратор может иметь несколько портов. Когда на один из них поступает пакет, он копируется и направляется на все остальные порты концентратора, поэтому такой пакет поступает во все сегменты сети LAN.

Лавинная рассылка (flooding). Способ передачи данных, применяемый коммутаторами и мостами, при использовании которого данные, полученные на некотором интерфейсе, рассылаются через все интерфейсы устройства, за исключением того, на котором они были первоначально получены.

Логический адрес (logical address). Общий термин, обозначающий адреса сетевого уровня и протоколов третьего уровня. Он не зависит от нижних уровней и зачастую противопоставляется адресам канального уровня, называемым физическими, поскольку последние зависят от используемой технологии физического уровня.

Магистральный интерфейс (trunk interface). Физическое и логическое соединение между двумя коммутаторами, по которому передается сетевой трафик. В современных коммутаторах используются магистральные соединения стандартов 802.1Q или ISL.

Маршрут хоста (host route). Маршрут с маской /32, представляющий собой маршрут к одному IP-адресу хоста.

Маршрутизируемый протокол (routed protocol). Протокол, отвечающий за передачу данных, например AppleTalk, DECnet или IP.

Маска подсети (subnet mask). 32-разрядная маска адреса, используемая протоколом IP для описания битов части сети и хоста в адресе подсети. Части сети адреса соответствуют двоичные 1 в маске, а хоста — 0.

Маска подсети переменной длины (Variable-Length Subnet Mask — VLSM). Возможность задавать различные маски для одной и той же сети класса А, В или С

в различных подсетях. Мaska VLSM позволяет оптимизировать доступное адресное пространство.

Международная организация по стандартизации (International Organization for Standardization — ISO). Международная ассоциация национальных организаций по стандартизации, обеспечивающая разработку и поддержку глобальных стандартов в сфере коммуникаций и обмена информацией. ISO разработала популярную эталонную модель взаимодействия открытых систем — OSI.

Межкоммутаторный канал (Inter-Switch Link — ISL). Собственный протокол компании Cisco, который сохраняет информацию виртуальной сети LAN при обмене трафиком между коммутаторами и маршрутизаторами.

Межсетевая операционная система корпорации Cisco (Internetwork Operating System — Cisco IOS). Программное обеспечение межсетевой операционной системы корпорации Cisco обеспечивает функциональность, расширяемость и безопасность всех аппаратных продуктов. Программное обеспечение хранится в виде образа во флеш-памяти, загружается в оперативную память устройства, обеспечивает его работу и выполнение всех необходимых функций.

Метод скользящего окна (sliding window). Метод управления потоком, при котором получатель дает отправителю разрешение на пересылку данных до заполнения окна. Когда окно заполняется, отправитель прекращает передачу до тех пор, пока получатель не объявит о расширении окна. Этот метод управления потоком используется в протоколе TCP и других транспортных протоколах, а также в некоторых протоколах канального уровня.

Метрика (metric). Числовое значение, вырабатываемое каким-либо алгоритмом для каждого маршрута в сети. Обычно чем меньше метрика, тем предпочтительнее маршрут.

Механизм создания подсетей (subnetting). Метод деленияенного адреса любого из классов на более мелкие части. Этот механизм позволил избежать полного исчерпания доступных IP-адресов (версии 4).

Микросегментация (microsegmentation). Позволяет создавать в локальной сети частные или выделенные сегменты, в которых на каждый сегмент приходится только одна рабочая станция. В этом случае каждая станция получает мгновенный доступ ко всей полосе пропускания, и ей не приходится конкурировать с другими за доступ к имеющейся полосе пропускания.

Многомодовый оптоволоконный кабель (Multimode Fiber — MM fiber). Оптоволоконный носитель, в котором свет распространяется в нескольких модах за счет того, что диаметр его больше и пучок света может входить под разными углами. Полоса пропускания такого кабеля меньше, чем у одномодового, но в нем обычно используются более дешевые источники световых импульсов — светодиодные излучатели, а не лазеры.

Множественный доступ с обнаружением коллизий (Carrier Sense Multiple Access/Collision Detect — CSMA/CD). Механизм доступа к среде передачи, при использовании которого устройства, готовые к передаче данных, предварительно прослушивают канал для выяснения, не занят ли он. Если в течение заданного промежутка времени канал не занят, начинается передача. Если два устройства начинают передачу одновременно, происходит коллизия, которая регистрируется всеми участвующими в ней устройствами. Такая коллизия вызывает у устройств задержку повторной передачи в течение некоторого случайным образом выбираемого промежут-

ка времени. Метод доступа CSMA/CD используется в сетях спецификаций Ethernet и IEEE 802.3.

Множественный доступ с предотвращением коллизий (Carrier Sense Multiple Access/Collision Avoidance — CSMA/CA). Механизм доступа к среде передачи, при использовании которого устройства стараются избежать коллизий за счет использования специального фрейма. Такой метод доступа к среде используется в беспроводных сетях.

Модем (modem), *модулятор-демодулятор* (modulator-demodulator). Устройство, преобразующее цифровые сигналы в аналоговые, и наоборот. На станции-отправителе modem преобразует цифровые сигналы в форму, соответствующую каналам аналоговой связи. В пункте назначения аналоговые сигналы преобразуются в цифровую форму. Модемы позволяют передавать информацию по обычным телефонным линиям.

Модуль обслуживания канала/модуль обработки данных (Channel Service Unit/Data Service Unit — CSU/DSU). Устройство, работающее со стандартами первого уровня в последовательных каналах, устанавливаемое оператором связи и определяющее, как телекоммуникационное оборудование будет взаимодействовать с последовательным портом маршрутизатора.

Мультиплексирование с ортогональным частотным разделением сигналов (Orthogonal Frequency Division Multiplexing — OFDM). Метод кодирования данных в беспроводных сетях, позволяющий достичь более высоких скоростей передачи данных, чем кодирование FHSS или DSSS.

Направленный широковещательный адрес (directed broadcast address). См. *широковещательный адрес подсети*.

Неполносвязная топология (partial-mesh topology). В сети с такой топологией, по крайней мере, одно устройство имеет несколько соединений с другими устройствами сети, однако при этом сеть не обладает полносвязной структурой. Вместе с тем неполносвязная топология обеспечивает определенный уровень избыточности за счет наличия нескольких альтернативных маршрутов.

Неэкранированная витая пара (Unshielded Twisted Pair — UTP). Среда передачи данных, представляющая собой четыре пары свитых медных проводников в пластиковой оболочке без металлизированного экрана. Широко используется в различных сетях.

Номер порта (port number). Поле в заголовке TCP или UDP, идентифицирующее приложение, которое пересыпает (порт отправителя) или принимает (порт получателя) поток сегментов данных.

Нулевая подсеть (zero subnet). Подсеть в классовой сети IPv4, в которой в адресе подсети стоят двоичные нули. В десятичном виде нулевая подсеть может быть легко идентифицирована, поскольку ее адрес совпадает с адресом сети.

Обнаружение ошибок (error detection). Процесс определения, был ли фрейм канального уровня изменен в процессе передачи. Для решения этой задачи обычно используется *контрольная сумма фрейма* (Frame Check Sequence — FCS) в концевике фрейма.

Оборудование клиента (Customer Premises Equipment — CPE). Оконечное оборудование (терминалы, телефоны, модемы и т.п.), устанавливаемое телефонной компанией у клиента и подключенное к сети телефонной компании.

Образ IOS (IOS Image). Файл, содержащий операционную систему IOS.

Общественная телефонно-телеграфная компания (Post, Telephone and Telegraph — PTT). Коммерческая компания или правительственные организации, обеспечиваю-

щая телефонное обслуживание. Отделения РТТ существуют во всех странах и обеспечивают местную и междугородную телефонную связь.

Одноадресатный фрейм с неизвестным получателем (unknown unicast frame). Фрейм Ethernet, MAC-адрес получателя которого отсутствует в таблице коммутации (таблице MAC-адресов) коммутатора, поэтому устройство должно разослать его с использованием лавинного механизма.

Одномодовый оптоволоконный кабель (single-mode fiber). Разновидность оптического волокна, с тонким сердечником, в который луч света может входить под одним определенным углом. Пропускная способность такого волокна намного больше, чем у многомодового, но для передачи данных нужен источник с узким спектром сигнала, например лазер.

