Официальное руководство
по подготовке к сертификационным экзаменам

Изучи, подготовься, попрактикуйся и успешно сдай экзамен!



Cisco CCNA ICND2 200-101

Маршрутизация и коммутация

Академическое издание

www.williamspublishing.com
www.ciscopress.ru
ciscopress.com

УЭНДЕЛЛ ОДОМ, CCIE® №1624

Официальное руководство
по подготовке к сертификационным экзаменам

Cisco CCNA ICND2 200-101

Маршрутизация и коммутация
Академическое издание

Официальное руководство
по подготовке к сертификационным экзаменам

Cisco CCNA ICND2 200-101 Маршрутизация и коммутация

Академическое издание

УЭНДЕЛЛ ОДОМ, CCIE® №1624



Москва • Санкт-Петербург • Киев
2015

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 CCNA ICND2 200-101: маршрутизация и коммутация, акад. изд. : Пер. с англ. — М. : ООО "И.Д. Вильямс", 2015. — 736 с. : ил. — Парал. тит. англ.

ISBN 978-5-8459-1907-6 (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 фотокопирование и запись на магнитный носитель, если на это нет письменного разрешения издательства Cisco Press.

Authorized translation from the English language edition published by Cisco Press, Copyright © 2013 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 © 2015

Научно-популярное издание
Уэнделл Одом

Официальное руководство Cisco по подготовке к сертификационным экзаменам CCNA ICND2 200-101: маршрутизация и коммутация

академическое издание

Литературный редактор *И.А. Попова*
Верстка *О.В. Мишутина*
Художественный редактор *Е.Д. Дынник*
Корректор *Л.А. Гордиенко*

Подписано в печать 25.09.2015. Формат 70x100/16
Гарнитура Times
Усл. печ. л. 59,34. Уч.-изд. л. 40,9.
Тираж 500 экз. Заказ № 5040.

Отпечатано способом ролевой струйной печати
в АО «Первая Образцовая типография»
Филиал «Чеховский Печатный Двор»
142300, Московская область, г. Чехов, ул. Полиграфистов, д.1

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

ISBN 978-5-8459-1907-6 (рус.)
ISBN 978-1-5871-4488-2 (англ.)

© Издательский дом "Вильямс", 2015
© Pearson Education, Inc., 2013

Оглавление

Введение 18

Часть I. Коммутация LAN 53

Глава 1. Концепции протокола распределенного связующего дерева 54
Глава 2. Реализация протокола распределенного связующего дерева 85
Глава 3. Поиск и устранение неисправностей коммутации LAN 119

Часть II. Маршрутизация IP версии 4 175

Глава 4. Поиск и устранение неисправностей маршрутизации IPv4. Часть I 176
Глава 5. Поиск и устранение неисправностей маршрутизации IPv4. Часть II 203
Глава 6. Создание резервного маршрутизатора первого транзитного участка 231
Глава 7. Виртуальные частные сети 254
Обзор части II 274

Часть III. Протоколы маршрутизации IP версии 4 277

Глава 8. Реализация протокола OSPF для IPv4 278
Глава 9. Концепции протокола EIGRP 315
Глава 10. Реализация протокола EIGRP для IPv4 342
Глава 11. Поиск и устранение неисправностей протоколов маршрутизации IPv4 374

Часть IV. Глобальные сети 407

Глава 12. Реализация двухточечных сетей WAN 408
Глава 13. Концепции протокола Frame Relay 440
Глава 14. Реализация протокола Frame Relay 460
Глава 15. Другие типы глобальных сетей 499

Часть V. Протокол IP версии 6 523

Глава 16. Поиск и устранение неисправностей маршрутизации IPv6 524
Глава 17. Реализация протокола OSPF для IPv6 553
Глава 18. Реализация протокола EIGRP для IPv6 584
Обзор части V 607

Часть VI. Управление сетью 611

Глава 19. Управление сетевыми устройствами 612
Глава 20. Управление файлами IOS 634
Глава 21. Управление лицензиями IOS 660

Часть VII. Подготовка к экзамену 681

Глава 22. Подготовка к сертификационному экзамену 682

Часть VIII. Приложения (в книге) 699

Приложение А. Справочные числовые таблицы 700
Приложение Б. Обновление экзамена ICND2 704
Список терминов 705
Предметный указатель 727

Приложения (на веб-сайте) 735

Приложение В. Ответы на контрольные вопросы 736
Приложение Г. Таблицы для запоминания материала 750
Приложение Д. Таблицы для запоминания материала с ответами 762
Приложение Е. Решения для диаграмм связей 775
Приложение Ж. План изучения 788

Содержание

Об авторе 15
О соавторе 15
Технические рецензенты 15
Посвящения 16
Благодарности 16

Введение **18**

Об экзаменах 18
Экзамены, позволяющие получить сертификаты CCENT и CCNA 18
Типы экзаменационных вопросов 19
Как проводится экзамен CCNA 20
Темы экзамена ICND1 21
Темы экзамена ICND2 25
Темы экзамена 200-120 CCNA 28
О книге 29
Особенности книги 29
Структура книги, главы и приложения 33
Справочная информация 36
Установка процессора Pearson IT Certification Practice Test и вопросов 36
Экзаменационные базы данных PCPT этой книги 38
О диаграммах связей 39
О приобретении практических навыков 41
Дополнительная информация 43
Условные обозначения сетевых устройств 44
Соглашения по синтаксису команд 44
От издательства 45

Первые шаги **46**

Коротко о сертификационных экзаменах Cisco 46
Рекомендации по изучению книги 47
Дополнительные задания 50
Итак, приступим 51

Часть I. Коммутация LAN **53**

Глава 1. Концепции протокола распределенного связующего дерева **54**

Основные темы 55
Обзор коммутации LAN 55
Протокол распределенного связующего дерева (IEEE 802.1D) 60
Дополнительные средства протокола STP 77
Обзор 81
Резюме 81
Контрольные вопросы 81

Ключевые темы 83
Заполните таблицы и списки по памяти 84
Ключевые термины 84

Глава 2. Реализация протокола распределенного связующего дерева 85

Основные темы 86
Настройка и проверка протокола STP 86
Поиск и устранение неисправностей STP 102
Обзор 114
Резюме 114
Контрольные вопросы 114
Ключевые темы 115
Ключевые термины 116
Таблицы команд 116

Глава 3. Поиск и устранение неисправностей коммутации LAN 119

Основные темы 120
Обобщенные методологии поиска неисправностей 120
Поиск неисправностей коммутации на уровне данных локальной сети 128
Примеры и упражнения на поиск и устранение неисправностей 150
Обзор 169
Резюме 169
Ключевые темы 169
Заполните таблицы и списки по памяти 170
Ответы на задачи примера 1 по поиску и устранению неисправностей 170
Обзор части I 171
Повторите вопросы из обзоров глав 171
Ответьте на вопросы обзора части 171
Повторите ключевые темы 171
Создайте диаграмму связей концепций протокола STP 171

Часть II. Маршрутизация IP версии 4 175

Глава 4. Поиск и устранение неисправностей маршрутизации IPv4. Часть I 176

Основные темы 178
Предсказание нормального поведения при направлении IPv4 178
Локализация проблемы с использованием команды `ping` 183
Локализация проблем с использованием команды `traceroute` 194
Обзор 201
Резюме 201
Ключевые темы 201
Ключевые термины 202

Глава 5. Поиск и устранение неисправностей маршрутизации IPv4. Часть II 203

Основные темы 204
Проблемы между хостом и стандартным маршрутизатором 204

Проблемы перенаправления пакетов между маршрутизаторами 217
Обзор 229
Резюме 229
Ключевые темы 229
Заполните таблицы и списки по памяти 230

Глава 6. Создание резервного маршрутизатора первого транзитного участка 231

Основные темы 232
Концепции протокола FHRP 232
Настройка и проверка FHRP 242
Обзор 249
Резюме 249
Контрольные вопросы 249
Ключевые темы 251
Заполните таблицы и списки по памяти 252
Ключевые термины 252
Таблицы команд 252

Глава 7. Виртуальные частные сети 254

Основные темы 255
Основы сетей VPN 255
Сети VPN на базе технологии IPSec 258
Туннели GRE 261
Обзор 270
Резюме 270
Контрольные вопросы 271
Ключевые темы 272
Заполните таблицы и списки по памяти 272
Ключевые термины 272
Таблицы команд 272

Обзор части II 274

Повторите вопросы из обзоров глав 274
Ответьте на вопросы обзора части 274
Повторите ключевые темы 274
Создайте диаграмму связей первопричин проблем IPv4 274
Создайте диаграмму связей команд FHRP 275

Часть III. Протоколы маршрутизации IP версии 4 277

Глава 8. Реализация протокола OSPF для IPv4 278

Основные темы 279
Принцип работы протокола OSPF 279
Настройка и проверка протокола OSPF 298
Обзор 310
Резюме 310
Контрольные вопросы 310

Ключевые темы 312
Заполните таблицы и списки по памяти 312
Ключевые термины 312
Таблицы команд 313

Глава 9. Концепции протокола EIGRP 315

Основные темы 316
EIGRP и дистанционно-векторные протоколы маршрутизации 316
Концепции и принцип работы протокола EIGRP 326
Обзор 338
Резюме 338
Контрольные вопросы 339
Ключевые темы 340
Заполните таблицы и списки по памяти 340
Ключевые термины 341

Глава 10. Реализация протокола EIGRP для IPv4 342

Основные темы 343
Настройка и проверка протокола EIGRP 343
Метрики EIGRP, оптимальные и резервные маршруты 351
Другие параметры конфигурации EIGRP 360
Обзор 368
Резюме 368
Контрольные вопросы 368
Ключевые темы 370
Заполните таблицы и списки по памяти 371
Ключевые термины 371
Таблицы команд 371

Глава 11. Поиск и устранение неисправностей протоколов маршрутизации IPv4 374

Основные темы 376
Методы поиска и устранения проблем в протоколах маршрутизации 376
Интерфейсы, участвующие в маршрутизации 378
Соседские отношения 387
Обзор 401
Резюме 401
Ключевые темы 401
Заполните таблицы и списки по памяти 402
Таблицы команд 402
Обзор части III 404
Повторите вопросы из обзоров глав 404
Ответьте на вопросы обзора части 404
Повторите ключевые темы 404
Создайте диаграмму связей первопричин проблем OSPF и EIGRP 404
Создайте диаграмму связей команд OSPF и EIGRP 405

Часть IV. Глобальные сети 407

Глава 12. Реализация двухточечных сетей WAN 408
Основные темы 409
Протокол HDLC в сети WAN на базе выделенных линий 409
Протокол PPP в сети WAN на базе выделенных линий 421
Поиск и устранение неисправностей в последовательных каналах 427
Обзор 435
Резюме 435
Контрольные вопросы 435
Ключевые темы 437
Заполните таблицы и списки по памяти 438
Ключевые термины 438
Таблицы команд 438

Глава 13. Концепции протокола Frame Relay 440
Основные темы 441
Обзор технологии Frame Relay 441
Адресация в технологии Frame Relay 448
Адресация сетевого уровня в среде Frame Relay 452
Обзор 457
Резюме 457
Контрольные вопросы 457
Ключевые темы 459
Заполните таблицы и списки по памяти 459
Ключевые термины 459

Глава 14. Реализация протокола Frame Relay 460
Основные темы 461
Настройка и проверка протокола Frame Relay 461
Поиск и устранение неисправностей в протоколе Frame Relay 480
Обзор 494
Резюме 494
Контрольные вопросы 494
Ключевые темы 497
Заполните таблицы и списки по памяти 497
Таблицы команд 497

Глава 15. Другие типы глобальных сетей 499
Основные темы 500
Частные глобальные сети, соединяющие предприятия 500
Открытые глобальные сети и доступ к Интернету 506
Обзор 517
Резюме 517
Контрольные вопросы 518
Ключевые темы 519
Заполните таблицы и списки по памяти 519
Ключевые термины 519

Обзор части IV 520
Повторите вопросы из обзоров глав 520
Ответьте на вопросы обзора части 520
Повторите ключевые темы 520
Создайте диаграмму связей первопричин проблем и их изоляции 520
Создайте диаграмму связей конфигурации Frame Relay 521

Часть V. Протокол IP версии 6 523

Глава 16. Поиск и устранение неисправностей маршрутизации IPv6 524
Основные темы 525
Нормальная работа протокола IPv6 525
Поиск и устранение неисправностей IPv6 537
Обзор 549
Резюме 549
Ключевые темы 549
Заполните таблицы и списки по памяти 550
Ключевые термины 550
Таблицы команд 551

Глава 17. Реализация протокола OSPF для IPv6 553
Основные темы 554
Настройка протокола OSPFv3 554
Концепции OSPF, проверка, поиск и устранение неисправностей 562
Обзор 579
Резюме 579
Контрольные вопросы 580
Ключевые темы 581
Заполните таблицы и списки по памяти 582
Ключевые термины 582
Таблицы команд 582

Глава 18. Реализация протокола EIGRP для IPv6 584
Основные темы 585
Конфигурация EIGRPv6 585
Концепции, проверка, поиск и устранение неисправностей EIGRPv6 591
Обзор 601
Резюме 601
Контрольные вопросы 602
Ключевые темы 604
Заполните таблицы и списки по памяти 604
Ключевые термины 604
Таблицы команд 604
Обзор части V. Повторите вопросы из обзоров глав 607
Ответьте на вопросы обзора части 607
Повторите ключевые темы 607
Создайте диаграмму связей поиска и устранения неисправностей 607
Создайте диаграмму связей команд OSPFV3 и EIGRPV6 608

Часть VI. Управление сетью 611

Глава 19. Управление сетевыми устройствами 612

Основные темы 613
Простой протокол управления сетью 613
Регистрация системных сообщений (системный журнал) 619
Протокол NetFlow 623
Обзор 630
Резюме 630
Контрольные вопросы 631
Ключевые темы 632
Заполните таблицы и списки по памяти 633
Ключевые термины 633