Одноранговый режим (ad hoc mode). В беспроводных сетях — метод работы, когда клиенты беспроводной сети обмениваются данными напрямую без использования точек доступа.

Окно (window). Количество битов, которые могут быть пересланы без подтверждения.

Оконечное оборудование канала передачи данных (Data Circuit-terminating Equipment — DCE). Устройство, используемое для конвертирования данных пользователя из цифрового формата DTE в форму, приемлемую для оборудования служб распределенной сети.

Оперативная память (Random-Access Memory — RAM). Память, которая функционирует только при включенном питании, ее содержимое может записываться и считываться микропроцессором.

Основная причина (root cause). Стандартный термин в поиске и устраниении неисправностей, описывающий причину неработоспособности чего-либо. Основная задача сетевого инженера — найти и устранить такую причину, в результате проблема будет или решена, или перейдет в другую проблему.

Отказ в обслуживании (DoS — Denial-of-Service). Тип сетевой атаки, призванной заблокировать сеть, завалив ее потоком бесполезного трафика.

Открытая коммутируемая телефонная сеть (Public Switched Telephone Network — PSTN). Общее обозначение телефонных сетей и служб, в отличие от глобальных компьютерных сетей. Иногда используется аббревиатура POTS.

Открытый IP-адрес (public IP address). Адрес, являющийся частью зарегистрированной сети или диапазона сетей регионального агентства Центра по присвоению адресов Интернета (Internet Assigned Numbers Authority — IANA). Такой адрес может использовать только организация, зарегистрировавшая его на себя, и маршрутизаторы в Интернете будут знать маршруты к открытym зарегистрированным IP-адресам.

Пакет (packet). Логически сгруппированная информация, состоящая из заголовка, содержащего управляющую информацию, и (как правило) данных пользователя. Чаще всего пакетами называют блоки данных сетевого уровня. На разных уровнях эталонной модели OSI и в разных областях техники для описания логического группирования информации используются термины *дейтаграмма, фрейм, сообщение и сегмент*.

Передача голоса по сети IP (Voice over IP — VoIP). Позволяет маршрутизатору передавать по объединенным сетям IP голосовой трафик (например, телефонные переговоры или факсимильные сообщения) с теми же функциями, надежностью и качеством, что и по телефонной линии.

Перекрещенный кабель (crossover cable). Кабель, в котором перекрещена пара, чтобы правильно подать, передать и получить сигналы между однотипными устройствами. В сетях 10BASE-T и 100BASE-TX провода контактов 1 и 2 подключены к контактам 3 и 6 на другом конце кабеля, а 3 и 6, соответственно, ведут к контактам 1 и 2 на другом конце кабеля.

Пересылка данных (forwarding). Процесс передачи фрейма к получателю с одного интерфейса устройства на другой.

Побитовое булево "И" (bitwise Boolean AND). Операция логического "И" для двух чисел одинаковой длины, выполняемая сначала для первого бита числа, потом для второго, для третьего и т.д.

Подсеть (subnet). Некоторая часть сети класса А, В или С, выделенная сетевым инженером. С помощью подсетей можно сэкономить адресное пространство и создать группы IP-адресов.

Подуровень управления доступом к передающей среде (Media Access Control — MAC). Нижний из двух подуровней канального уровня, определенных спецификацией IEEE. Подуровень MAC управляет доступом к передающей среде, таким как передача маркера или конкуренция за доступ.

Подуровень управления логическим каналом (Logical Link Control — LLC). Верхний из двух подуровней канального уровня, определенных в стандарте IEEE. Подуровень LLC осуществляет контроль ошибок, управление потоками, созданием фреймов и адресацией на уровне MAC. Основным протоколом LLC является спецификация IEEE 802.2, которая описывает как вариант сети с установкой соединения, так и без него.

Позитивное подтверждение и повторная передача (Positive Acknowledgment and Retransmission — PAR). Общее название механизмов обнаружения и исправления ошибок во многих протоколах, например в TCP. Получатель должен переслать подтверждение о том, что данные были успешно получены (позитивное подтверждение) или, если подтверждение не получено, отправитель будет пересыпать данные повторно (повторная передача).

Поле типа протокола (protocol type field). Поле в заголовке фрейма в локальной сети, идентифицирующее следующий за ним заголовок верхнего уровня. Включает в себя поле DIX Ethernet Type, поле стандарта IEEE 802.2 DSAP и поле типа протокола SNAP.

Полносвязная топология (full mesh). Вариант топологии сети, в котором все устройства соединены со всеми и могут взаимодействовать напрямую.

Полудуплексная передача (half duplex). Возможность передачи данных между передающей и принимающей станциями в каждый конкретный момент времени только в одном направлении.

Пользовательский режим (user mode). Режим интерфейса командной строки маршрутизатора или коммутатора, в котором пользователь может вводить команды, не влияющие на работу устройства, обычно просматривать текущее состояние служб и портов, но не может настраивать устройство.

Порт (port). В терминологии IP — процесс верхнего уровня, который принимает данные от нижних уровней. Порты нумеруются и привязываются к конкретным процессам. Например, протокол SNMP приписан к порту с номером 25. Номер порта такого типа называется *зарезервированным портом*, или *адресом*.

Последовательный кабель (serial cable). Разновидность кабеля, в котором используются разные интерфейсы для подключения к модулю или устройству CSU/DSU выделенной линии.

Постоянное запоминающее устройство (Read-Only Memory — ROM). Тип компьютерной памяти, в которой данные записаны предварительно.

Префиксная запись (prefix notation). Краткий формат записи маски подсети, в котором указывается только количество единичных (содержащих 1) битов в маске после косой черты. Например, /24 описывает маску с 24 единичными битами, т.е. маску сети класса С. Часто количество единичных битов в маске сети называют длиной префикса.

Приложение CCP (Cisco Configuration Professional). Графический, веб-ориентированный интерфейс, используемый для конфигурирования устройств Cisco, включая маршрутизаторы и коммутаторы. Приложение CCP предназначено для замены диспетчера SDM (Cisco Security Device Manager), предпочтительного графического приложения для конфигурирования маршрутизаторов и коммутаторов Cisco.

Проверка доступности адресата (Packet Internet Groper — Ping). Команда, используемая для отправки эхо-запроса протокола ICMP и получения на него ответа. Часто используется в сетях IP для проверки наличия связи с сетевым устройством.

Прозрачный мост (transparent bridge). Устройство, которое было предшественником современных коммутаторов локальных сетей. Мости пересыпают фреймы между сегментами локальной сети на основании MAC-адреса получателя, как и коммутаторы, а прозрачными их называют потому, что их присутствие в сети незаметно для оконечных устройств.

Протокол Frame Relay. Стандартный протокол коммутируемой передачи данных канального уровня, который управляет несколькими виртуальными каналами между подключенными устройствами с помощью инкапсуляции HDLC. Он эффективнее протокола X.25 и обычно рассматривается как его замена.

Протокол HTTP. Протокол передачи гипертекста (Hypertext Transfer Protocol), используемый веб-браузерами и веб-серверами для передачи файлов, например текстовых и графических.

Протокол Secure Shell (SSH). Протокол уровня приложений TCP/IP, позволяющий эмулировать терминальное подключение к серверу и использующий динамический обмен ключами и шифрование, для обеспечения безопасности соединения.

Протокол граничного шлюза (Border Gateway Protocol — BGP). Является наиболее распространенным протоколом класса EGP.

Протокол двухточечного соединения (Point-to-Point Protocol — PPP). Преемник протокола SLIP, который обеспечивает соединения “маршрутизатор-маршрутизатор” и “хост-сеть” по синхронным и асинхронным каналам. Протокол SLIP был разработан для работы с IP, но PPP может работать с несколькими протоколами сетевого уровня, такими как IP, IPX и ARA.

Протокол динамической конфигурации хоста (Dynamic Host Configuration Protocol — DHCP). Обеспечивает механизм динамического распределения и повторного использования освобождаемых IP-адресов, а также автоматическую настройку маски, стандартного шлюза и IP-адреса сервера DNS.

Протокол Интернета (Internet Protocol — IP). Протокол сетевого уровня в стеке протоколов TCP/IP; обеспечивает передачу данных между сетями без предварительной установки соединения.