Глава 20. Управление файлами IOS 634

Основные темы 635
Управление файлами Cisco IOS 635
Восстановление пароля 645
Управление файлами конфигурации 649
Обзор 655
Резюме 655
Контрольные вопросы 656
Ключевые темы 657
Ключевые термины 658
Таблицы команд 658

Глава 21. Управление лицензиями IOS 660

Основные темы 661
Пакет IOS 661
Активация программного обеспечения IOS при универсальном образе 663
Обзор 674
Резюме 674
Контрольные вопросы 674
Ключевые темы 676
Заполните таблицы и списки по памяти 676
Ключевые термины 676
Таблицы команд 676
Обзор части VI 678
Повторите вопросы из обзоров глав 678
Ответьте на вопросы обзора части 678
Повторите ключевые темы 678

Часть VII. Подготовка к экзамену 681

Глава 22. Подготовка к сертификационному экзамену 682

Советы о самом экзамене 682
Обзор экзамена 686

Часть VIII. Приложения (в книге) 699

Приложение А. Справочные числовые таблицы 700

Приложение Б. Обновление экзамена ICND2 704

Список терминов 705

Предметный указатель 727

Часть IX. Приложения (на веб-сайте) 735

Приложение В. Ответы на контрольные вопросы 736

Приложение Г. Таблицы для запоминания материала 750

Приложение Д. Таблицы для запоминания материала с ответами 762

Приложение Е. Решения для диаграмм связей 775

Приложение Ж. План изучения 788

Об авторе

Уэнделл Одом (Wendell Odom), сертифицированный эксперт компании Cisco CCIE (Cisco Certified Internetwork Expert), № 1624, работает в сфере сетевых технологий с 1981 года. Он работал сетевым инженером, консультантом, системным инженером, инструктором и принимал участие в разработке курсов по сетям, а ныне занимается проектированием и разработкой средств сертификации. Уэнделл является автором всех предыдущих редакций серии книг *CCNA Official Certification Guide* издательства Cisco Press для подготовки к экзаменам CCNA, книг по технологиям Cisco QOS и многих других, а также одним из авторов книги *CCIE Routing and Switch*. Уэнделл консультировал также компанию Pearson при подготовке ее новой версии эмулятора CCNA 640-802 Network Simulator. Кроме того, он также поддерживает инструментальные средства обучения, ссылки на свои блоги и другие ресурсы на сайте `http://www.certskills.com`.

О соавторе

Энтони Секейра (Anthony Sequeira), CCIE No. 15626, — сертифицированный инструктор по системам Cisco (CCSI), автор почти всех уровней и курсов по сертификации Cisco. Формально Энтони начал свою карьеру в области информационных технологий в 1994 году на IBM в Тампе, штат Флорида. Он быстро создал собственную компьютерную консалтинговую компанию, Computer Solutions, а затем обнаружил свою истинную страсть: писать и обучать технологиям Microsoft и Cisco. Энтони присоединился к компании Mastering Computers в 1996 году и читал лекции о передовых компьютерных технологиях по всему миру. Компания Mastering Computers превратилась в революционно новую сетевую учебную компанию KnowledgeNet, и Энтони оставался ее преподавателем много лет. В настоящее время он собирается получить свой второй сертификат CCIE в области безопасности и очень занят преподаванием для следующего поколения KnowledgeNet, StormWind Live. Энтони является также сертифицированным специалистом VMware.

Технические рецензенты

Элан Бир (Elan Beer), CCIE No. 1837, — старший консультант и инструктор Cisco, специализирующийся на проектах многопротокольных сетей, их конфигурации, решении проблем и обслуживании сетей. За последние двадцать пять 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 техноло-

гиях 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.

Посвящения

Памяти Карсела Ланье Odom (Carcel Lanier C.L) — дедушки и отца, носившего цвета хаки, тихого, сносившего старые дома (по одному за раз), посещавшего ярмарки скота, любившего пешие прогулки и подремать во время утренней воскресной проповеди.

Благодарности

Эта книга и сопутствующая ей книга по ICND1 представляют седьмое издание в длинной серии книг издательства Cisco Press, призванных помочь в сдаче экзамена на сертификат CCENT и CCNA по маршрутизации и коммутации. С учетом столь длинной истории, начиная с первого издания в 1998 году, над этими книгами поработало множество людей. За последние пятнадцать лет в эти книги успели внести свой вклад очень много людей, осуществлявших техническое редактирование, разработку, литературное редактирование, редактирование проекта, корректуру, индексацию, управление рабочим процессом, внутренний дизайн, дизайн обложки, маркетинг и все те действия, без которых нельзя выпустить книгу. Спасибо вам всем за вашу роль в выпуске книги.

Большинство участников предыдущего издания присоединились к работе над нынешним, включая редактора проекта Дрю Каппа (Drew Cupp). Несмотря на мои частые коррекции содержимого и заголовков, Дрю удалось сохранить ясность всех деталей упорядочивая их на ходу, т.е. делая свою привычную работу: обеспечение простоты и единообразия материала по всей книге. Спасибо, Дрю, за то, что провел меня через этот путь.

Мой соавтор, Энтони Секейра, выполнил прекрасную работу, внеся свой вклад в часть книги по управлению сетью. Энтони весьма пригодился его интерес к протоколам и инструментам управления, а также практический опыт писателя и великолепные навыки преподавателя. Спасибо, что помог сделать эту книгу полней.

Что касается технического редактирования, то Элан Бир сделал свою работу, как обычно, безупречно! Он находил небольшие ошибки в перекрестных ссылках на отдельные страницы, способные ввести читателя в заблуждение и затруднить понимание некоторых фраз. И так по всем техническим вопросам. Фантастическая работа, спасибо, Элан.

Брет Бартоу (Brett Bartow) снова был исполнительным редактором книги, как и почти с самого начала выпуска этих изданий. Когда моя семья спросила меня о роли Брета за эти годы, лучшее всего подошли слова “товарищ по команде”. Брет мог бы работать в Pearson Education, но он всегда работает со мной, не упуская бизнес-вопросов и находя наилучшие способы отношения между издателем и автором. Спасибо за еще одну прекрасную работу над этой книгой, Брет!

Документы Word перебрасываются туда-сюда, пока не получится готовый красивый текст. Только благодаря Сандре Шрёдер (Sandra Schroeder), Тоне Симпсон (Tonya Simpson) и всей рабочей группе стало возможно волшебство создания из этих документов Word готовой книги. Они сделали все, от исправления моей грамматики, подбора слов и оборотов речи до последующей сборки и компоновки проекта. Спасибо, что собрали все это вместе и красиво оформили. Тоня на удивление удачно жонглировала сотнями элементов двух книг по CCNA, одновременно управляя несколькими процессами. Спасибо за это! И отдельное спасибо за внимание к подробностям.

Процесс подготовки рисунков для этих книг проходил немного не так, как для других книг. Совместно мы приложили массу усилий по модернизации рисунков обеих книг, как по дизайну, так и по содержимому, а также предоставили цветные версии для электронных книг. Особая благодарность Лоре Роббинс (Laura Robbins) за сотрудничество при работе над цветом и стандартами дизайна в этом процессе. Кроме того, благодарю Майка Танамаши (Mike Tanamachi) за рисунки и их переделку после каждых моих изменений.

Благодарю Криса Бернс (Chris Burns) из CertSkills за работу над задачами, используемыми как в приложениях, так и в книге, а также за проверку некоторых глав.

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.

Благодарю свою жену Крис. Жесткий график написания книги серьезно повлиял на то, что я хотел, но не всегда мог. Благодарю мою дочь Ханну за все исследования и работы, мешающие иногда школьным занятиям. Благодарю Иисуса Христа за возможность писать.

Введение

Об экзаменах

В первую очередь, эта книга задумана как учебник для курса изучения сетей в колледже. В то же время, если желание сделать карьеру в области телекоммуникаций появилось позже, эта книга окажет существенную помощь в этом начинании, облегчив сдачу экзамена на сертификат Cisco.

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.

Экзамены, позволяющие получить сертификаты CCENT и CCNA

Компания Cisco объявила об изменениях в сертификации CCENT и CCNA по маршрутизации и коммутации (CCNA Routing and Switching), а также в связанных с ними экзаменах 100-101 ICND1, 200-101 ICND2 и 200-120 CCNA в начале 2013 года. Для тех, кто знает, как проходили прежние экзамены Cisco ICND1, ICND2 и CCNA, скажем, что структура осталась той же. Для новичков в сертификации Cisco данное введение начинается с обсуждения основ.

Почти все новички в сертификации Cisco начинают с сертификата CCENT или CCNA. Сертификат CCENT требует примерно половины знаний и квалификации, необходимой для сертификата CCNA. Таким образом, сертификат CCENT — это более простой первый этап.

Сертификация CCENT требует только одного этапа: сдачи экзамена ICND1. Достаточно просто.

Для получения сертификата CCNA есть две возможности, как показано на рис. I.1: можно сдать экзамены ICND1 и ICND2 либо только сдать один экзамен CCNA. (Обратите внимание: для сдачи экзамена ICND2 нет никакой отдельной сертификации.)

Как можно заметить, хотя сертификат CCENT можно получить, сдав экзамен ICND1, вовсе необязательно иметь сертификат CCENT, прежде чем получать сертификат CCNA Routing and Switching. Вполне можно сдать экзамен CCNA и пропустить сертификацию CCENT.

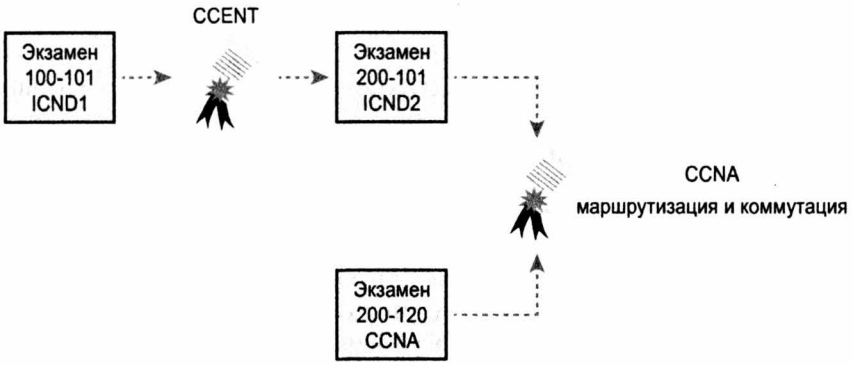


Рис. I.1. Сертификация и экзамены начального уровня компании Cisco

Что касается самих тем экзаменов ICND1 и ICND2, то они разные, лишь с небольшим количеством совпадений. Например, экзамен ICND1 рассматривает основы открытого протокола поиска первого кратчайшего маршрута (Open Shortest Path First — OSPF). На экзамене ICND2 протокол OSPF рассматривается более подробно, но обсуждение этих дополнительных подробностей полагается на основы из ICND1. Многие из тем ICND2 полагаются на разделы из ICND1, перекрывая таким образом некоторый материал.

Экзамен CCNA включает все темы экзаменов ICND1 и ICND2 — ни больше ни меньше.

Типы экзаменационных вопросов

Экзамены ICND1, ICND2 и CCNA имеют одинаковый формат. В центре сертификации претендент находится в тихой комнате наедине с компьютером. Прежде чем начнется экзамен, у каждого будет шанс выполнить несколько других заданий, например, можно решить примеры контрольных вопросов только для того, чтобы привыкнуть к компьютеру и механизму проверки. У любого, обладающего квалификацией пользователя персонального компьютера, не должно быть никаких проблем с экзаменационной системой.

После начала экзамена вопросы на экране появляются один за другим. Обычно они относятся к одной из следующих категорий:

- многовариантный выбор (Multiple Choice — MC) одного ответа;
- многовариантный выбор нескольких ответов;
- 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 в списке — фактически выбор правильного ответа. Многовариантный формат требует указать или щелкнуть на кружке около правильного ответа (ответов). Экзаменационное программное обеспечение компании Cisco традиционно указывает количество правильных ответов и не позволит выбрать

слишком много ответов. Тестлеты — это вопросы с одним общим сценарием и многовариантными вопросами в общем сценарии.

Вопросы с перетаскиванием ответов (DND) требуют перемещения мышью элементов GUI. Нажав и не отпуская левую кнопку мыши, переместите пиктограмму или кнопку на экране в другое место, а затем отпустите кнопку мыши, чтобы расположить объект где-либо в другом месте (обычно в списке). Иногда, например, чтобы дать правильный ответ, придется расположить до пяти 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. На экзамене такое задание оценивается по той конфигурации, которая была сделана, или по изменениям, внесенным в существующую конфигурацию.

Симлеты — одни из наиболее сложных экзаменационных 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.

Используя экзаменационный учебник Cisco (Cisco Exam Tutorial), можно просмотреть и даже опробовать эти типы команд. Сертификационный учебник Cisco (Cisco Certification Exam Tutorial) можно найти на сайте `http:/www.cisco.com`, если ввести "exam tutorial".

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 добывается главным образом с вполне практической целью — знать, что нужно учить больше, что меньше и что можно совсем не учить.

Компания Cisco вполне открыто предоставляет темы каждого из экзаменов. Она хочет, чтобы публике были известны и темы экзаменов, и какие именно знания и навыки потребуются для каждой темы при сдаче сертификационных тестов. Для этого компания Cisco публикует список, содержащий все темы.

Многие из экзаменационных вопросов Cisco включают темы по сети и описания. Описания демонстрируют, до какой степени должна быть понятна тема и какие навыки необходимы. Задание подразумевает также наличие определенных навыков. Например, одно задание может начинаться со слова "Опишите..." или со слов "Опишите, настройте и устраните 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

Темы экзамена ICND1 перечислены в табл. I.1–I.7. Далее, в табл. I.8–I.12, приведены темы экзамена ICND2. В этих таблицах отмечены главы, в которых затрагиваются данные экзаменационные темы.