Протокол маршрутизации (routing protocol). Протокол, осуществляющий реализацию какого-либо алгоритма маршрутизации. Примерами протоколов маршрутизации могут служить протоколы IGRP, OSPF и RIP.

Протокол маршрутизации внешнего шлюза (Exterior Gateway Protocol — EGP). Протокол Интернета, использующийся для обмена маршрутной информацией между автономными системами.

Протокол маршрутизации внутреннего шлюза (Interior Gateway Protocol — IGP). Протокол Интернета, использующийся для обмена маршрутной информацией в автономных системах. Примерами широко используемых протоколов класса IGP являются: IGRP, OSPF и RIP.

Протокол маршрутной информации (Routing Information Protocol — RIP). Протокол типа IGP, поставлявшийся с системами BSD UNIX. Это наиболее широко распространенный протокол маршрутизации в локальных сетях. Протокол RIP использует в качестве метрики счетчик транзитных узлов. Первая версия протокола устарела и постепенно становится непопулярной, а вторая, RIPv2, еще широко используется, поскольку содержит много дополнительных функций, в том числе поддержку масок VLSM.

Протокол обеспечения безопасности для беспроводных сетей (Wired Equivalent Privacy — WEP). Механизм обеспечения безопасности, описанный в стандарте 802.11. Предназначен для защиты процесса взаимодействия сетевой платы и точки доступа от несанкционированного прослушивания.

Протокол обнаружения устройств Cisco (Cisco Discovery Protocol — CDP). Протокол CDP используется для получения информации о соседних устройствах, такой, как тип присоединенных устройств, интерфейсы маршрутизатора, которые в настоящий момент присоединены, и номера моделей устройств. Данный протокол работает практически во всем оборудовании компании Cisco: в коммутаторах, маршрутизаторах, серверах доступа и др.

Протокол передачи пользовательских дейтаграмм (User Datagram Protocol — UDP). Является протоколом транспортного уровня без установления соединения из группы протоколов TCP/IP. UDP — это простой протокол, который обеспечивает обмен дейтаграммами без подтверждений или гарантий доставки, требуя, чтобы обработка ошибок и повторную передачу контролировал какой-либо другой протокол. Этот протокол описан в документе RFC 768.

Протокол распределенного связующего дерева (Spanning Tree Protocol — STP). Используемый в мостах и коммутаторах протокол, в котором задействован алгоритм связующего дерева для обеспечения динамического самообучения мостов и предотвращения образования кольцевых маршрутов. Мосты обмениваются сообщениями BPDU, которые позволяют обнаружить кольцевые маршруты и устраниТЬ их, отключая отдельные интерфейсы.

Протокол третьего уровня (layer 3 protocol). Протокол, соответствующий требованиям уровня 3 эталонной модели OSI, определяющий принципы маршрутизации и адресации в сети. Протоколы IP, IPX и AppleTalk DDP являются примерами протоколов третьего уровня.

Протокол управления передачей (Transmission Control Protocol — TCP). Протокол транспортного уровня с установлением соединения, который обеспечивает надежную дуплексную передачу. Относится к стеку TCP/IP.

Протокол управления передачей/протокол Интернета (Transmission Control Protocol / Internet Protocol — TCP/IP). Название набора протоколов, разработанных Министерством обороны США в 1970-х годах для построения всемирной сети. TCP и IP — два наиболее известных протокола из этого стека.

Протокол управляющих сообщений Интернета (Internet Control Message Protocol — ICMP). Представляет собой протокол Интернета сетевого уровня стека TCP/IP, сообщающий об ошибках и предоставляющий другую информацию относительно обработки пакетов IP. Описан в документе RFC 792.

Прямое лабораторное подключение (back-to-back link). Последовательный канал между двумя маршрутизаторами без модулей CSU/DSU, установленный за счет подключения кабеля DTE одного маршрутизатора к кабелю DCE другого. Обычно такое подключение используется в лабораторных работах для соединения двух устройств без использования выделенной линии от местного оператора связи.

Прямой кабель (straight-through cable). Кабель, в котором сохранен порядок следования контактов на обоих концах. Если провод подсоединен к контакту с номером 1 на одном конце кабеля, то и на другом конце он будет подсоединен к аналогичному контакту 1.

Разделяемая сеть Ethernet (shared Ethernet). Сеть Ethernet, в которой используется концентратор или коаксиальный кабель и устройства должны конкурировать за возможность передачи в такой среде, разделяя ее ресурсы между собой.

Расширение спектра сигнала прямой последовательности (Direct Sequence Spread Spectrum — DSSS). Технология, в которой передача данных является более надежной, поскольку каждый бит (0 или 1) представляется некой последовательностью нулей и единиц, которая называется элементарной последовательностью.

Расширение спектра со скачкообразным изменением частоты (Frequency Hopping Spread Spectrum — FHSS). Метод кодирования данных в беспроводной сети, в котором передача каждого следующего блока данных осуществляется на близко расположенной, но другой частоте. В современных стандартах беспроводных сетей не используется.

Расширенный набор служб (Extended Service Set — ESS). Вариант беспроводной сети, в которой есть несколько точек доступа, между которыми возможен роуминг.

Режим асинхронной передачи (Asynchronous Transfer Mode — ATM). Международный стандарт поэлементной передачи, при которой несколько типов данных (например, голосовые, видео- и цифровые данные) передаются в виде ячеек фиксированной длины (53 байта). Ячейки фиксированной длины обрабатываются на аппаратном уровне, что, в свою очередь, позволяет сократить задержки при передаче. Режим ATM предназначен для таких высокоскоростных сетей, как E3, SONET и T3.

Режим инфраструктуры (infrastructure mode). Режим работы беспроводной сети, в котором каждый клиент обменивается данными с точкой доступа, что позволяет клиентам получать доступ к ресурсам только через нее. Между собой клиенты также не обмениваются данными напрямую, а делают это только через точку доступа.

Режим коммутации без фрагментации (fragment-free switching). Режим коммутации, при котором перед пересылкой фреймов фильтруются фрагменты коллизий, являющиеся основным источником ошибок в сети.

Режим коммутации с промежуточным хранением (store-and-forward switching). Техника коммутации, при которой фрейм перед пересылкой в порт назначения полностью записывается в память устройства и обрабатывается. Обработка включает в

себя подсчет контрольной суммы и проверку адреса получателя. Дополнительно фрейм должен быть временно сохранен до тех пор, пока сетевые ресурсы (например, канал) не станут доступны для пересылки фрейма.

Режим конфигурации (configuration mode). Используется для ввода односторочных команд и команд, которые вносят изменения в глобальную конфигурацию маршрутизатора. Команды сохраняются в текущем конфигурационном файле устройства (running-config).

Самообучение (learning). Процесс, используемый коммутаторами для обнаружения MAC-адресов и их относительного месторасположения. Коммутаторы просматривают MAC-адреса отправителей для всех входящих фреймов с целью построения таблицы коммутации.

Самотестирование при включении питания (Power-On Self-Test — POST). Набор диагностических средств, которые проверяют функционирование аппаратуры при включении питания.

Сбалансированный гибридный протокол маршрутизации (balanced hybrid routing protocol). Протокол маршрутизации, использующий элементы дистанционно-векторного протокола и протокола маршрутизации по состоянию канала. *Расширенный протокол маршрутизации внутреннего шлюза* (Enhanced Interior Gateway Routing Protocol — EIGRP) компании Cisco является единственным представителем этого класса протоколов.

Сегмент (segment). 1. Часть сети, ограниченная мостами, маршрутизаторами или коммутаторами, например в сети Ethernet. В среде Ethernet сегмент может представлять собой как один участок кабеля, так и единый домен коллизий, в котором есть много кабелей. 2. В спецификации протокола TCP — логически сгруппированная информация на транспортном уровне эталонной модели OSI, иногда называемая L4PDU.

Сегментация (segmentation). Процесс разделения больших блоков данных от приложения на маленькие, размер которых соответствует используемой среде и технологии передачи данных.

Сервер определения имен (name server). Сервер, установленный в сети, где запущена служба преобразования сетевых имен в IP-адреса, и наоборот.

Сетевая модель (networking model). Общий термин, описывающий некоторый набор протоколов и стандартов, объединяемых по некоторому признаку. Впоследствии согласно модели разрабатываются сетевые устройства, позволяющие объединить хосты в сеть. Примерами сетевых моделей являются TCP/IP и OSI.

Сетевая часть адреса (network part). Часть адреса длиной 1, 2 или 3 октета (байта) в стандарте IPv4, основанная на классе сети A, B или C.

Сетевой адрес (network address, network number). Адрес сетевого уровня, который относится к логическому, а не физическому сетевому устройству. Он также называется *протокольным адресом* (protocol address).

Сеть (network). Группа компьютеров, принтеров, маршрутизаторов, коммутаторов и других устройств, которые могут взаимодействовать в некоторой среде передачи.

Симметричность (symmetric). Характеристика многих технологий доступа к Интернету, предполагающая, что нисходящий и восходящий каналы имеют одинаковую скорость передачи данных и емкость.

Синхронизация (clocking). Процесс передачи специализированного служебного сигнала по кабелю в основной полосе пропускания или по отдельному контакту, по которому принимающее устройство согласует свою работу с передающим устройством.

Синхронная оптическая сеть (Synchronous Optical Network — SONET). Спецификация высокоскоростной (свыше 2,5 Гбит/с) синхронной сети на базе оптоволокна, разработанная Bellcore. Основным блоком сети SONET является STS-1. В 1988 году стандарт SONET был утвержден в качестве международного.

Синхронность (synchronous). Вставка временных меток в поток битов. На практике устройство на одном конце линии подстраивается под скорость передачи другого конца линии, тем не менее, принимая поток данных, оборудование обнаруживает небольшие отклонения и должно постоянно подстраивать свою скорость.

Система доменных имен (Domain Name System — DNS). Система, используемая в Интернете для трансляции имен хостов в сетевые адреса.

Система обнаружения вторжений (Intrusion Detection System — IDS). Средство безопасности в сетях, исследующее сложные шаблоны трафика и сравнивающее их с известными сигнатурами и профилями атак, позволяющее классифицировать атаки на сети и уведомлять сетевого администратора.

Система предотвращения вторжений (Intrusion Prevention System — IPS). Средство безопасности в сетях, исследующее сложные шаблоны трафика и сравнивающее их с известными сигнатурами и профилями атак, позволяющее классифицировать атаки и предпринимать определенные действия по их предотвращению.

Служба telnet. Стандартный протокол эмуляции терминала из группы протоколов TCP/IP. Протокол telnet используется для организации подключений с дистанционного терминала и позволяет пользователям входить в дистанционную систему и использовать ее ресурсы так, словно они подключены к локальной системе. Описан в документе RFC 854.

Сосед CDP (CDP neighbor). Устройство на другом конце некоторого телекоммуникационного кабеля, рассылающее пакеты CDP.

Состояние канала (link state). Один из классов алгоритмов, используемых в протоколах маршрутизации. Протоколы с учетом состояния каналов строят базу данных со множеством деталей о каналах (подсетях) и их состоянии (работает, выключен), на основании которой строится таблица оптимальных маршрутов.

Спецификация Ethernet. Базовая спецификация LAN, созданная корпорацией Xerox и впоследствии развивавшаяся корпорациями Xerox, Intel и Digital Equipment. Сети Ethernet используют метод доступа CSMA/CD и разнообразные типы кабелей со скоростями передачи 10, 100 и 1000 Мбит/с. Стандарты Ethernet и IEEE 802.3 аналогичны.

Спецификация IEEE 802.2. Протокол IEEE для локальных сетей LAN, определяющий реализацию подуровня LLC канального уровня эталонной модели OSI. Стандарт IEEE 802.2 задает методы обработки ошибок и интерфейс службы сетевого (третьего) уровня.

Спецификация IEEE 802.3. Протокол IEEE для сетей LAN, определяющий реализацию подуровня MAC канального уровня (т.е. физическую часть последнего). В спецификации IEEE 802.3 используется метод доступа CSMA/CD для набора возможных скоростей передачи данных в разнообразных физических средах.

Стандартная маска (default mask). Маска, используемая в сетях класса A, B или C, которая не создает каких-либо подсетей. Сети класса A соответствуют маска 255.0.0.0, класса B — 255.255.0.0, класса C — 255.255.255.0.

Стандартный маршрут (default route). Маршрут в маршрутизаторе, по которому отправляются все пакеты, сеть получателя для которых отсутствует в явном виде в таблице маршрутизации.

Стандартный шлюз/стандартный маршрутизатор (default gateway/default router). В конфигурации хоста IP — IP-адрес маршрутизатора, которому узел будет пересыпать пакеты в том случае, если IP-адрес получателя пакета относится к другой подсети.

Стартовый конфигурационный файл (startup-config file). В коммутаторах и маршрутизаторах компании Cisco под управлением операционной системы IOS так называется файл, размещаемый в памяти NVRAM устройства, в котором хранятся настройки устройства, используемые при загрузке и копируемые в текущий конфигурационный файл в оперативной памяти в процессе запуска.

Схема расположения выводов (pinout). Схема подключения проводников в кабеле к контактам разъема.

Таблица маршрутизации (routing table). Представляет собой некоторую разновидность базы данных, хранящуюся в маршрутизаторе или другом устройстве объединенной сети, в которой содержится информация о маршрутах к конкретным сетям-получателям и в большинстве случаев метрики, связанные с этими маршрутами.

Таймер обновлений маршрутизации (update timer). Период этого таймера задает частоту рассылки сообщений об обновлении маршрутизации.

Таймер простоя (inactivity timer). Параметр таблицы MAC-адресов коммутатора, который связан с каждой из записей таблицы и отсчитывается от нуля или сбрасывается до нуля в том случае, когда коммутатор получил фрейм с имеющимся у него в таблице MAC-адресом. Записи с наибольшими значениями таймера удаляются первыми в том случае, если нужно освободить место в таблице для новых записей.

Текущий конфигурационный файл (running-config file). В коммутаторах и маршрутизаторах компании Cisco под управлением операционной системы IOS так называется файл, размещаемый в оперативной памяти устройства, в котором хранятся текущие настройки устройства.

Терминальное оборудование (Data Terminal Equipment — DTE). Устройство, расположенное на пользовательском конце интерфейса “пользователь–сеть”, которое может выступать в качестве источника данных, получателя данных или и того и другого. Устройство DTE соединяется с сетью данных через устройство DCE (например, модем) и для синхронизации зачастую использует временные сигналы, генерируемые устройством DCE. Терминальное оборудование включает в себя такие устройства, как компьютеры, трансляторы протоколов и мультиплексоры. С точки зрения провайдера устройство DTE находится вне сети провайдера услуг и обычно представляет собой маршрутизатор.

Тестовый пакет (keepalive). Сообщение, отправляемое одним сетевым устройством, которое сигнализирует другому сетевому устройству о работоспособности виртуального канала между ними.

Точка демаркации, или граница (demarc). Так называют узел, в котором кабель провайдера службы подключается к кабельной системе организации или здания.

Точка доступа (access point). Устройство в беспроводной локальной сети, позволяющее клиентам обмениваться данными друг с другом и с остальной сетью. Точка доступа подключена к проводной локальной сети и имеет радиосвязь для беспроводных соединений.

Трансляция адресов с использованием портов (Port Address Translation — PAT). Метод трансляции, который позволяет пользователю сохранять адреса в глобальном адресном пуле, позволяя транслировать порты отправителей в соединениях TCP или диалогах UDP. Разные локальные адреса затем преобразуются в глобальные, где трансляция порта обеспечивает их уникальность.

Трансляция сетевых адресов (Network Address Translation — NAT). Механизм сокращения необходимости в глобально уникальных IP-адресах. Позволяет подключаться к Интернету организации с локально уникальными адресами за счет трансляции этих адресов в глобально маршрутизируемое адресное пространство.

Универсальный указатель ресурсов (Universal Resource Locator — URL). Стандартная схема адресации для доступа к гипертекстовым документам и другим службам через браузер в сети TCP/IP. Например, адрес <http://www.cisco.com/univercd> представляет собой URL, идентифицирующий протокол (HTTP), название хоста (www.cisco.com), а также путь к странице (/univercd).

Упорядоченная передача данных (ordered data transfer). Сетевая функция, входящая в стек TCP/IP, в которой протокол определяет, как хост отправителя должен нумеровать пересылаемые данные и как хост получателя должен переупорядочивать блоки данных, если они пришли в неправильном порядке. Эта функция также определяет, как уничтожать блоки данных, которые не могут быть доставлены в нужном порядке.