Таблицы соответствуют организации тем Cisco и сгруппированы по темам и разделам. Разделы просто представляют более подробное описание специфических терминов и концепций тем экзаменационных задач. Основные темы в таблицах выделены полужирным шрифтом, а разделы оставлены обычным.

Таблица I.1. Темы экзамена ICND1. Работа сетей передачи данных IP

Глава	Работа сетей передачи данных IP
1–4, 6, 15	**Назначение и функции различных сетевых устройств, таких как маршрутизаторы, коммутаторы, мосты и концентраторы**
1–4, 6, 15	**Выбор компонентов сети, удовлетворяющих заданной спецификации**
5	**Наиболее распространенные приложения и их воздействие на сеть**
1	**Описание предназначения и основных принципов протоколов в моделях OSI и TCP/IP**
2–5, 6, 9, 16, 24, 25	**Передача данных между двумя хостами по сети**
2, 6, 15	**Выбор подходящей среды, кабелей, портов и разъемов для подключения сетевых устройств Cisco к другим сетевым устройствам и хостам в сети LAN**

Таблица I.2. Темы экзамена ICND1. Технологии коммутации сетей LAN

Глава	Технологии коммутации сетей LAN
2, 6	**Технологии и методы управления доступом к передающей среде для сети Ethernet**
6, 9	**Базовые концепции коммутации и работа коммутаторов Cisco**
6	Домены коллизий
6, 9	Широковещательные домены
6	Типы коммутации
6, 9	Таблица CAM
7	**Настройка и проверка начальной конфигурации коммутатора, включая управление удаленным доступом**
7	**Команды операционной системы Cisco IOS для базовой настройки коммутатора**

Окончание табл. 1.2

Глава	Технологии коммутации сетей LAN
7, 18, 28	**Проверка состояния сети и работоспособности коммутатора с помощью базовых сетевых утилит `ping`, `telnet` и `ssh`**
9	**Создание логических сегментов сети VLAN и необходимость маршрутизации между ними**
9	**Принцип сегментации сети и базовые концепции управления трафиком**
9	**Настройка и проверка сети VLAN**
9, 10	**Настройка и проверка магистрального соединения на коммутаторах Cisco**
9, 10	Протокол DTP
10	Автопереговоры

Таблица I.3. Темы экзамена ICND1. IP-адресация (IPv4/IPv6)

Глава	IP-адресация (IPv4/IPv6)
11	**Работа и необходимость использования частных и открытых IP-адресов при IPv4-адресации**
25, 26	**Выбор подходящей схемы IPv6-адресации, удовлетворяющей требованиям адресации в среде LAN/WAN**
11, 19, 20, 21	**Выбор подходящей схемы IPv4-адресации (использующей VLSM и суммирование), удовлетворяющей требования адресации в среде LAN/WAN**
27, 28, 29	**Технологические требования для запуска протокола IPv6 совместно с протоколом IPv4 как двойного стека**
25–28	**Описание IPv6-адреса**
25, 26	Глобальный одноадресатный адрес
27	Многоадресатный адрес
27	Локальный адрес канала связи
26	Уникальный локальный адрес
27	Адрес в формате eui 64
28	Автоматическая настройка

Таблица I.4. Темы экзамена ICND1. Технологии маршрутизации IP

Глава	Технологии маршрутизации IP
16	**Базовые концепции маршрутизации**
16	CEF
16	Передача пакета
16	Процесс поиска маршрутизатора
15–18, 27	**Настройка и проверка применения CLI для установки базовой конфигурации маршрутизатора**
16–18, 27	Команды Cisco IOS для базовой настройки маршрутизатора
16, 27	**Настройка и проверка состояния интерфейса Ethernet**
16–18, 27–29	**Проверка конфигурации маршрутизатора и сетевого подключения**
16–18, 27, 29	Команды Cisco IOS для просмотра базовой информации маршрутизатора и сетевого подключения

Окончание табл. 1.4

Глава	Технологии маршрутизации IP
16, 29	**Настройка и проверка конфигурации маршрутизации для статического или стандартного маршрута, согласно заданным требованиям маршрутизации**
4, 16, 17, 25, 29	**Различия методов маршрутизации и протоколов маршрутизации**
4, 17, 29	Статика или динамика
17	Состояние канала или вектор расстояния
16, 25	Ближайшая точка перехода
16, 25	Таблица IP-маршрутизации
17, 29	Пассивные интерфейсы
17, 29	**Настройка и проверка OSPF (единая область)**
17, 29	Преимущество единой области
17	Настройка OSPF v2
29	Настройка OSPF v3
17, 29	Идентификатор маршрутизатора
17, 29	Пассивный интерфейс
16	**Настройка и проверка маршрутизации между VLAN (Router on a stick)**
16	Субинтерфейсы
16	Восходящая маршрутизация
16	Инкапсуляция
8, 16	**Настройка интерфейсов SVI**

Таблица I.5. Темы экзамена ICND1. Службы IP

Глава	Службы IP
18, 28	**Настройка и проверка DHCP (маршрутизатор IOS)**
18, 28	Настройка интерфейса маршрутизатора для использования DHCP
18	Параметры DHCP
18	Исключенные адреса
18	Период резервирования
22, 23	**Типы, средства и приложения ACL**
22	Стандарт
23	Порядковые номера
23	Редактирование
23	Расширенные
23	Именованные
22, 23	Нумерованные
22	Средства регистрации
22, 23	**Настройка и проверка ACL в сетевой среде**
23	Именованные
22, 23	Нумерованные
22	Средства регистрации

Окончание табл. 1.5

Глава	Службы IP
24	**Базовые операции NAT**
24	Цель
24	Пул
24	Статический
24	1 к 1
24	Перегрузка
24	Исходная адресация
24	Односторонний NAT
24	**Настройка и проверка NAT для заданных требований сети**
23	**Настройка и проверка NTP на клиенте**

Таблица I.6. Темы экзамена ICND1. Защита сетевых устройств

Глава	Защита сетевых устройств
8, 15, 23	**Настройка и проверка средств защиты сетевых устройств**
8, 15	Защита устройства паролем
8, 15	Привилегированный режим или защита
23	Транспорт
23	Отключение telnet
8	SSH
8	VTY
23	Физическая защита
8	Служебный пароль
8	Описание основных методов аутентификации
8, 10	**Настройка и проверка средств защиты порта коммутатора**
8	Автоматическое обнаружение MAC-адресов
8	Ограничение MAC-адресов
8, 10	Статические и динамические
8, 10	Реакция при нарушении защиты
8, 10	Отключение из-за ошибки
8, 10	Отключение
8, 10	Ограничение
8	Отключение неиспользуемых портов
8	Восстановление после ошибки
8	Присвоение неиспользуемых портов неиспользуемым VLAN
23	Установка собственной сети VLAN отличной от VLAN 1
22, 23	**Настройка и проверка списков ACL для фильтрации сетевого трафика**
23	**Настройка и проверка списков ACL для ограничения обращений по telnet и SSH к маршрутизатору**

Таблица I.7. Темы экзамена ICND1. Поиск и устранение неисправностей

Глава	Поиск и устранение неисправностей
12–15, 18–21, 25–28	**Поиск и устранение распространенных проблем, связанных с настройкой хоста и IP-адресации**
9, 10	**Поиск неисправностей и решение проблем сетей VLAN**
9, 10	Идентификация настроенных сетей VLAN
9, 10	Исправление принадлежности порта
9, 10	Настройка IP-адреса
9, 10	**Поиск неисправностей и решение проблем магистрального соединения на коммутаторах Cisco**
9, 10	Исправление состояния магистрального канала
9, 10	Исправление конфигурации инкапсуляции
9, 10	Исправление разрешенных VLAN
22, 23	**Поиск неисправностей и решение проблем списков ACL**
22, 23	Статистика
22, 23	Разрешенные сети
22, 23	Направление
22, 23	Интерфейс
10	**Поиск неисправностей и решение проблем уровня 1**
10	Фреймирование
10	CRC
10	Карлики
10	Гиганты
10	Отброшенные пакеты
10	Запоздалые коллизии
10	Ошибки ввода и вывода

Темы экзамена ICND2

Темы экзамена ICND2 приведены в табл. I.8–I.12, там же содержатся ссылки на главы книги по ICND2, в которых затрагиваются темы экзамена. Обратите внимание: в каждой таблице приведена основная тема экзамена. Информация по каждой теме разделена на несколько подуровней иерархии, которые отмечены отступами.

Таблица I.8. Темы экзамена ICND2. Технологии коммутации сетей LAN

Глава	Технологии коммутации сетей LAN
1	**Идентификация дополнительных технологий коммутации**
1	RSTP
1	PVSTP
1	EtherChannels
1, 2	**Настройка и проверка работы PVSTP**
1, 2	Описание выбора корневого моста
2	Режим связующего дерева

Таблица I.9. Темы экзамена ICND2. Технологии маршрутизации IP

Глава	Технологии маршрутизации IP
20	**Процесс загрузки операционной системы Cisco IOS маршрутизатора**
20	POST
20	Процесс загрузки маршрутизатора
12	**Настройка и проверка состояния последовательного интерфейса**
20, 21	**Управление файлами Cisco IOS**
20	Параметры загрузки
20	Образ (образы) Cisco IOS
21	Лицензии
21	Просмотр лицензии
21	Смена лицензии
8–11, 16–18	**Различия методов маршрутизации и протоколов маршрутизации**
8	Административное расстояние
9	Разделение диапазона
8, 9, 17, 18	Метрика
8, 9, 17, 18	Следующий транзитный узел
8, 17	**Настройка и проверка протокола OSPF (одиночная область)**
8, 11, 17	Соседские отношения
8, 11, 17	Состояние OSPF
8, 17	Несколько областей
8	Настройка OSPF v2
17	Настройка OSPF v3
8, 17	Идентификатор маршрутизатора
8, 17	Типы сообщений LSA
9, 10, 18	**Настройка и проверка EIGRP (одиночная область)**
9, 10, 18	Приемлемое расстояние / Возможные преемники / Административное расстояние
9, 18	Условие применимости
9, 18	Композиция метрик
9, 10, 18	Идентификатор маршрутизатора
9, 10	Автоматический отчет
9, 10, 18	Выбор пути
9, 10, 18	Баланс нагрузки
9, 10, 18	Равномерный
9, 10, 18	Неравномерный
9, 10, 18	Пассивный интерфейс

Таблица I.10. Темы экзамена ICND2. Службы IP

Глава	Службы IP
6	**Выявление технологии высокой доступности (FHRP)**
6	VRRP
6	HSRP
6	GLBP
19	**Настройка и проверка системного журнала**
19	Использование вывода системного журнала
19	**Описание SNMP v2 и v3**

Таблица I.11. Темы экзамена ICND2. Поиск и устранение неисправностей

Глава	Поиск и устранение неисправностей
3, 4, 5, 16	**Поиск и устранение наиболее распространенных проблем сети**
19	**Использование данных сетевого потока**
2	**Поиск и устранение неисправностей в работе RST**
2	Корневой коммутатор
2	Приоритет
2	Правильный режим
2	Состояние порта
4, 5, 16	**Поиск и устранение проблем маршрутизации**
4, 5, 16	Разрешение маршрутизации
4, 5, 16	Правильность таблицы маршрутизации
4, 5, 16	Выбор правильного пути
11, 17	**Поиск и устранение проблем OSPF**
11, 17	Соседские отношения
11, 17	Таймеры Hello и Dead
11, 17	Область OSPF
11, 17	Максимальный блок передачи данных интерфейса
11, 17	Типы сетей
11, 17	Состояние соседей
11, 17	База данных топологии OSPF
11, 18	**Поиск и устранение проблем EIGRP**
11, 18	Соседские отношения
11, 18	Номер AS
11, 18	Балансировка нагрузки
11, 18	Разделенный диапазон
3, 5	**Поиск и устранение проблем маршрутизации interVLAN**
5	Подключение
5	Инкапсуляция
5	Подсеть

Окончание табл. I.11

Глава	Поиск и устранение неисправностей
3, 5	Собственная сеть VLAN
3, 5	Состояние режима порта магистрального канала
12, 14	**Поиск и устранение проблем реализации WAN**
12	Последовательные интерфейсы
12	PPP
14	Frame Relay
19	**Контроль статистики NetFlow**
2	**Поиск и устранение проблем EtherChannel**

Таблица I.12. Темы экзамена ICND2. Технологии WAN

Глава	Технологии WAN
15, 13, 7	**Различные технологии WAN**
15	Metro Ethernet
15	VSAT
15	Сотовый 3G / 4G
15	MPLS
12, 15	T1/E1
15	ISDN
15	DSL
13	Frame Relay
15	Кабель
7	VPN
12	**Настройка и проверка простого последовательного соединения WAN**
12	**Настройка и проверка соединения PPP между маршрутизаторами Cisco**
14	**Настройка и проверка Frame Relay на маршрутизаторах Cisco**
15	**Реализация и устранение проблем PPPoE**

Темы экзамена 200-120 CCNA

Экзамен 200-120 CCNA фактически охватывает весь материал экзаменов ICND1 и ICND2, по крайней мере исходя из опубликованных экзаменационных тем. На момент написания книги экзамен CCNA включал все темы, приведенные в табл. I.1–I.12. Короче говоря, CCNA = ICND1 + ICND2.

ВНИМАНИЕ!

Поскольку экзаменационные темы со временем могут измениться, имеет смысл перепроверить их на веб-сайте Cisco по адресу `http://www.cisco.com/go/ccent` или `http://www.cisco.com/go/ccna`. Если компания Cisco добавит впоследствии новые темы экзаменов, в приложении Б, "Обновление экзамена ICND2", описано, как перейти на сайт `http://www.ciscopress.com` и загрузить дополнительную информацию о вновь добавленных темах.