Управление потоком (flow control). Представляет собой методику, благодаря которой не допускается ситуация, когда передающий объект переполняет данными принимающий объект. При полном заполнении буферов принимающего устройства посылающему устройству отправляется сообщение о необходимости отложить передачу данных до завершения обработки данных в буферах. Примером механизма управления потоками является метод скользящего окна в TCP.

Установка соединения (connection establishment). Процесс, в ходе которого протокол с установлением соединения создает виртуальный канал. В протоколе TCP соединение создается в результате трехэтапного согласования канала с помощью специализированных сегментов.

Учет (accounting). В терминах безопасности служба, записывающая действия пользователя, в том числе и попытки доступа.

Фильтр (filter). Обычно процесс или устройство, которое определяет, передавать или не передавать трафик дальше на основе заданных критериев, таких как адрес отправителя, получателя или протокол.

Флеш-память (flash memory). Специализированный тип электронно-перепрограммируемой постоянной памяти (Electrically Erasable Programmable Read-Only Memory — EEPROM), содержимое которой может быть стерто и перепрограммировано заново. Информация в этом типе памяти сохраняется при выключенном питании, в ней нет движущихся механических частей, что уменьшает вероятность отказа.

Фрейм (frame). Логически сгруппированная информация, пересылаемая в виде блока данных канального уровня по среде сети.

Хост (host). Любое устройство, использующее IP-адрес.

Цифровая сеть с комплексным обслуживанием (Integrated Services Digital Network — ISDN). Протокол, используемый телефонными компаниями и позволяющий передавать по телефонным сетям данные, голос и другие типы трафика. Часто используется в качестве средства доступа к Интернету, а также как средство

установки резервного канала между маршрутизаторами на случай отказа основного соединения WAN.

Цифровой абонентский канал (Digital Subscriber Line — DSL). Открытая сетевая технология, обеспечивающая высокую скорость передачи на ограниченные расстояния по обычному медному проводу. Используется в качестве технологии доступа к Интернету для подключения пользователя к провайдеру.

Цифровой сигнал уровня 0 (Digital Signal level 0 — DS0). Спецификация формирования фреймов при передаче цифровых сигналов по одному каналу с полосой пропускания 64 Кбит/с для передачи одного голосового вызова в импульсно-кодовой модуляции

Цифровой сигнал уровня 1 (Digital Signal level 1 — DS1). Спецификация формирования фреймов при передаче цифровых сигналов по одному каналу с полосой пропускания 1,544 Мбит/с по линии T1 (в США) или 2,108 Мбит/с по линии E1 (в Европе). Канал этого уровня включает в себя 24 подканала DS0 по 64 и 8 Кбит/с управляющей информации для соединения T1.

Частные адреса (private addresses). Зарезервированные IP-адреса в классах сетей А, В и С, которые предназначены только для использования в локальной сети какой-либо организации. Эти адреса описаны в документе RFC 1918; они не маршрутизируются в Интернете.

Частота синхроимпульсов (clock rate). Частота, с которой интерфейс последовательного канала передает биты в среду передачи данных.

Часть подсети (subnet part). В подсетях адресного пространства IPv4 — одна из трех частей адреса или маски подсети, уникальным образом идентифицирующая подсеть в рамках классовой сети.

Часть хоста (host part). Термин, описывающий часть адреса формата IPv4, которая уникальным образом идентифицирует хост в подсети. Часть хоста в адресе идентифицируется двоичными нулями в маске подсети.

Четырехпроводной канал (four-wire circuit). Линия от телекоммуникационной компании, состоящая из двух витых пар. Каждая из пар используется для передачи сигнала в одном направлении, за счет чего достигается дуплексный режим работы.

Шина (bus). Набор электрических цепей, через которые передаются данные от одной части компьютера другой.

Ширина полосы пропускания (bandwidth). Объем информации, проходящей через сетевое соединение за определенный период времени. Сам термин пришел из ранних стандартов телекоммуникационных технологий, когда таким термином описывался частотный диапазон или ширина частотного диапазона устройств для передачи данных.

Широковещательная подсеть (broadcast subnet). Разделяя сеть класса А, В или С на подсети, инженер должен выделить адрес, в части хоста которого все биты равны 1. Такой адрес и является широковещательным, а для последней подсети он совпадает с широковещательным адресом классовой сети. Последнюю подсеть классовой сети зачастую называют широковещательной.

Широковещательный адрес (broadcast address). Используется для широковещательной рассылки пакетов всем сетевым устройствам. См. *широковещательный адрес подсети*.

Широковещательный адрес подсети (subnet broadcast address). Специализированный адрес в каждой из подсетей, представляющий собой наибольший адрес блока

для подсети. Адрес работает таким образом, что если пакет отправлен на широковещательный адрес, то его получат все устройства в подсети.

Широковещательный адрес сети (network broadcast address). В стандарте IPv4 — специальный адрес в каждой классовой или бесклассовой сети, используемый для широковещательной пересылки пакета всем хостам в сети. В числовом выражении такой адрес представляет собой наибольший адрес в сети, например, для классовой частной сети 10.0.0.0 широковещательный адрес будет равен 10.255.255.255.

Широковещательный домен (broadcast domain). Это совокупность всех устройств, которые получают широковещательные фреймы от любого из устройств этой совокупности. Границы широковещательного домена обычно определяются маршрутизаторами (в коммутируемых сетях — виртуальными сетями VLAN), поскольку маршрутизаторы не пересылают широковещательные фреймы.

Широковещательный фрейм (broadcast frame). Фрейм, рассылаемый всем хостам сегмента локальной сети, адрес получателя которого равен FFFF.FFFF.FFFF.

Шифрование (encryption). Применение специального алгоритма для изменения внешнего вида данных таким образом, чтобы их содержание было непонятно для тех, кому не предоставлены соответствующие средства дешифрования.

Экранированная витая пара (Shielded Twisted Pair — STP). Тип кабеля витой пары, в которой каждая пара имеет свой экран, а весь кабель защищен общим экраном.

Энергонезависимая память (NonVolatile RAM — NVRAM). Оперативное запоминающее устройство, содержимое которого сохраняется при отключении питания.

Эталонная модель взаимодействия открытых систем (Open System Interconnection — OSI reference model). Структурная модель сети, разработанная Международной организацией по стандартизации (ISO). Эта модель включает в себя семь уровней, каждый из которых выполняет свои специфические функции, такие как адресация, управление потоком, контроль ошибок, инкапсуляция и надежная передача сообщений. Эталонная модель OSI используется как универсальный метод обучения сетевых специалистов для понимания ими функций компьютерной сети.

Язык гипертекстовой разметки (HyperText Markup Language — HTML). Простой язык гипертекстового форматирования документов, в котором используются теги (неотображаемый текст разметки документа) для указания способа представления частей документа приложениями просмотра, такими, как веб-браузеры.

Предметный указатель

A

- AAA, 274
- Access Point, 333
- ACM, 348
- AD, 548
- Address Resolution Protocol, 163
- Adjacent-layer interaction, 64
- Administrative Distance, 548
- Advanced Encryption Standard, 356
- AES, 356
- AP, 333
- ARP, 144; 163
- ASN, 538
- ATM, 610
- Autosummarization, 540

B

- Back-to-back link, 122
- Bandwidth, 338
- Basic Service Set, 335
- Beacon frame, 354
- BGP, 538
- BIA, 104
- Border Gateway Protocol, 538
- Broadcast
 - addresses, 104
 - domain, 223
 - subnet, 474; 562
- BSS, 335; 347

C

- Cable
 - modem, 495
 - TV, 494
- Cat OS, 240
- CATV, 494; 607
- CCX, 348
- CDP, 309
- Channel Service Unit, 491
- Chunk, 185
- CIDR, 408
- CIR, 133
- Circuit, 601
- Cisco Discovery Protocol, 309
- Classful

- addressing, 419
- IP network, 391
- Classless
 - addressing, 419
 - Interdomain Routing, 408
- CLI, 239; 270
- CLN, 650
- Clocking, 502
- CO, 599
- Collision, 320
 - domain, 100; 223
- Command-Line Interface, 270
- Committed Information Rate, 133
- Convergence, 541
 - time, 161
- CRC, 319
- CSU/DSU, 491