О книге

Благодаря этой книге вы приобретете знания и навыки, необходимые для сдачи экзамена 200-101 ICND2. Ее содержимое составляет вторую половину материала для экзамена CCNA ICND2, а первая содержится в первом томе академического издания.

Особенности обеих книг одинаковы, поэтому, читая второй том после первого, нет необходимости читать повторно совпадающее "Введение". Кроме того, если планируется использовать книги для подготовки к сдаче именно экзамена 200-120 CCNA, а не двух экзаменов последовательно, то имеет смысл ознакомиться с планом подготовки к экзамену, приведенным в конце данного раздела.

Особенности книги

Самая важная и вполне очевидная цель этой книги — помочь читателю получить знания и сдать экзамены ICND2. Изначально цель книги была несколько другой, поэтому название книги немного вводит в заблуждение. Тем не менее методы изложения материала, используемые в данной книге, несомненно, окажут существенную помощь в сдаче экзаменов, а также помогут читателю стать высококвалифицированным специалистом в области информационных технологий и сетей.

В книге используется несколько средств, призванных помочь читателю обнаружить свои слабые места и темы, по которым следует улучшить свои знания и навыки, запомнить концептуальные моменты и дополнительные детали, а также разобраться в соответствующих технологиях досконально. Задача книги состоит не в том, чтобы помочь читателю сдать экзамен за счет зубрежки и хорошей памяти, а в том, чтобы он понимал и изучил ключевые технологии современных телекоммуникаций. Сертификат CCNA Routing and Switching 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:

- поможет понять, какие темы экзамена следует изучить дополнительно;
- 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;
- кроме того, на веб-странице книги по адресу: `http://www.williamspublishing.com/Books/978-5-8459-1907-6.html`, можно загрузить образ DVD-диска, содержащий практические примеры и задания по рассматриваемым темам, а также дополнительное тестовое программное обеспечение для подготовки к экзамену.

Особенности глав

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.

- **Введение и темы экзамена.** Каждая глава начинается с введения, основных тем главы и списка тем официального экзамена, затронутых в этой главе.
- **Основные темы.** В этой основной части описаны протоколы, концепции и конфигурации, рассматриваемые в текущей главе.
- **Обзор.** В конце раздела основных тем каждой главы содержится раздел "Обзор", содержащий набор учебных действий, подлежащих выполнению в конце главы. Каждая глава содержит те действия, которые наиболее подходят для изучения ее тем и могут включать следующие разделы.
  - **Резюме.** Полный перечень основных тем главы. Убедитесь в полном понимании всех этих пунктов. В противном случае вернитесь к повторному изучению главы.
  - **Контрольные вопросы.** Позволяют самостоятельно оценить свой уровень знаний по темам данной главы.
  - **Ключевые темы.** 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 веб-странице книги. В другом приложении те же таблицы заполнены только частично, остальное читатель должен заполнить самостоятельно.
  - **Ключевые термины.** Хотя на экзаменах не попадаются вопросы, в которых нужно просто дать определение какого-либо термина, на экзамене CCNA требуется знание терминологии компьютерных сетей. В этом разделе перечислены основные термины главы, для которых нужно дать развернутые описания и сверить их со словарем 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, наряду 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.

Обзор части

Этот раздел призван помочь в подготовке к практическому применению всех концепций данной части книги. (Каждая часть содержит несколько взаимосвязанных глав.) Обзор части включает примеры контрольных вопросов, требующих применения концепций из нескольких глав данной части, позволяя выяснить, действительно ли поняты все темы или не совсем. Здесь также приведены упражнения на проверку памяти, позволяющие научиться в уме объединять концепции, конфигурации и способы проверки, чтобы, независимо от формулировки экзаменационного

вопроса или конкретной конфигурации, проанализировать ситуацию и ответить на вопрос.

Наряду со списком задач в обзоре части содержатся контрольные вопросы, позволяющие проследить прогресс в обучении. Ниже приведен список наиболее распространенных задач, встречающихся в разделах обзоров частей; обратите внимание, что обзоры не всех частей содержат задачи каждого типа.

- **Повторите вопросы из обзора главы.** Хотя вопросы уже были представлены в обзорах глав, повторный ответ на те же вопросы в обзоре части может быть полезен. Раздел обзора части предлагает не только повтор вопросов из обзора главы, но и использование экзаменационного приложения PCPT, поставляемого вместе с книгой, для дополнительной практики в ответах на вопросы с многовариантным выбором на компьютере.
- **Ответы на вопросы.** Экзаменационное приложение PCPT предоставляет несколько баз данных с вопросами. Одна экзаменационная база данных содержит вопросы, специально написанные для обзоров частей. Чтобы помочь в приобретении навыков, необходимых для ответов на более сложные вопросы об анализе на экзаменах, в каждый из данных вопросов включено по нескольку концепций, иногда из нескольких глав.
- **Ключевые темы.** Да, снова! Это действительно самые важные темы в каждой главе.
- **Конфигурационные диаграммы связей.** Диаграммы связей — это графические организационные инструменты, которые очень многие находят полезными при обучении и в работе для уяснения взаимодействия различных концепций. Процесс создания диаграмм связей поможет мысленно построить взаимосвязи между концепциями и командами конфигурации, а также выработать понимание отдельных команд. Диаграмму связей можно создать на бумаге или при помощи любого графического программного обеспечения на компьютере. (Более подробная информация по этой теме приведена в разделе "О диаграммах связей" введения к данной книге.)
- **Проверочные диаграммы связей.** Эти упражнения призваны помочь соотнести команды `show` маршрутизатора и коммутатора с сетевыми концепциями или командами конфигурации. Диаграммы связей можно создать на бумаге или с помощью любого подходящего программного обеспечения.
- **Повтор заданий из обзора главы.** (Необязательно.) Повтор заданий поможет лучше уяснить пройденный материал.

Подготовка к сертификационному экзамену

В последней главе, "Подготовка к сертификационному экзамену", приведен перечень действий, которые стоит предпринять при окончательной подготовке к сдаче экзамена.

Другие особенности

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

- **Тренировочные тесты на веб-сайте**. На веб-странице книги `http://www.williamspublishing.com/Books/978-5-8459-1907-6.html` есть программное обеспечение Pearson IT Certification Practice Test для самотестирования. Имея образ DVD-диска и код цифрового ваучера для этой книги, запустите специальный экзамен, который очень похож на настоящий, как по курсу ICND1 и CCNA, так и по ICND2. (Ссылка на образ DVD-диска и инструкция по получению кода цифрового ваучера указана на веб-странице данной книги по адресу: `http://www.williamspublishing.com/Books/978-5-8459-1907-6.html`.)
- **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 образа DVD-диска, загруженного с веб-страницы книги.
- **Электронная книга.** Данное академическое издание укомплектовано бесплатным экземпляром электронной книги и теста. Электронное издание представлено в трех форматах: PDF, EPUB и Mobi (исходный формат Kindle).
- **Видеолекция.** На образе DVD-диска также есть четыре видеоролика по темам протоколов OSPF, EIGRP, метрикам EIGRP, а также протоколам PPP и CHAP.
- **Дополнительные материалы на веб-сайте**. На веб-сайте `http://www.ciscopress.com/title/1587143739` 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.
- **Веб-сайт** `http://www.pearsonitcertification.com`. Это великолепный ресурс по всем темам, связанным с сертификацией IT. Обратитесь к статьям, видео, блогам и другим средствам подготовки к сертификации CCNA Routing and Switching от лучших авторов и профессиональных преподавателей.
- **Симулятор CCNA Simulator.** Если вы ищете более профессиональный практикум, то рассмотрите возможность покупки эмулятора CCNA Network Simulator. Вы можете купить экземпляр этого программного обеспечения от Pearson по адресу `http://pearsonitcertification.com/networksimulator` или в другом месте. Чтобы помочь вам в изучении, я написал руководство, которое сопоставляет каждую из этих лабораторных работ на 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 Routing and Switching. Сайт предоставляет информацию, которая поможет вам создать собственную лабораторную работу, исследовать соответствующие страницы по каждой главе этой книги и книги по ICND1, а также блоги автора CCENT Skills и CCNA Skills. Начните с адреса `http://www.certskills.com`, а затем переходите на интересующие вас вкладки.

Структура книги, главы и приложения

Книга состоит из 21 основной главы, в каждой из которых рассмотрен определенный набор тем экзамена ICND2. В последней главе представлено краткое резюме по материалам книги и даны советы по сдаче сертификационного экзамена. Краткое описание глав приведено ниже.

Часть I "Коммутация LAN"

- **Глава 1, "Концепции протокола распределенного связующего дерева"**. Рассматриваются концепции, лежащие в основе протокола распределенного связующего дерева IEEE (STP), а также то, что заставляет некоторые интерфейсы коммутатора блокировать фреймы, чтобы предотвратить их зацикливание в локальной сети с резервным коммутатором.
- **Глава 2, "Реализация протокола распределенного связующего дерева"**. Демонстрируются настройка, проверка, поиск и устранение неисправностей реализации протокола STP на коммутаторах Cisco.
- **Глава 3, "Поиск и устранение неисправностей коммутации LAN"**. Содержится обзор тем по коммутации LAN из книги ICND1, а также их более глубокое рассмотрение. В частности, рассматриваются наиболее распространенные проблемы коммутации сетей LAN, их поиск и устранение.

Часть II "Маршрутизация IP версии 4"

- **Глава 4, "Поиск и устранение неисправностей маршрутизации IPv4. Часть I"**. Содержится обзор маршрутизации IPv4, а также рассматривается применение двух ключевых инструментов поиска проблем маршрутизации: команд `ping` и `traceroute`.
- **Глава 5, "Поиск и устранение неисправностей маршрутизации IPv4. Часть II"**. Рассматриваются наиболее распространенные проблемы IPv4, поиск их первопричин и устранение.
- **Глава 6, "Создание резервного маршрутизатора первого транзитного участка"**. Обсуждается потребность в протоколе резервирования первого транзитного участка (FHRP), а также то, как протоколы заставляют несколько маршрутизаторов действовать как единый стандартный маршрутизатор. Рассматриваются подробности настройки и проверки протокола резервного маршрутизатора (HSRP), а также протокола балансировки нагрузки шлюза (GLBP).
- **Глава 7, "Виртуальные частные сети"**. Обсуждается потребность в технологии VPN при передаче данных частной сети по таким открытым сетям, как Интернет. Здесь обсуждается также базовая настройка туннелей с использованием обобщенной маршрутной инкапсуляции (GRE) на маршрутизаторах Cisco.

Часть III "Протоколы маршрутизации IP версии 4"

- **Глава 8, "Реализация протокола OSPF для IPv4"**. Содержится обзор тем по протоколу OSPF версии 2 (OSPFv2) из книги ICND1. Кроме того, детально рассматриваются их концепции с более подробным обсуждением процессов OSPF и базы данных, а также дополнительными параметрами настройки.
- **Глава 9, "Концепции протокола EIGRP"**. Знакомит с основами работы расширенного протокола маршрутизации внутреннего шлюза (EIGRP) для IPv4

(EIGRPv4), сосредоточиваясь на соседских отношениях EIGRP, вычислении метрик и скорости конвергенции при смене маршрута на резервный.

- **Глава 10, "Реализация протокола EIGRP для IPv4"**. Продолжает рассмотрение концепций, обсуждаемых в предыдущей главе, а также демонстрируется настройка и проверка этих средств.
- **Глава 11, "Поиск и устранение неисправностей протоколов маршрутизации IPv4"**. Рассматриваются наиболее распространенные проблемы протоколов маршрутизации IPv4 на чередующихся примерах применения протоколов OSPF и EIGRP.

Часть IV "Глобальные сети"

- **Глава 12, "Реализация двухточечных сетей WAN"**. Описаны основные концепции построения выделенной линии WAN, а также основы двух популярных протоколов для этих каналов связи: HDLC и PPP.
- **Глава 13, "Концепции протокола Frame Relay"**. Рассматривается построение сетей WAN Frame Relay между маршрутизаторами (акцент сделан на протоколах и концепциях, а не на конфигурации).
- **Глава 14, "Реализация протокола Frame Relay"**. Продолжает рассмотрение концепций главы 13; демонстрируются настройка, проверка, поиск и устранение неисправностей тех же средств.
- **Глава 15, "Другие типы глобальных сетей"**. Дает общее представление о многих других типах технологий WAN, включая глобальные сети Ethernet, мультипротокольную коммутацию по меткам (MPLS) и цифровой абонентский канал (DSL).

Часть V "Протокол IP версии 6"

- **Глава 16, "Поиск и устранение неисправностей маршрутизации IPv6"**. Содержится обзор тем маршрутизации IPv6, обсуждавшихся в книге ICND1. Рассматриваются некоторые из наиболее распространенных проблем маршрутизацией IPv6, поиск их первопричин и устранение.
- **Глава 17, "Реализация протокола OSPF для IPv6"**. Содержит обзор тем по протоколу OSPF версии 3 (OSPFv3) из книги ICND1. Приведено более глубокое сравнение некоторых концепций протокола OSPFv3 и уже упоминавшегося в главе 8 протокола OSPFv2.
- **Глава 18, "Реализация протокола EIGRP для IPv6"**. Продолжает обсуждение концепций протокола EIGRP, начатое для протокола IPv4 в главе 9, и демонстрирует те же концепции относительно протокола EIGRP для IPv6 (EIGRPv6). Далее рассматривается настройка и проверка протокола EIGRPv6.

Часть VI "Управление сетью"

- **Глава 19, "Управление сетевыми устройствами"**. Обсуждаются концепции и настройка трех наиболее популярных инструментальных средств управления сетью: простого протокола управления сетью (SNMP), системного журнала и NetFlow.
- **Глава 20, "Управление файлами IOS"**. Рассматривается ряд необходимых подробностей внутренней организации маршрутизатора и его операционной

системы IOS. В частности, обсуждается процесс загрузки маршрутизатора, выбор им используемого образа IOS и различных областей, где маршрутизатор может хранить свои образы IOS.

- **Глава 21, "Управление лицензиями IOS".** Описаны методы предоставления конкретному маршрутизатору Cisco прав использования определенного образа IOS и набора средств при помощи лицензий IOS.

Часть VII "Подготовка к экзамену"

- **Глава 22, "Подготовка к сертификационному экзамену".** Приведен план окончательной подготовки к сертификационному экзамену после завершения изучения книги, включая дополнительные материалы и ключевые моменты.

Часть VIII "Приложения (в книге)"

- **Приложение А, "Справочные числовые таблицы".** Состоит из нескольких таблиц с цифровой информацией, включая таблицу преобразования чисел в двоичную систему и список степеней числа 2.
- **Приложение Б, "Обновление экзамена ICND2".** Состоит из небольших тем и блоков материала для повторения пройденных тем. Это приложение время от времени обновляется и размещается по адресу `http://www.ciscopress.com/title/1587143739`. 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.
- **Список терминов** содержит определения всех терминов из разделов "Ключевые термины" в конце каждой главы.

Часть IX "Приложения (на веб-сайте)"

Перечисленные ниже приложения в цифровом формате размещены на веб-странице книги `http://www.williamspublishing.com/Books/978-5-8459-1907-6.html`.

- **Приложение В, "Ответы на контрольные вопросы".** Содержит ответы на контрольные вопросы всех глав.
- **Приложение Г, "Таблицы для запоминания материала".** Содержит ключевые таблицы и списки из всех глав, где удалена некоторая информация. Эти таблицы можно распечатать и использовать для тренировки памяти — заполнить их, не заглядывая в книгу. Их цель помочь запомнить те факты, которые могут быть полезны на экзаменах.
- **Приложение Д, "Таблицы для запоминания материала с ответами".** Содержит заполненные таблицы (т.е. фактически ответы) к приложению Г.
- **Приложение Е, "Решения для диаграмм связей".** Содержит рисунки с ответами на все упражнения с диаграммами связей.
- **Приложение Ж, "План изучения".** Таблица с основными этапами, по которой можно проследить свой прогресс в обучении.

Справочная информация

В этом коротком разделе охвачено несколько тем, доступных по ссылке из других глав. Их можно прочитать сразу, а можно пропустить и вернуться к ним позже. В частности, обратите внимание на последнюю страницу введения, где приведена контактная информация, а также указан способ связи с издательством Cisco Press.

Установка процессора Pearson IT Certification Practice Test и вопросов

Расположенный на веб-странице книги образ DVD содержит экзаменационный процессор Pearson IT Certification Practice Test (PCPT), позволяющий оценить свои знания на реалистичных экзаменационных вопросах и тестлетах. Используя процессор Pearson IT Certification Practice Test, можно учиться, находясь в режиме обучения, или смоделировать реальные условия экзамена ICND2 или CCNA.

Процесс установки состоит из двух основных этапов. Экземпляр процессора Pearson IT Certification Practice Test содержится на образе DVD, но там нет базы данных экзаменационных вопросов ICND2 и CCNA. После установки программного обеспечения PCPT его последнюю версию, а также базы данных с вопросами можно загрузить по Интернету.

Используйте цифровой ваучер для доступа к электронным версиям книги и экзаменационным вопросам

Для использования экзаменационного программного обеспечения следует задействовать цифровой ваучер продукта (инструкция по получению цифрового ваучера приведена на веб-странице книги по адресу `http://www.williamspublishing.com/Books/978-5-8459-1907-6.html`). Для этого необходимо предпринять следующее.

Этап 1 Если у вас уже есть учетная запись Cisco Press, перейдите на сайт `www.ciscopress.com/account` и зарегистрируйтесь. Если учетной записи нет, перейдите по адресу `www.ciscopress.com/join` и создайте ее

Этап 2 На странице учетной записи найдите поле Digital Product Voucher вверху правого столбца

Этап 3 Введите свой цифровой код продукта и щелкните на кнопке Submit (Передать)

ВНИМАНИЕ!

Цифровой ваучер предназначен для одноразового использования, не передавайте его третьим лицам!

Этап 4 Теперь на странице вашей учетной записи в разделе покупок появились ссылки на товары и загрузки. Для загрузки файлов электронной книги щелкайте на ссылках. Для доступа и загрузки экзаменационных вопросов Premium Edition к процессору Pearson IT Certification Practice Test, как описано в следующих разделах, используйте код доступа

Установка программного обеспечения с образа DVD

По сравнению с установкой другого программного обеспечения процесс установки данного программного обеспечения весьма прост. Если программное обеспечение Pearson IT Certification Practice Test от другого продукта компании Pearson уже установлено, нет никакой необходимости устанавливать его повторно. Просто запустите его на своем рабочем столе и активизируйте экзамены из этой книги, используя код доступа (см. предыдущий раздел). Ниже приведена последовательность действий по установке.

Этап 1 Смонтируйте образ DVD в вашей операционной системе. За инструкциями обратитесь к поисковой системе

Этап 2 Программное обеспечение будет запущено автоматически. Оно позволит получить доступ ко всему программному обеспечению Cisco Press на виртуальном DVD, включая экзаменационный процессор и приложения к книге на английском языке (скачать эти же приложения на русском языке можно по ссылке, которая приведена на веб-странице книги `http://www.williamspublishing.com/Books/978-5-8459-1907-6.html`). В главном меню щелкните на ссылке Install the Exam Engine (Установить экзаменационный процессор)

Этап 3 Отвечайте на вопросы в окнах мастера установки, как и при установке любого программного обеспечения

Процесс установки позволяет активизировать экзамены при помощи кода активизации. Этот процесс требует регистрации на веб-сайте Pearson. Поскольку регистрация необходима для активации экзамена, пожалуйста, зарегистрируйтесь, когда вас попросят. Если регистрация на веб-сайте Pearson уже есть, повторная регистрация не нужна — используйте свою уже существующую учетную запись.

Активация и загрузка экзаменационных вопросов

После установки экзаменационного процессора необходимо активизировать связанные с этой книгой экзаменационные вопросы (если это еще не было сделано в процессе установки) следующим образом.

Этап 1 Запустите программное обеспечение PCPT из меню кнопки Start (Пуск) операционной системы Windows или при помощи пиктограммы на рабочем столе

Этап 2 Для активации и загрузки связанных с этой книгой экзаменационных вопросов на вкладке My Products или Tools щелкните на кнопке Activate

Этап 3 На следующем экране введите ключ активации, указанный в продуктах Premium Edition на странице вашей учетной записи на сайте `www.ciscopress.com`. Затем щелкните на кнопке Activate

Этап 4 Процесс активации загрузит экзамен. Щелкните на кнопке Next, а затем на Finish

По завершении процесса активации на вкладке My Products должен быть указан ваш новый экзамен. Если экзамен не виден, удостоверьтесь, что перешли в меню на вкладку My Products. Теперь программное обеспечение и экзамен практики готовы к использованию. Выберите экзамен и щелкните на кнопке Open Exam.

Для обновления уже активизированного и загруженного экзамена перейдите на вкладку инструментов, а затем щелкните на кнопке Update Products. Обновление экзаменов гарантирует наличие последних изменений и обновлений данных экзамена.

Если необходимо проверить обновления к программному обеспечению PCPT, перейдите на вкладку инструментов и щелкните на кнопке Update Application. Это гарантирует наличие последней версии программного обеспечения.

Экзаменационные базы данных PCPT этой книги

Экзаменационные вопросы поставляются в различных экзаменах или экзаменационных базах данных. При установке программного обеспечения PCPT и вводе кода активации загружается последняя версия всех экзаменационных баз данных. Только по одной книге ICND1 вы получаете десять разных экзаменов или десять разных наборов вопросов (рис. I.2).

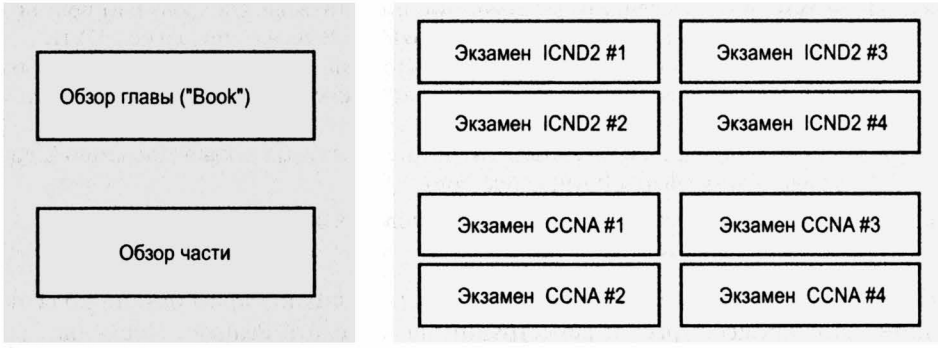


Рис. I.2. Экзамены, экзаменационные базы данных PCPT и время их использования

Любую из этих баз данных можно использовать в любое время как в режиме обучения, так и в режиме экзаменационной практики. Однако многие предпочитают отложить некоторые из экзаменов до завершения изучения всей книги. На рис. I.2 показан план, приведенный ниже.

- Во время чтения обзора части используйте процессор PCPT для обзора вопросов глав (в приложении обозначено как "Book Questions") данной части в режиме обучения.
- Во время чтения обзора части используйте вопросы, специально определенные для данной части книги (вопросы в обзоре части), в режиме обучения.
- Оставьте экзамены для использования с заключительной главой книги в режиме имитации экзамена, как описано в главе 22.

Эти два режима PCPT обеспечивают более удобный способ обучения по сравнению с реальным экзаменом, где время ограничено. В режиме обучения ответы можно просмотреть немедленно, что облегчает изучение тем. Кроме того, в базе данных можно выбрать некое подмножество вопросов, например, просмотреть вопросы только глав из одной части книги.

Режим экзамена практически имитирует фактический экзамен. Он выдает набор вопросов по всем главам и требует ответить на них за установленное время. По завершении предоставляются результаты экзамена.

Как просмотреть вопросы только обзоров глав конкретной части

Каждый обзор части содержит повтор вопросов из обзоров глав этой части. Хотя вполне можно пролистать страницы книги и найти вопросы всех обзоров глав, значительно проще просмотреть их в приложении PCPT, достаточно немного попрактиковаться в чтении вопросов на экзаменационном программном обеспечении. Но их можно прочитать и в книге.

Для просмотра вопросов обзора главы в приложении PCPT необходимо выбрать в меню пункт Book Questions (Вопросы из книги) и главы соответствующей части. Это можно сделать так.

Этап 1 Запустите программное обеспечение PCPT

Этап 2 В главном меню выберите элемент данного продукта по имени Cisco CCNA Routing and Switching ICND2 200-101 Official Cert Guide и щелкните на Open Exam

Этап 3 Вверху следующего окна должны быть перечислены экзамены. Установите флажок напротив ICND2 Book Questions и сбросьте другие флажки. Затем выберите вопросы "book", т.е. вопросы из обзоров в конце каждой главы

Этап 4 В этом же окне можно щелкнуть внизу экрана, чтобы сбросить все главы, а затем выбрать все главы необходимой части книги

Этап 5 Справа в окне выберите другие параметры

Этап 6 Для запуска набора вопросов щелкните на кнопке Start

Как просмотреть вопросы только обзоров частей

Среди предоставляемых этой книгой баз данных экзаменационных вопросов есть база, созданная исключительно для изучения обзоров частей. Вопросы в обзорах глав сосредоточены больше на фактах и простых приложениях. Вопросы в обзорах частей, напротив, больше похожи на реальные экзаменационные вопросы.

Для просмотра этих вопросов следуйте той же инструкции, что и при просмотре вопросов из обзоров глав, но вместо базы данных "Part Review" выбираете базу "Book".

Этап 1 Запустите программное обеспечение PCPT

Этап 2 В главном меню выберите элемент данного продукта по имени Cisco Cisco CCNA Routing and Switching ICND2 200-101 Official Cert Guide и щелкните на Open Exam

Этап 3 Вверху следующего окна должны быть перечислены экзамены. Установите флажок напротив Part Review Questions и сбросьте другие флажки. В результате будут выбраны вопросы из обзора в конце части

Этап 4 В этом же окне можно щелкнуть внизу экрана, чтобы сбросить все задачи, а затем выбрать те части книги, вопросы из обзоров частей которых необходимы. В результате приложение PCPT загрузит вопросы из выбранных обзоров частей

Этап 5 Справа в окне выберите другие параметры

Этап 6 Для запуска набора вопросов щелкните на кнопке Start

О диаграммах связей

Диаграммы связей — это многоцелевой организационный графический инструмент. Например, диаграммы связей применяются как альтернативный способ делать заметки.

Диаграммы связей могут также использоваться для улучшения осознания концепций. Они подчеркивают взаимосвязи и отношения между понятиями. Уделяя время обдумыванию изучаемой темы и организуя свои мысли в диаграмму связей, вы укрепляете существующие и создаете новые ассоциации в памяти, а также вырабатываете собственную систему взглядов.

Короче говоря, диаграммы связей помогут усвоить то, что вы изучаете.

Механика диаграмм связей

Каждая диаграмма связей начинается с чистого листа бумаги или окна в графическом приложении. Сначала изображается большая центральная идея с ветвями, распространяющимися в любом направлении. Ветви содержат меньшие концепции, идеи, команды, изображения, т.е. все, что должна представлять идея. Все концепции, которые могут быть сгруппированы, должны быть помещены рядом. При необходимости можно создавать все более и более глубокие ветви, хотя большинство диаграмм связей этой книги не будет превышать лишь нескольких уровней.

ВНИМАНИЕ!