D

- Data
 - Communication Equipment, 122
 - Link Connection Identifier, 131
 - Terminal Equipment, 122
- DCE, 122
- DDN, 66
- Default
 - gateway, 157
 - mask, 393
 - route, 533; 615
- Digital
 - Service Unit, 491
 - Subscriber Line, 44
- DLCI, 131
- DMZ, 199
- DNS, 180
- Domain Name System, 180
- DoS, 195
- Dotted-Decimal Notation, 66
- DRAM, 256
- DSL, 44; 602
 - modem, 495
- DSLAM, 603
- DSSS, 339
- DTE, 122
- Dynamic window, 182

E

EGP, 537
 EIRP, 342
 EMI, 319
 Encapsulation, 70
 Encoding, 94
 Enterprise network, 42
 ESS, 335; 347
 Extended Service Set, 335

F

FCC, 337
 FCS, 108
 FHSS, 339
 File Transfer Protocol, 87; 180
 FIN bit, 184
 Flooding, 217
 Forward acknowledgment, 181
 Frame, 69; 71; 131
 Check Sequence, 108
 Framing, 105
 FTP, 87; 180

H

Half duplex, 100
 HDLC, 125; 499; 626
 Header, 69; 125
 High-Level Data Link Control, 125; 499
 Hop count, 540
 Host, 66
 HTTP, 187
 Hub, 47; 91

I

ICANN, 538
 ICMP, 167
 IDS, 351
 IEEE, 59
 IFS, 260
 IGP, 537
 Inside
 global, 619
 host, 619
 interface, 619
 Integrated Services Router, 492
 Interesting octet, 457
 Interface, 239; 286
 International Organization for
 Standardization, 58
 Internet

Control Message Protocol, 167
 Protocol, 64
 Service Provider, 44
 Internetwork, 147
 IOS, 240
 IP, 64
 host, 67; 148
 network, 366
 routing, 67
 subnet, 366
 IPS, 351
 IP-адресация, 148
 ISM, 338
 ISO, 58
 ISP, 44
 ISR, 492

J

Jamming signal, 99

L

LAN, 42
 LAPF, 131
 Layer, 59
 LED, 241
 Link Access Procedure Frame, 131
 LLC, 88
 Local Area Network, 42
 Logical
 address, 146
 addressing, 141
 Link Control, 88

M

MAC, 88
 Magic number, 457
 MAN, 116
 Manual summarization, 540
 Mask, 157
 Media Access Control, 88
 Metric, 539; 547
 MIC, 356
 MIMO, 340
 MTU, 185
 Multicast addresses, 104
 Multiplexing, 176

N

Name resolution, 564
 NAT, 377; 616

Network, 147
 access, 68
 address, 395
 Address Translation, 377; 616
 ID, 395
 number, 395
 Networking model, 57
 Next hop, 535
 NVRAM, 256

O

OFDM, 340
 Open System Interconnection, 54; 58
 OSI, 54; 58
 Outside interface, 619

P

Packet, 71
 PAR, 183
 PAT, 616
 Path selection, 141
 PCM, 124
 Permanent Virtual Circuit, 369
 Pin, 95
 Ping, 167
 Point-to-Point Protocol, 126; 499
 Port, 239
 Port Address Translation, 616
 PPDIOO, 368
 PPP, 126; 499; 629
 Prefix, 407
 Protocol, 57
 Data Unit, 77
 type, 107
 PSK, 353
 PSTN, 598
 Pulse Code Modulation, 124
 PVC, 132; 369; 610
 PCM, 600

Q

QoS, 187

R

RAM, 256
 Reassembly, 611
 Repeater, 90
 Requests for Comments, 59
 RFC, 59
 RIP, 148
 ROM, 256

Routed protocol, 148
 Router, 66
 Routing, 67; 141
 Information Protocol, 148
 protocol, 141; 148
 table, 142
 update, 162

S

Same-layer interaction, 64
 SAR, 611
 Segment, 71; 185
 Server farm, 490
 Site, 490
 Sliding window, 182
 SLSM, 528
 Small Office/Home Office, 43; 490
 SNMP, 283
 SNR, 341
 Socket, 177
 SOHO, 43; 490
 SONET, 610
 SSID, 347
 cloaking, 354
 Static-Length Subnet Masking, 528
 STP, 214
 Subnet, 147; 366
 address, 383
 block, 477
 broadcast address, 372; 444
 ID, 444
 mask, 372
 number, 372
 zero, 471
 SWAN, 351

T

TAC, 511
 TCP, 174
 TCP/IP, 53
 TDM, 124
 Telnet, 246
 Temporal Key Integrity Protocol, 356
 TFTP, 180
 TKIP, 356
 Trailer, 69; 125
 Transmission Control Protocol, 62; 174
 Transmission Control Protocol/Internet
 Protocol, 53
 Trivial File Transfer Protocol, 180
 Twisted pair, 94

U

- UAA, 104
 Ubnet broadcast, 383
 UDP, 174
 UHF, 338
 Unicast
 address, 391
 IP address, 444
 U-NII, 338
 Universal Resource Locators, 61
 Unshielded Twisted Pair, 85; 231
 Unshielded Twisted-Pair, 210
 URL, 61
 User Datagram Protocol, 62; 174
 UTP, 210; 231

V

- VC, 131; 610
 VCI, 610
 Virtual
 Circuit, 131
 Private Network, 201; 492
 VLAN, 226
 Voice over IP, 492
 VoIP, 492
 VPI, 610
 VPN, 201; 492
 VTP, 294

W

- WAN, 44; 598
 WEP, 352
 Wide Area Network, 44; 598
 Wireless LAN, 332
 WLAN, 332
 WWW, 190

Z

- ZCF, 348
 Zero subnet, 471; 562

A

- Адрес, 47
 broadcast, 103
 IP, 148
 MAC, 104
 MAC, 85
 multicast, 103
 unicast, 103
 внутренний

- глобальный, 619
 локальный, 619
 канальный, 144
 логический, 146
 многоадресатный, 103; 213
 одноадресатный, 103; 213
 подсети, 372; 383; 562
 прошитый, 104
 сети, 395
 универсально управляемый, 104
 широковещательный, 103; 152; 213; 562
 направленный, 152

Адресация

- IP, 148; 150
 бесклассовая, 156
 классовая, 156
 логическая, 75; 141; 146

Алгоритм

- CSMA/CD, 99
 проверки целостности сообщений, 356

Альянс Wi-Fi, 334; 352

Асинхронная передача данных, 610

Ассоциация

- TIA, 95; 120
 телекоммуникационной
 промышленности, 95; 120

Атака

- DoS, 194; 195; 350
 доступа, 196
 отказ в обслуживании, 195
 разведывательная, 195

ATC, 599

Аутентификация, авторизации и учет, 274

Б

Базовый набор служб, 335

Байт, 149

Безопасность, 194

- беспроводной сети, 350
 эшелонированная, 197

Бесклассовая адресация, 408; 419

Бит FIN, 184

Блок, 185

- MTU, 185
 PDU, 77
 данных протокола, 77
 передачи максимальный, 185
 подсетей, 477

Брандмауэр, 194; 198

широковещательный, 224

В

Веб-адрес, 191
 Веб-браузер, 190
 Веб-сервер, 190
 Веб-страница, 190
 Взаимодействие
 на равноправных уровнях, 64
 на смежных уровнях, 64
 Виртуальная частная сеть, 492
 Вирус, 196
 Витая пара, 86; 94
 Внутренний хост, 619
 Выбор пути, 141
 Высокоуровневый протокол управления
 каналом, 125; 499

Г

Гиперссылка, 191

Д

Демаркация, 119
 Демодуляция, 601
 Десятичное представление с
 разделительными точками, 66
 Диапазон
 медицинский, 338
 нелицензируемый, 338
 частотный, 334; 337
 Домен
 коллизий, 100; 211; 223
 широковещательный, 223
 Доступ к сети, 68

Е

Емкость, 340

З

Заголовок, 69; 125
 Запрос на комментарии, 59
 Затухание, 90
 Зацикливание, 218
 Зона
 BSS, 340
 DMZ, 199
 демилитаризованная, 199
 покрытия, 341; 342