Хотя о диаграммах связей написано множество книг, Тони Бузан (Tony Buzan) продолжает формализацию и популяризацию диаграмм связей. Более подробная информация о диаграммах связей приведена на его веб-сайте по адресу `http://www.thinkbuzan.com`.

На рис. I.3 приведен пример диаграммы связей, отображающей часть концепций IPv6-адресации из части VII книги. Центральная концепция диаграммы связей — IPv6-адресация, а обзор части требует обдумать все факты, относящиеся к IPv6-адресации, и организовать их в диаграмму связей. Диаграмма связей позволяет наглядней представить концепции по сравнению с их текстовым описанием.



Рис. I.3. Пример диаграммы связей

О диаграммах связей, используемых в обзорах частей

В обзорах частей предлагаются упражнения с диаграммами связей. В этом коротком разделе перечислены некоторые из подробностей об упражнениях с диаграммами связей, собранные в одном месте.

Разделы обзоров частей используют два основных упражнений с диаграммами связей.

- Упражнения на конфигурацию требуют вспомнить взаимосвязанные команды конфигурации и сгруппировать их. Например, связанные команды в упражнении на конфигурацию, являющиеся подкомандами интерфейса,

должны быть сгруппированы, но, как показано, в режиме конфигурации внутреннего интерфейса.

- Упражнения по проверке требуют подумать о выводе команд `show` и связать вывод либо с влияющими на него командами конфигурации, либо с концепциями, объясняющими значение данной части вывода.

Конфигурационные диаграммы связей можно создать на бумаге либо с помощью любого подходящего программного обеспечения и даже любого графического редактора. Существует также множество специализированных приложений диаграмм связей. Независимо от способа составления, диаграммы связей должны подчиняться следующим правилам.

- Если времени для этого упражнения мало, сэкономьте его, составив собственную диаграмму связей, а не смотрите в предложенные ответы. Обучение происходит при самостоятельном решении задачи и создании собственной диаграммы связей.
- Закройте книгу, все свои заметки и не подглядывайте в них при первом создании диаграмм. Проверьте, получится ли нарисовать их без книги, своих заметок, Google и другой помощи.
- Прежде чем заглянуть в свои заметки, пройдите все диаграммы связей, заданные в обзоре части.
- И наконец, просмотрите свои заметки, чтобы завершить все диаграммы связей.
- Получая результаты, делайте заметки, чтобы использовать их впоследствии при окончательной подготовке к экзамену.

И наконец, при обучении с использованием этих средств учтите еще две важные рекомендации. Во-первых, используйте поменьше слов для каждого узла в диаграмме связей. Следует запомнить саму концепцию и ее взаимосвязи, а не объяснить идею кому-то еще. Пишите только то, что напомнит о концепции. Во-вторых, если работа с диаграммами связей вам не подходит, откажитесь от них. Делайте вместо них просто заметки на листе бумаги. Попытайтесь выполнить важнейшую часть упражнения, размышление над взаимодействием концепций, не позволяя инструменту мешать вам.

О приобретении практических навыков

Для сдачи экзамена нужны практические навыки использования маршрутизаторов и коммутаторов Cisco, а именно работы с интерфейсом командной строки Cisco (Command-Line Interface — CLI). CLI Cisco — это текстовый пользовательский интерфейс команд и ответов, позволяющий ввести команду для устройства (маршрутизатора или коммутатора) и получить ответное сообщение. Для ответов на экзаменационные вопросы с симлетами необходимо знать множество команд и быть в состоянии переходить в нужное место интерфейса CLI, чтобы использовать эти команды.

Наилучший способ овладеть этими командами — использовать их на практике. При первом чтении части I этой книги необходимо решить, как вы планируете приобретать навыки в CLI. В следующем разделе обсуждаются возможности и средства приобретения практических навыков работы с CLI.

Возможности лабораторных работ

Для эффективной выработки практических навыков работы с CLI нужны либо реальные маршрутизаторы и коммутаторы, либо, по крайней мере, нечто, действующее, как они. Новички в технологиях Cisco обычно предпочитают другие возможности для приобретения этих навыков.

В первую очередь можно использовать реальные маршрутизаторы и коммутаторы Cisco. Можно купить новые или подержанные либо позаимствовать на работе. Их можно также взять на прокат. Можно даже арендовать виртуальный маршрутизатор или коммутатор Cisco для лабораторных работ от Cisco Learning Labs.

Эмуляторы предоставляют и другую возможность. Эмуляторы маршрутизаторов и коммутаторов — это программные продукты, подражающие поведению интерфейса CLI Cisco, как правило, в учебных целях. У этих продуктов есть дополнительное преимущество при обучении: они комплектуются упражнениями и лабораторными работами.

Эмуляторы бывают всех форм и размеров, но издатель предлагает эмуляторы, специально разработанные для помощи в подготовке экзаменов CCENT и CCNA, кроме того, они соответствуют этой книге! Эмуляторы Pearson CCENT Network Simulator и Pearson CCNA Network Simulator обеспечивают превосходную среду для практики ввода команд, а также сотни специализированных лабораторных работ, призванных помочь подготовиться к экзамену. Базовый код у обоих продуктов одинаков. Просто продукт CCNA включает лабораторные работы и для ICND1, и для ICND2, в то время как продукт CCENT имеет лабораторные работы только для ICND1.

Автор книги вовсе не указывает вам, какие средства использовать, но вам, так или иначе, придется спланировать, как получать профессиональные навыки. Просто достаточно знать, что очень многие, готовясь к этим экзаменам, практиковались в использовании интерфейса CLI Cisco.

Я (Уэнделл) собрал на своем веб-сайте `certskills.com/labgear` некоторую информацию и мнения об этом решении. Эти страницы связаны с сайтами Dynamips и Pearson Simulator. Кроме того, поскольку данной информации нет ни в каком другом месте, на этом веб-сайте описаны подробности создания лабораторных работ CCNA с использованием реальных маршрутизаторов и коммутаторов Cisco.

Коротко о Pearson Network Simulator Lite

Дискуссия о способе получения практических навыков может показаться сначала немного странной. Хорошая новость — у вас есть простой и бесплатный первый этап: книга укомплектована симулятором Pearson NetSim Lite.

Эта "облегченная" версия популярного эмулятора CCNA Network Simulator от Pearson позволяет прямо сейчас опробовать интерфейс командной строки Cisco (CLI). Нет никакой необходимости покупать реальное устройство или полнофункциональный эмулятор, чтобы начать изучение интерфейса CLI. Достаточно установить его с образа DVD.

Конечно, одна из причин наличия версии NetSim Lite на этом диске в том, что издатель надеется на покупку вами полный версии продукта. Но даже если вы не используете полную версию, то вполне можете использовать для обучения лабораторные работы версии NetSim Lite, а уже затем принимать решение о том, что использовать далее.

ВНИМАНИЕ!

Каждая из книг, ICND1 и ICND2, содержит разные версии продуктов Sim Lite с соответствующими лабораторными работами. Если вы купили обе книги, установите оба экземпляра продукта.

Дополнительная информация

Комментарии и отзывы о книге можно оставить на веб-сайте издательства `http://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 Routing and Switching. Перед тем как сдавать соответствующие сертификационные экзамены, следует проверить, не изменились ли их темы, по адресам `http://www.cisco.com/go/ccna` и `http://www.cisco.com/go/ccent`.

Книга призвана помочь сетевому специалисту в обучении сетевым технологиям и сдаче сертификационных экзаменов CCENT и CCNA Routing and Switching. 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.

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.

От издательства

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

Мы ждем ваших комментариев. Вы можете прислать письмо по электронной почте или просто посетить наш веб-сайт, оставив на нем свои замечания. Одним словом, любым удобным для вас способом дайте нам знать, нравится ли вам эта книга, а также выскажите свое мнение о том, как сделать наши книги более подходящими для вас.

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

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

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

Первые шаги

В этом разделе приведено несколько ценных советов об использовании данной книги для обучения. Уделите несколько минут чтению данного раздела, прежде чем перейти к главе 1, — это позволит извлечь больше пользы из изучения книги, независимо от того, используется ли она для подготовки к сертификационным экзаменам CCNA Routing and Switching, или только для изучения базовых концепций работы с сетями.

Коротко о сертификационных экзаменах Cisco

Компания Cisco установила довольно высокую планку для сдачи экзаменов ICND1, ICND2 и CCNA. Любой может пройти обучение и сдать экзамен, но для этого недостаточно поверхностного чтения книги и наличия денег на оплату экзамена.

Сложность этих экзаменов обусловлена множеством аспектов. Каждый из экзаменов покрывает массу концепций, а также множество команд, специфических для устройств Cisco. Кроме знаний, экзамены Cisco требуют также наличия навыков. Необходима способность анализировать и предсказывать происходящее в сети, а также правильно настраивать устройства Cisco для работы в этих сетях. Следует быть готовым к диагностике и устранению проблем, когда сеть работает неправильно.

Более сложные вопросы этих экзаменов напоминают мозаику, причем четырех фрагментов из каждых пяти, как правило, нет. Для решения задачи придется мысленно воссоздать недостающие части. Чтобы сделать это, нужно хорошо понимать все сетевые концепции и их взаимодействие. Следует также уметь сопоставить эти концепции с происходящим на устройстве и командами конфигурации, контролирующими данное устройство. Чтобы проанализировать сеть и установить, почему она работает неправильно, понадобится сопоставить концепции и конфигурацию с выводом различных команд диагностики.

Экзамен ICND2 включает много тем по поиску и устранению неисправностей. Вот пример простого вопроса: почему маршрутизатор, использующий протокол OSPFv2, может оказаться не в состоянии сформировать соседские отношения с другим маршрутизатором. Но более реалистичный экзаменационный вопрос заставил бы подумать о том, почему маршрутизатор пропустил маршрут, связана ли первопричина с протоколом OSPF, и если да, то связана ли первопричина с соседями OSPF.

Вопросы предоставляют часть информации, как детали головоломки на рис. 1. Нужно применить к фактам свое знание маршрутизации IP и теории OSPF, чтобы додумать некоторые другие части проблемы. Для этого вопроса некоторые части проблемы могут остаться тайной, но при достаточном количестве деталей головоломки нужно быть готовым ответить на вопрос.

Например, тема создания подсетей IP подразумевает хорошее знание математических механизмов. Даже простой вопрос (слишком простой, чтобы быть реальным вопросом на экзамене) показывает, что для поиска идентификаторов подсети достаточно простого сложения и умножения.

Более реалистичный экзаменационный вопрос потребует для формулировки математической задачи объединения нескольких концепций. Например, в вопросе может бы дана схема сети, для которой требуется вычислить идентификатор подсе-

ти, используемый в указанной части схемы. Но на схеме нет никаких чисел вообще. Вместо них есть только вывод команды маршрутизатора, например команды **`show ip ospf database`**, которая действительно отображает некоторые числа. Однако, прежде чем можно будет использовать эти числа, возможно, понадобится установить, как устройства настроены и что дали бы другие команды диагностики. Таким образом, вопрос будет выглядеть как головоломка на рис. 1. Части вопроса потребуется расставить по своим местам; это позволит, используя различные команды и применяя свои знания, найти другие части головоломки. В результате для данного вопроса останутся неизвестным только некоторые части.

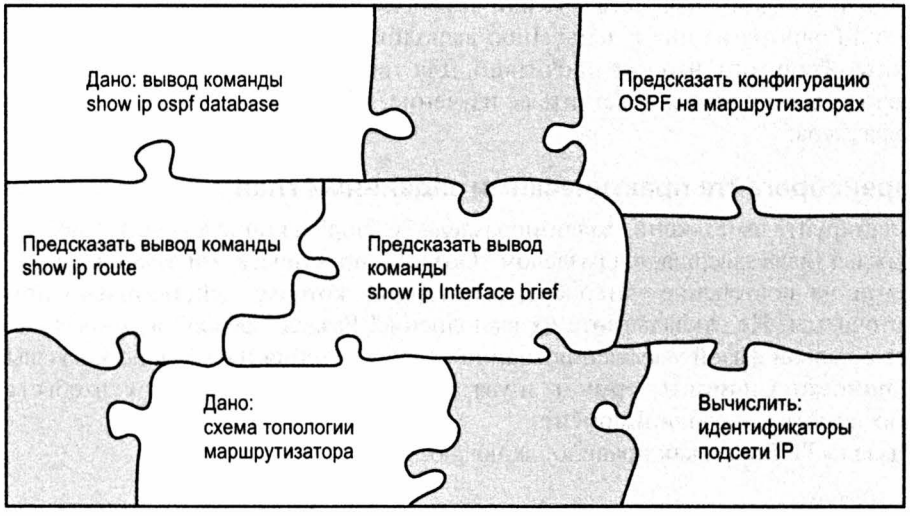


Рис. 1. Сборка головоломки требует аналитических навыков

Для приобретения таких навыков потребуется не только чтение и запоминание прочитанного. Конечно, в ходе обучения придется прочитать много страниц этой книги, узнать много фактов и запомнить взаимосвязь между ними. Однако большую часть этой книги составляет не текст, а упражнения, призванные помочь приобрести навыки для решения сетевых проблем.

Рекомендации по изучению книги

Если книга используется для изучения базовых сетевых концепций или подготовки к экзамену CCNA Routing and Switching, стоит обратить внимание на то, как именно использовать ее для достижения поставленной цели. Так что же необходимо кроме чтения и запоминания всех фактов для подготовки к сдаче экзамена CCNA Routing and Switching и успешной работы специалиста по сетям? Необходимо выработать навыки. Необходимо уметь мысленно связать каждую концепцию с другими, связанными с ней. Это потребует дополнительных усилий. Для помощи в этом ниже приведено пять ключевых точек зрения на то, как использовать настоящую книгу для приобретения этих навыков, прежде чем погрузиться в прекрасный, но сложный мир изучения работы с сетями на базе устройств Cisco.

Не одна книга, а 21 короткая задача по чтению и проверке

Считайте свое обучение набором задач по чтению и проверке всех относительно небольших взаимосвязанных тем.

В среднем каждая из основных глав этой книги (1–21) насчитывает приблизительно по 23 страницы текста. При внимательном просмотре любой из этих глав вы обнаружите раздел "Основные темы" в начале каждой главы. От него до раздела "Обзор" в конце главы насчитывается в среднем порядка 23 страниц.

Поэтому не рассматривайте эту книгу как одну большую книгу. Считайте первое чтение главы как отдельную задачу. Любой может прочитать 23 страницы, это не сложно. В каждой главе есть два или три основных раздела, и вы можете читать только по одному из них в день. Либо выполните лабораторные работы главы или сделайте обзор того, что уже прочитано. Для того чтобы материал книги был более удобочитаемым и чтобы облегчить ее изучение, она организована по темам небольшого размера.

Не пренебрегайте практическими заданиями глав

Планируйте выполнение заданий раздела "Обзор" в конце каждой главы.

Каждая глава завершается разделом "Обзор" с практическими заданиями и упражнениями на повторение материала, выполнение которых действительно помогает подготовиться. Не откладывайте их выполнение! Раздел "Обзор" в конце главы поможет с первой фазой углубления знаний и приобретения навыков по ключевым темам, поможет запомнить термины и увязать концепции в памяти так, чтобы вспомнить их в соответствующий момент.

Разделы "Обзор", как правило, включают следующее:

- Резюме
- Контрольные вопросы
- Ключевые темы
- Заполнение таблиц и списков по памяти
- Ключевые термины
- Таблицы команд
- Обзор конфигурации
- Упражнения по созданию подсетей

Используйте части книги как основные этапы

Рассматривайте книгу как шесть основных этапов, по одному на каждую главную тему.

Кроме вполне очевидной организации по главам, эта книга объединяет главы в шести основных темах, соответствующих частям книги. Завершение каждой части означает конец изучения одной из областей знаний. Уделите концу каждой части дополнительное время. Выполните в конце каждой части задачи раздела "Обзор части". Выясните свои слабые и сильные стороны. Шесть частей этой книги представлены на рис. 2.

Шесть основных этапов. Части книги

Коммутация LAN	Задачи части
Маршрутизация IP версии 4	Задачи части
Протоколы маршрутизации IP версии 4	Задачи части
Глобальные сети	Задачи части
Протокол IP версии 6	Задачи части
Управление сетью	Задачи части

Рис. 2. Части книги как основные этапы

Задания раздела "Обзор части" призваны помочь применить изученные в данной части концепции в условиях экзамена. В некоторых заданиях приведены примеры простых вопросов, чтобы можно было обдумать и проанализировать задачу. Этот процесс поможет усовершенствовать ваши знания и понять то, что было усвоено не до конца. В других заданиях используются упражнения, требующие мысленно объединить теоретические концепции с командами настройки и диагностики. Все задания раздела "Обзор части" как раз и помогут выработать необходимые навыки.

Обратите внимание: для доступа к практическим заданиям в обзорах частей требуется использовать программное обеспечение Pearson IT Certification Practice Test (PCPT). В обзорах частей требуется также повторять вопросы из обзоров глав, но используя программное обеспечение PCPT. Каждый обзор части требует также доступа к определенному набору вопросов, предназначенных для обзора концепций данной части. Программное обеспечение PCPT и базы данных экзаменационных вопросов, предоставляемые с этой книгой, дают право и на дополнительные вопросы; в главе 22 приведены дополнительные рекомендации о том, как лучше всего использовать эти вопросы для окончательной подготовки к экзамену.

Используйте главу по окончательной подготовке для совершенствования навыков

Выполняйте задания, вынесенные в заключительную главу книги.

Заключительная глава имеет две главные цели. Во-первых, она поможет углубить аналитические навыки, необходимые для ответа на более сложные вопросы экзамена. Многие вопросы требуют объединения понимания концепций со знанием конфигурации, проверки и диагностики. Простого чтения недостаточно для приобретения таких навыков, и задания данной главы окажут в этом помощь.

Задания заключительной главы помогут также выявить свои слабые стороны. Это позволит подготовиться к сложным вопросам на экзамене и выявить любые пробелы в знаниях. Большинство вопросов специально разработано так, чтобы выявить наиболее распространенные ошибки и заблуждения, а также помочь избежать части затруднений, с которыми обычно сталкиваются на реальном экзамене.

Установите цели и следите за прогрессом

И наконец, прежде чем начинать читать книгу и решать учебные задачи, уделите время выработке плана, установке неких целей и подготовьтесь к отслеживанию своего прогресса.

Создание списков задач может быть полезно, а может, и нет, в зависимости от индивидуальных особенностей, но выбор целей поможет всем, а для этого необходимо знать, какую работу предстоит выполнить.

Что касается списка решаемых при обучении задач, то не стоит его слишком детализировать. (В список можно включить все задачи из раздела "Обзор" в конце каждой главы, задачи из всех разделов "Обзор части" и задачи из заключительной главы.) Вполне достаточно списка лишь основных задач.

Для каждой обычной главы следует отследить по крайней мере две задачи: чтение раздела "Основные темы" и выполнение заданий раздела "Обзор" в конце главы. И не забывайте, конечно, задачи разделов "Обзор части" и заключительной главы. Пример плана для первой части книги приведен в табл. 1.

Таблица 1. Пример выдержки из плана

Элемент	Задача	Дата	Первая дата завершения	Вторая дата завершения (опционально)
Глава 1	Прочитать основные темы			
Глава 1	Выполнить задания обзора			
Глава 2	Прочитать основные темы			
Глава 2	Выполнить задания обзора			
Глава 3	Прочитать основные темы			
Глава 3	Выполнить задания обзора			
Обзор части I	Выполнить задания обзора части			

ВНИМАНИЕ!

Приложение Ж, "План изучения", на веб-сайте содержит полный план в виде таблицы. Эту таблицу можно изменить и сохранить в файле, чтобы отслеживать даты выполнения поставленных задач.

Используйте даты только как способ контроля за процессом обучения, а не как последний срок, к которому обязательно нужно успеть. Выбирайте реальные сроки, в которые можно уложиться. Устанавливая свои цели, учитывайте скорость чтения и объемы раздела основных тем каждой главы (его можно выяснить в оглавлении). Если закончите задачу быстрее, чем запланировано, следующие даты можете сдвинуть.

Если пропустите несколько дат, не расстраивайтесь и не пропускайте задачи в концы глав! Вместо этого подумайте о том, как скорректировать свои цели или немного плотнее поработать над обучением.

Дополнительные задания

Прежде чем читать книгу, придется выполнить еще несколько дополнительных заданий: установить программное обеспечение, найти файлы PDF и т.д. Все это

можно выполнить сейчас или когда появится перерыв в изучении первых глав книги. Но сделайте это пораньше, чтобы в случае проблем с установкой не останавливать изучения до момента их устранения.

Зарегистрируйтесь (бесплатно) в учебной сети Cisco Learning Network (CLN) по адресу `http://learningnetwork.cisco.com` и присоединяйтесь к группам по изучению CCENT и CCNA. Это позволит участвовать в обсуждениях тем, связанных с экзаменами CCENT (ICND1) и CCNA (ICND1 + ICND2). Зарегистрируйтесь, присоединитесь к группе и установите фильтр на электронную почту, чтобы перенаправлять сообщения в отдельную папку. Даже если нет времени читать все сообщения сразу, можете сделать это и позже, когда оно будет, или просто просмотреть темы сообщений в поисках интересных. Либо можно просто искать интересные сообщения на веб-сайте CLN.

Найдите и распечатайте копию приложения Г, "Таблицы для запоминания материала". Это задание используется в большинстве обзоров глав. Даны незаполненные таблицы, заполнение которых поможет запомнить ключевые факты.

Если вы купили электронную версию книги, найдите и загрузите файлы соответствующих ресурсов (видео и программное обеспечение Sim Lite) согласно инструкции на последней странице файла электронной книги в разделе "Где сопутствующие файлы?"

Установите экзаменационное программное обеспечение PCPT и активизируйте его экзамены. Более подробная информация о загрузке программного обеспечения приведена в разделе "Install the Pearson IT Certification Practice Test Engine and Questions" инструкции.

И наконец, установите программное обеспечение Sim Lit (если еще не куплена полная версия эмулятора). Эмулятор Sim Lit, поставляемый с этой книгой, содержит лишь часть упражнений и лабораторных работ полной версии Pearson Network Simulator.

Итак, приступим

Теперь приступим к первой из многих коротких задач: чтению главы 1. Наслаждайтесь!

В этой части внимание сосредоточено на теме сетей LAN Ethernet. Практически предпосылкой написания книги стало множество фундаментальных тем LAN Ethernet. Сертификация CCENT и настоящее академическое издание содержат довольно глубокое изложение тем локальных сетей Ethernet — им посвящено порядка 20% объема.

Часть I повторяет темы LAN Ethernet для экзамена CCNA, а также темы, включенные в экзамен CCENT. В частности, в главах 1-2 обсуждаются концепции настройки и проверки протокола распределенного связующего дерева (STP). Кроме того, здесь содержится обзор большей части тем экзамена CCENT по сетям LAN Ethernet, который поможет не только вспомнить некоторые из деталей, но и подготовить к изучению поиска и устранения неисправностей в локальных сетях Ethernet (глава 3).

Часть I. Коммутация LAN

Глава 1. “Концепции протокола распределенного связующего дерева”

Глава 2. “Реализация протокола распределенного связующего дерева”

Глава 3. “Поиск и устранение неисправностей коммутации LAN”

Обзор части I

Глава 1

Концепции протокола распределенного связующего дерева

Протокол *распределенного связующего дерева* (Spanning Tree Protocol — STP) предоставляет локальным сетям Ethernet дополнительные преимущества по установке избыточных каналов связи в локальной сети, а также помогает преодолеть известные проблемы, связанные с дополнительными каналами связи. Использование избыточных каналов связи в проекте позволяет сети LAN продолжать работу не только при отказе некоторых каналов связи, но даже некоторых коммутаторов. В надлежащем проекте сети LAN должно быть достаточно избыточности, чтобы никакая единая точка отказа не нарушила ее работу; протокол STP позволяет проекту использовать избыточность, не создавая других проблем.

В настоящей главе рассматриваются концепции протокола STP. В частности, обсуждается, почему локальные сети нуждаются в протоколе STP, что он делает для решения определенных проблем в локальных сетях с избыточными каналами связи и как осуществляет свою работу. Глава состоит из двух основных разделов: в первом рассматриваются базовые функции протокола STP, во втором — его дополнительные средства.

Но прежде чем перейти к протоколу STP, уделим внимание краткому обзору тем по сетям LAN. Некоторым из читателей этой книги хорошо известно о коммутации LAN, перенаправлении фреймов, таблицах MAC-адресов и обо всем, что происходит в локальных сетях Ethernet. Возможно, кто-то из читателей недавно получил свой сертификат CCENT, сдав экзамен ICND1, а кто-то только закончил читать первый том книги. Однако некоторые из подробностей, возможно, стоит освежить в памяти. Поэтому первый раздел данной главы содержит краткий обзор некоторых из важнейших тем по сетям Ethernet из книги по ICND1, чтобы, читая о протоколе STP, не пришлось припоминать детали сетей Ethernet.

В этой главе рассматриваются следующие экзаменационные темы
Технологии коммутации сетей LAN
Идентификация дополнительных технологий коммутации
RSTP
PVSTP
EtherChannels
Настройка и проверка работы PVSTP
Описание выбора корневого моста

Основные темы

Обзор коммутации LAN

ВНИМАНИЕ!

Этот раздел содержит обзор тем по коммутации LAN экзамена ICND1 и сертификата CCENT. Не стесняйтесь просто просмотреть или пропустить следующий основной раздел, "Протокол распределенного связующего дерева (IEEE 802.1D)", если хорошо помните темы по локальным сетям Ethernet.

Современные локальные сети состоят из проводных и беспроводных соединений со множеством устройств. Эти соединения обеспечивают любому устройству средства передачи и получения данных от других устройств в сети. Совместно с соединениями WAN и Интернетом, подключенные к локальной сети устройства могут общаться с другими устройствами в других частях корпоративной сети и во всем мире.

Проводные части современных локальных сетей используют стандарты Ethernet и коммутаторы LAN. Стандарты Ethernet определяют характеристики кабельной проводки, а также правила канального уровня, включая фреймирование и адреса. Физически локальная сеть Ethernet может быть маленькой или большой, но она включает три основных компонента:

- устройства с платой сетевого интерфейса Ethernet (NIC);
- коммутаторы LAN Ethernet;
- соединяющие устройства кабели (сетевые платы — с портам коммутатора, порты коммутатора — друг с другом и т.д.)

На рис. 1.1 приведен пример с шестью компьютерами, подключенными к одному коммутатору LAN.

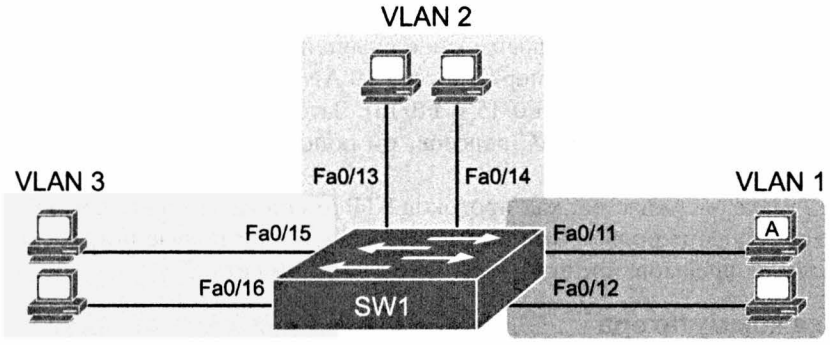


Рис. 1.1. Небольшая локальная сеть Ethernet с сетями VLAN

Логика перенаправления коммутатора LAN

Протокол STP ограничивает выбор направлений перенаправления коммутатором фреймов с целью предотвращения проблем с петлями. Эта проблема возникает

потому, что в некоторых случаях базовая логика коммутатора LAN буквально перенаправляет фрейм в сети LAN по бесконечному кругу, если нет такого внешнего метода, как протокол STP, позволяющего предотвратить это. Таким образом, чтобы понять логику протокола STP, необходимо вспомнить базовую логику коммутатора LAN, особенно логику перенаправления. Тогда станет понятно, почему без протокола STP фреймы могут передаваться по кругу и как он предотвращает петли.