И

Идентификатор
 DLCI, 131; 610

OUI, 104
 SSID, 347
 маскировка, 354
 виртуального
 канала, 610
 маршрута, 610
 набора служб, 347
 организации, 104
 подключения канального уровня, 131
 подсети, 444; 446
 порта, 310
 сети, 395
 устройства, 310
 Импульсно-кодовая модуляция, 124; 600
 Инкапсуляция, 70; 144
 HDLC, 499; 626
 PPP, 634

Институт

ANSI, 120
 IEEE, 85; 213; 333; 352
 инженеров по электротехнике и
 электронике, 85; 88; 333
 стандартизации США, 120

Интерактивная подсказка, 250

Интересующий октет, 457

Интерфейс, 239; 286; 498

CLI, 239

внешний, 619

внутренний, 619

командной строки, 239; 270

сети VLAN 1, 283

Интерференция, 319; 341

K

Кабель
 UTP, 85; 92; 319

перекрещенный, 96

прямой, 96

Кабельное телевидение, 494; 607

Кабельный modem, 495

Канал, 601

PVC, 132

абонентский, 599

цифровой, 602

виртуальный, 131; 610

постоянный, 132; 610

связи, 130

синхронный, 121

скорость, 121

- Качество обслуживания, 187
Классовая адресация, 419
Кодирование, 94
Коллизия, 89; 92; 320; 344
 запоздалая, 320
Команда
 ping, 529
 show ip arp, 571
 traceroute, 571
Коммутатор, 100; 212
Коммутация
 без буферизации, 220
 без фрагментации, 220
 каналов, 601
 пакетов, 128; 131
 с буферизацией, 219
 фреймов, 131
Коммутируемая среда Ethernet, 102
Конвергенция, 161; 541
Контакт, 95
Конфигурационный регистр, 511; 512
Концевик, 69; 125; 144
Концентратор, 47; 91; 211
- Л**
- Линия
 арендованная, 116
 выделенная, 116; 201; 602
 демаркационная, 119
 коснольная, 248
 четырехпроводная, 128
Локальная сеть, 42
- М**
- Магическое число, 457
Маршрут
 кольцевой, 535
 стандартный, 533
 статический, 528
 резервный, 548
Маршрутизатор, 66; 494; 525
 с интегрированными службами, 492
Маршрутизация, 67; 141; 142; 157; 564
 IP, 67
 анонс, 162; 535
 петля, 535
 протокол, 148
 таблица, 142
Маска, 157
 длины
 постоянной, 528
- по умолчанию, 393
подсети, 372
Международная организация по стандартизации, 58
Метод
 DSSS, 339
 FHSS, 339
 OFDM, 340
 с ортогональным частотным разделением сигналов, 340
Метрика, 539; 547
Микросегментация, 212; 221
Модель
 OSI, 58
 TCP/IP, 59
 взаимодействия открытых систем, 54; 58
 сетевая, 53
Модем, 601
 DSL, 495
Модуль
 CSU/DSU, 118; 491; 602
 обработки данных, 118; 491
 обслуживания канала, 118; 491
Модуляция, 601
Мост, 211
Мультиплексирование, 176
 OFDM, 340
 TDM, 124
 временное, 124
 с использованием портов, 175
Мультиплексор доступа DSL, 603
- Н**
- Надежность, 181
Неэкранированная витая пара, 85; 92; 210; 231
Номер сети, 395
Нулевая подсеть, 471
- О**
- Обнаружение ошибок, 174
Одноадресатный
 IP-адрес, 150; 444
 адрес, 391
Окно
 динамическое, 182
 скользящее, 182
Оконечное оборудование канала передачи данных, 122
Октет, 149
Операционная система

Cat OS, 240
 IOS, 240
 коммутаторов Catalyst, 240
 межсетевая, 240
 Отказ в обслуживании, 194; 350

П

Пакет, 71
 ICMP эхо-ответа, 529
 Память
 NVRAM, 256
 RAM, 256
 ROM, 256
 оперативная, 256
 флеш, 256
 энергонезависимая, 256
 Передача голоса по сети IP, 492
 Площадка, 490
 Повторитель, 90
 Повторная сборка, 611
 Подкоманда, 254
 Подсеть, 147; 366
 IP, 366; 444
 нулевая, 562
 нуль, 471
 широковещательная, 562
 Подуровень
 LLC, 88
 MAC, 88
 контроля доступа к среде передачи
 данных, 88
 управления логическим каналом, 88
 Позитивное подтверждение и повторная
 передача, 183
 Поле
 контрольной суммы, 108
 типа протокола, 107
 Полоса пропускания, 121; 338
 Порт, 239; 286
 дополнительный, 498; 504
 отправителя, 179
 получателя, 177; 619
 последовательный, 121; 244
 Постоянный виртуальный канал, 369
 Преобразование
 IP- в MAC-адрес, 565
 имен, 564
 Префикс, 157; 407
 Присвоение адреса, 564
 Провайдер, 116
 служб Интернета, 44

Простейший протокол передачи
 файлов, 180
 Протокол, 57; 64
 ARP, 144; 165
 BGP, 538
 CDP, 309
 DHCP, 166
 EGP, 537
 FTP, 180
 HDLC, 125; 626
 HTTP, 60; 191
 IGP, 537
 IP, 66
 PPP, 126; 629
 RIP, 148
 SNMP, 180; 283
 SSH, 247
 TCP, 62; 174
 UDP, 62; 174; 186
 граничного шлюза, 538
 двухточечного соединения, 126; 499
 доступа к каналу связи Frame Relay, 131
 Интернета, 53; 64
 маршрутизации, 141; 148; 161
 бесклассовый, 540
 классовый, 540
 маршрутизуемый, 148
 маршрутной информации, 148
 обнаружения устройств Cisco, 309
 передачи
 гипертекста, 60; 187; 191
 данных, 53
 файлов, 87; 180
 пользовательских дейтаграмм, 62;
 174; 186
 преобразования
 IP-адресов, 144
 адресов, 163
 распределенного связующего
 дерева, 214
 сетевого уровня, 144
 управления
 передачей, 62; 174; 175
 сетью, 180; 283
 управляющих сообщений
 Интернета, 167
 целостности временного ключа, 356
 шлюза
 внешнего, 537
 внутреннего, 537
 Прямое

- лабораторное подключение, 122
подтверждение, 181
Пул DHCP, 637
- P**
- Разъем
 GBIC, 93
 RJ-45, 92
 SFP, 93
 малоформатный модульный, 93
Распределенная сеть, 598
Рассеяние, 342
Расстояние административное, 548
Рассылка
 ARP, 165
 лавинная, 217
 маршрута, 535
 многоадресатная, 213
Расширенный набор служб, 335
Режим
 асинхронной передачи, 128
 безопасности, 287
 блокирования, 218
 дуплексный, 102; 212; 287; 317
 конфигурирования, 253
 передачи данных, 218
 полудуплексный, 100; 317
 пользовательский, 248
 привилегированный, 248
Резидентская подсеть, 444
Роуминг, 336
- C**
- Сегмент, 71; 185
Сегментация, 185; 211; 611
Сеть, 147
 Ethernet, 42; 85
 DIX, 88
 коммутируемая, 102
 IP, 149; 366
 классовая, 391
 VLAN, 226
 VPN, 201
 WLAN, 332
 виртуальная частная, 201
Интернет, 44
картирование, 349
класса
 A, 151
 B, 151
 C, 151
- классовая, 150
корпоративная, 42
локальная, 81; 116
 виртуальная, 226
 территориальная, 228
малых и домашних офисов, 43
объединенная, 44; 147
распределенная, 44; 114; 116
региональная, 116
с многостанционным доступом, 130
самозащищающаяся, 197
телефонная, 598
- Сигнал оповещения о коллизии, 99
Сигнал-шум, 341
Сигнатура, 196
Симплет, 304
Синхронизация, 121; 502
Система
 IDS, 351
 IPS, 351
 автономная, 537
 номер, 538
 вторжений
 обнаружения, 201; 351
 предотвращения, 201; 351
 доменных имен, 180
Системный журнал, 282; 290
Скорость
 канала, 123
 ограничение, 612
 порта, 243
Согласованная скорость передачи, 133
Сокет, 177
Стандарт, 353
 1000BASE-T, 97
 10BASE2, 88
 10BASE5, 88
 802.11, 334
 802.11a, 335
 802.11b, 335
 802.11g, 335
 802.11i, 357
 AES, 356
 CSMA/CA, 344
 CSMA/CD, 89; 100; 220; 319
 IEEE
 802.3, 85
 IEEE
 802.2, 85
 T568A, 95
 WEP, 353

WPA, 356
 WPA2, 357
Стандартный
 маршрут, 533; 615
 шлюз, 157
Стек TCP/IP, 58
Суммирование
 автоматическое, 540
 вручную, 540
Счетчик транзитных узлов, 540

T

Таблица
 коммутации, 215
 маршрутизации, 159
 мостовая, 215
 CAM, 215
Таймер
 бездействия, 218
 обновлений, 314
 хранения информации, 314
Тактовая частота, 121
Терминальное оборудование, 122
Технология Frame Relay, 130
Точка
 демаркации, 119
 доступа, 333
 незарегистрированная, 351
Транзитный узел, 535
Трансляция
 адресов с использованием портов, 616
 сетевых адресов, 377; 616

У

Узел
 головной, 608
 транзитный, 533; 572
Улучшенный стандарт шифрования, 356
Универсальный указатель ресурсов, 61
Уровень, 59
 доступа к сети, 229
 TCP/IP, 68
 доступа к сети, 230
Интернет
 TCP/IP, 65
 канальный, 75
 представления, 74
 приложений, 74
 TCP/IP, 60

распределения, 229; 230
 сеансовый, 74
 сетевой, 75
 транспортный, 75; 174
 TCP/IP, 63
 физический, 75
 ядра сети, 231
Устройство
 DCE, 131
 DTE, 131
Утилита ping, 167
Учебная сеть Cisco, 650

Ф

Файл
 конфигурации, 257
 стартовой, 257
 текущей, 257
Ферма серверов, 490
Фильтрация
 URL, 200
 MAC-адресов, 355
 фреймов, 214
 электронной почты, 200
Фрейм, 69; 71; 125; 131; 610
Фрейм-бакен, 354
Фреймирование, 105; 125

X

Хост, 66
 IP, 67; 148

Ц

Цифровой абонентский канал, 44

III

Широковещательная подсеть, 474
Широковещательный адрес подсети, 372; 383; 444; 447
Шифрование, 351

Э

Эталонная модель, 57

Я

Ячейка, 610



Официальное руководство Cisco по подготовке к сертификационным экзаменам **CCENT/CCNA ICND1 640-822**

Третье издание

ЭТА КНИГА ПОМОЖЕТ ОСВОИТЬ
НУЖНЫЕ ТЕМЫ, В ЧАСТНОСТИ:

- модели сетей TCP/IP и OSI;
- использование сетевых маршрутизаторов и коммутаторов Cisco;
- конфигурирование и диагностика коммутаторов Ethernet;
- беспроводные локальные сети;
- IP-адресация и подсети;
- протоколы маршрутизации;
- конфигурирование и диагностика маршрутизаторов;
- безопасность в сетях;
- концепции и конфигурирование каналов распределенных сетей.

Прилагаемый DVD



Содержит два бесплатных полных экзаменационных практикума ICND1 и два бесплатных полных экзаменационных практикума CCNA, эмулятор CCNA ICND1 Network Simulator, Lite Edition и 60 минут обучающего видео на английском языке.

Минимальные системные требования для практических сертификационных тестов: операционная система Windows XP (SP3), Windows Vista (SP2) или Windows 7; наличие Microsoft .NET Framework 4.0 Client, Microsoft SQL Server Compact 4.0; процессор 1 ГГц класса Pentium (или эквивалентный); оперативная память 512 Мбайт; дисковое пространство 650 Мбайт плюс по 50 Мбайт для каждого загруженного практического экзамена.

Настоящая книга является частью серии *Official Cert Guide Series* издательства Cisco Press. Книги этой серии являются официальным первоисточником для подготовки к экзамену. Они предоставляют теоретические и практические материалы, которые помогут кандидатам на сертификат Cisco Career Certification выявить свои слабые стороны, сконцентрировать усилия по изучению и повысить уверенность в себе по мере приближения дня экзамена.

Третье издание этой книги — лучший учебник для экзаменов Cisco. Автор бестселлеров и опытный преподаватель Уэнделл Одом делится советами по подготовке к экзамену, помогая вам выявить слабые стороны, улучшить концептуальные знания и практические навыки. Книга ознакомит вас с процедурой организованной подготовки к тестам с использованием проверенных временем методов и техник обучения. Главная таблица экзаменационных тем существенно упрощает поиск. Контрольные вопросы в начале каждой главы позволяют читателю пройти самопроверку и решить, сколько времени следует потратить на каждую тему. Разделы для подготовки к экзаменам в конце каждой главы помогут запомнить самые важные концепции по каждой из тем и существенно сэкономить время на сертификационных экзаменах, что значительно увеличит вероятность успешной сдачи тестов. В последней главе даны дополнительные советы и описаны ресурсы для подготовки к сертификационному экзамену, а также приведен некоторый формальный план подготовки. Главы по поиску и устранению неисправностей помогут читателю подготовиться к решению практических задач и самым сложным заданиям сертификационного экзамена.

Данное издание было существенно переработано: обновлено содержимое, добавлены новые упражнения и расширены определенные темы, являющиеся ключом к пониманию и успеху сдачи экзаменов CCENT и CCNA. Тема IP-адресов была переписана и реорганизована так, чтобы отразить проверенные временем методики изучения концепций и специфических элементов головоломки подсетей. Кроме того, глава, посвященная моделям сетей TCP/IP и OSI, также была полностью переработана и изменена.

На прилагаемом к книге DVD содержится мощный процессор Pearson IT Certification Practice Test, укомплектованный сотнями выверенных реалистичных экзаменационных вопросов. Процессор оценивания предоставляет множество возможностей настройки и средств составления отчетов, обеспечивает полную оценку ваших знаний и поможет сосредоточиться на изучении наиболее необходимого именно для вас. В новое издание включен также бесплатный экземпляр эмулятора CCNA ICND1 640-822 Network Simulator, Lite Edition, укомплектованный лабораторными работами, которые помогут вам отточить свои практические навыки работы с пользовательским интерфейсом маршрутизаторов и коммутаторов Cisco. На DVD содержится также более чем 60-минутная видеолекция от автора на английском языке, посвященная подсетям.

Хорошо выверенный по уровню детализации, оснащенный средствами оценки, вопросами и упражнениями, этот официальный учебник поможет овладеть концепциями и методиками, которые позволят преуспеть на экзамене.

Третье издание этой книги — часть рекомендуемого учебного курса от Cisco, которое включает имитацию и практическое обучение от Cisco Learning Partners, а также средства самостоятельной подготовки от издательства Cisco Press. Чтобы получить дополнительную информацию об очных курсах под руководством сертифицированных инструкторов, электронных версиях курсов и лабораторных работах, предлагаемых партнерами по обучению компании Cisco во всем мире, посетите сайт www.cisco.com/go/authorizedtraining.

ТРЕБУЕТСЯ КОД АКТИВАЦИИ!

При регистрации ПО Pearson IT Certification Practice Test, находящегося на прилагаемом DVD, нужно ввести код активации, который выдается бесплатно всем, купившим книгу.

Пожалуйста, отправьте запрос в произвольной форме по адресу: activation_code@ciscopress.ru, в котором укажите ваши ФИО, ISBN книги, место ее приобретения и цену.



Уэнделл Одом, CCIE® №1624, один из наиболее уважаемых в мире авторов книг о сетях Cisco. Им написаны книги по сертификации Cisco начального уровня (CCENT и CCNA), сертификации более высокого (CCNP) и отраслевого (CCIE) уровня, которые отличаются технической глубиной и точностью. Уэнделл работал сетевым инженером, консультантом, системным инженером, а также инструктором и разработчиком курсов, автором книг и видео, а также программного обеспечения и блогов, связанных с сертификацией Cisco. Его веб-сайт со ссылками на различные учебные инструменты и ресурсы находится по адресу www.certskills.com.

ISBN 978-5-8459-1807-9



www.williamspublishing.com
www.ciscopress.ru
ciscopress.com

Категория: Cisco Press — сертификация
компании Cisco

Содержание: экзамены CCENT
и CCNA ICND1 640-822

12044

9 785845 918079