Ниже описаны этапы перенаправления фреймов коммутатором LAN при игнорировании роли протокола STP.

Ключевая тема

Резюме по логике перенаправления коммутатора LAN

Этап 1 Определить сеть VLAN, в которую должен быть перенаправлен фрейм, следующим образом:

A. Если фрейм поступает на интерфейс доступа, использовать сеть доступа VLAN интерфейса

B. Если фрейм поступает на магистральный интерфейс, использовать сеть VLAN, указанную в магистральном заголовке фрейма

Этап 2 Добавить MAC-адрес отправителя в таблицу MAC-адресов, указав входящий интерфейс и идентификатор VLAN

Этап 3 Найти MAC-адрес получателя фрейма в таблице MAC-адресов, но только среди записей о VLAN, выявленных на этапе 1. Использовать один из следующих этапов, в зависимости от того, найден ли MAC-адрес получателя

A. Найден. Перенаправить фрейм через единственный интерфейс, указанный в найденной записи таблицы адресов

B. Не найден. Разослать фрейм на все остальные порты доступа в той же сети VLAN и на все порты магистрального канала, для которых эта сеть VLAN указана как полностью поддерживаемая (активная, в списке разрешенных, не сокращена, маршрутизируется STP)

Предположим, например, что фрейм в сети на рис. 1.1 послан компьютером A. Согласно рисунку, порт F0/11 коммутатора находится в сети VLAN 1, поэтому на этапе 1 коммутатор определяет фрейм как находящийся в сети VLAN 1. Коммутатор не перенаправил бы фрейм на порты в сети VLAN 2 (интерфейсы F0/13 и F0/14) или сети VLAN 3 (интерфейсы F0/15 и F0/16). Затем коммутатор нашел бы MAC-адрес получателя в таблице MAC-адресов, но поиск осуществляется только среди записей для сети VLAN 1.

Далее в главе обсуждается, как протокол STP вмешивается в эту логику, ограничивая интерфейсы, используемые коммутатором как при получении, так и при перенаправлении фреймов, предотвращая таким образом петли.

Проверка коммутатора

Логика коммутатора LAN очень проста, для ее описания действительно достаточно лишь нескольких строк, поскольку потенциально коммутаторы должны быть способны перенаправлять миллионы фреймов в секунду. Получить фрейм, определить сеть VLAN, соотнести MAC-адрес получателя с MAC-адресом в таблице, выбрать исходящий интерфейс и перенаправить фрейм. Однако смысл команд `show` может быть трудно понять, особенно если использовать их в реальных сетях не каж-

дый день. Данный раздел содержит обзор нескольких ключевых команд show, которые окажутся полезными при рассмотрении протокола STP.

Просмотр таблицы MAC-адресов

Первый пример выводит таблицу MAC-адресов на двух коммутаторах, SW1 и SW2, как показано на рис. 1.2. Рисунок демонстрирует концепцию таблиц MAC-адресов на примере двух компьютеров и одного маршрутизатора, находящихся в сети VLAN 10. Пример 1.1 демонстрирует вывод команды show mac address-table dynamic, отображающей все динамически изученные записи таблицы MAC-адресов на коммутаторе для всей сети VLAN.

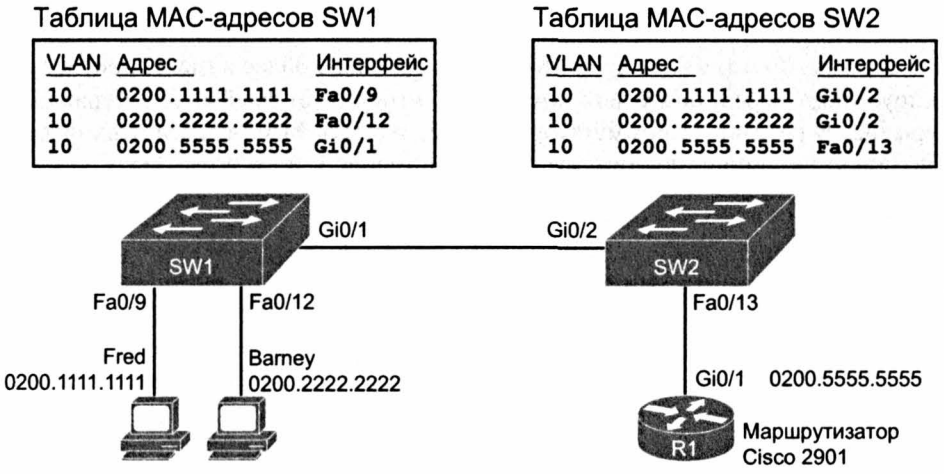


Рис. 1.2. Пример сети LAN с таблицами MAC-адресов

Пример 1.1. Исследование записей таблиц MAC-адресов на коммутаторах SW1 и SW2

```
SW1# show mac address-table dynamic
          Mac Address Table
-------------------------------------------
Vlan  Mac Address     Type       Ports
----  -----------     --------   -----
  10  0200.1111.1111  DYNAMIC    Fa0/9
  10  0200.2222.2222  DYNAMIC    Fa0/12
  10  0200.5555.5555  DYNAMIC    Gi0/1


SW2# show mac address-table dynamic
          Mac Address Table
-------------------------------------------
Vlan  Mac Address     Type       Ports
----  -----------     --------   -----
  10  0200.1111.1111  DYNAMIC    Gi0/2
  10  0200.2222.2222  DYNAMIC    Gi0/2
  10  0200.5555.5555  DYNAMIC    Fa0/13
```

Обратите внимание, что вывод каждой команды на каждом коммутаторе повторяет в основном ту же информацию таблицы MAC-адресов, представленную на рис. 1.2. Оба коммутатора изучили все три MAC-адреса, поэтому каждое из этих трех устройств может посылать фреймы, которые достигнут обоих коммутаторов. Но у каждого коммутатора разная информация перенаправления (порт). Например, в таблице MAC-адресов MAC-адресу компьютера Fred (0200.1111.1111) на коммутаторе SW1 соответствует порт Fa0/9, а на коммутаторе SW2 — порт Gi0/2. Эта графа в таблице указывает локальному коммутатору, на какой из его локальных портов перенаправить фрейм.

Протокол STP не оставляет никаких пометок или примечаний в выводе этой команды. Но он влияет на набор портов, для которых коммутатор может изучать MAC-адреса, таким образом, протокол STP косвенно изменяет то, что выводит команда `show mac address-table`. Как будет отмечено далее в главе, протокол STP блокирует порт, в результате чего коммутатор игнорирует фреймы, поступающие на интерфейс. В результате коммутатор не будет изучать MAC-адреса этих фреймов, что повлияет на записи таблицы, выводимые командой `show mac address-table`.

Определение сети VLAN фрейма

Процесс перенаправления коммутатора уровня 2 подразумевает перенаправление фрейма в контексте одной сети VLAN. Таким образом, фрейм поступает на коммутатор, и он должен определить сеть VLAN, из который прибыл фрейм. Затем коммутатор уровня 2 перенаправляет фрейм на порты только в той же сети VLAN или на порты магистрального канала, поддерживающего эту сеть VLAN.

Порты коммутатора Cisco работают либо как порты доступа, либо как порты магистрального канала, и тип порта определяет, как коммутатор рассматривает сеть VLAN входящего фрейма. У порта доступа интерфейс коммутатора ассоциируется с одной сетью VLAN. Фреймы, поступившие на порт доступа, считаются частью сети доступа VLAN, заданной подкомандой интерфейса `switchport access vlan` *`идентификатор_vlan`*. Фрейм для портов магистрального канала поступает с тегом VLAN в заголовке магистрального канала; этот тег задает идентификатор сети VLAN.

В примере 1.2 содержится вывод нескольких команд `show`, отображающих информацию об интерфейсах коммутатора и связанных с ними сетях VLAN. Команда `show interfaces status` выводит все интерфейсы коммутатора и их текущее состояние. Здесь также указано, работает ли порт как интерфейс VLAN, как порт доступа, или засвидетельствован факт, что порт работает как магистральный канал.

Пример 1.2. Отображение интерфейсов и сетей VLAN

```
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          connected   10       auto    auto   10/100BaseTX
Fa0/10         notconnect  1        auto    auto   10/100BaseTX
Fa0/11         connected   1      a-full      10   10/100BaseTX
Fa0/12         connected   10       half     100   10/100BaseTX
Fa0/13         connected   1      a-full    a-100   10/100BaseTX
Fa0/14         disabled    1        auto    auto   10/100BaseTX
Fa0/15         connected   3        auto    auto   10/100BaseTX
Fa0/16         connected   3      a-full     100   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 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
                                                Fa0/10, Fa0/11, Fa0/13, Fa0/14
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Gi0/2
3    VLAN0003                         active    Fa0/15, Fa0/16
10   WO-example                       active    Fa0/9, Fa0/12
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

В нижней части примера приведен вывод команды `show vlan brief`, отображающий все сети VLAN со списком всех соответствующих им портов доступа. (Обратите внимание: эти команды соответствуют схеме сети на рис. 1.2.)

Уделим минуту, чтобы снова подумать о задаче протокола STP. Протокол STP не оказывает никакого влияния ни на одну из команд в примере 1.2. Например, в команде `show interfaces status` протокол STP не изменяет присвоение VLAN, состояние магистрального канала или состояние интерфейса с `connected` на другое. Протокол STP требует использования команд, начинающихся на `show spanning-tree`, с информацией, применимой ко всем интерфейсам, будь то интерфейсы доступа, магистральные линии или поддерживаемые ими VLAN.

Проверка магистральных каналов

Заключительная тема обзора посвящена выводу команды коммутаторов LAN, которая, в отличие от предыдущих, действительно представляет прямую "улику" деятельности протокола STP — команду `show interfaces trunk`.

Интерфейсы коммутатора Cisco будут работать в магистральном режиме VLAN, если они настроены правильно на обоих концах магистрального канала. Магистральный канал может поддерживать все сети VLAN, известные локальному коммутатору. Но магистральный канал может решить не перенаправлять фреймы для некой сети VLAN в связи с различиями функций коммутаторов; одной из этих функций является протокол STP.

Команда `show interfaces trunk` демонстрирует несколько важных идей. В первую очередь, она выводит только работающие в настоящее время магистральные каналы и не выводит магистральные каналы, которые могли бы "договориться" о магистральном соединении в будущем. Она также выводит сети VLAN, для которых коммутатор в настоящее время перенаправляет фреймы, в последней строке вывода для каждого порта (пример 1.3).

Пример 1.3. Команда show `interfaces trunk` с подробностями последнего списка VLAN

```
SW1# show interfaces trunk

Port     Mode         Encapsulation     Status      Native vlan
Gi0/1    desirable    802.1q            trunking    1

Port     Vlans allowed on trunk
Gi0/1    1-4094

Port     Vlans allowed and active in management domain
Gi0/1    1, 3, 10

Port     Vlans in spanning tree forwarding state and not pruned
Gi0/1    1, 3, 10
```

Вывод этой команды имеет четыре группы сообщений. Первая демонстрирует список работающих магистральных каналов и их параметров. Следующие три выводят сети VLAN, поддерживаемые на каждом магистральном канале, в порядке все более ограничивающих списков. Любая VLAN, выведенная в заключительном (выделенном) списке, способна передавать и получать через этот порт. В данном случае порт Gi0/1 коммутатора SW1 перенаправит фреймы для сетей VLAN 1, 3 и 10, но не для любых других.

Эта команда важна для протокола STP потому, что она выводит информацию, на которую протокол STP воздействует непосредственно. Протокол STP использует для каждой сети VLAN состояние *перенаправления* (forwarding) и *блокировки* (blocking) порта. Если протокол STP блокирует порт определенной VLAN, то ее не будет в заключительном списке внизу вывода команды `show interfaces trunk`. (Настройка и проверка протокола STP, а также примеры блокировки STP и их влияние на вывод этой команды приведены в главе 2.)

Протокол распределенного связующего дерева (IEEE 802.1D)

Без *протокола распределенного связующего дерева* (Spanning Tree Protocol — STP) локальная сеть с избыточными каналами связи могла бы передавать фреймы Ethernet по кругу неопределенно долгое время. Протокол STP позволяет блокиро-

вать некоторые порты коммутатора так, чтобы они не передавали фреймы. Протокол STP разумно выбирает блокируемые порты с учетом двух задач.

- Все устройства в сети VLAN способны передавать фреймы на все другие устройства. Т.е. блокировать следует не слишком много портов, чтобы не отрезать одни части сети LAN от других.
- Фреймы имеют короткую продолжительность существования, что не позволит передавать их по кругу неопределенно долго.

Протокол STP соблюдает баланс, позволяя доставлять фреймы каждому устройству, но не вызывать проблем, связанных с круговой передачей фреймов по сети.

Для предотвращения круговой передачи фреймов протокол STP добавляет дополнительную проверку на каждом интерфейсе, прежде чем коммутатор использует его для передачи или получения пользовательского трафика. Проверка такова: если порт находится в состоянии перенаправления для данной сети VLAN, то использовать его, как обычно; если он находится в состоянии блокировки, блокировать весь пользовательский трафик, не посылать и не передавать пользовательский трафик на этом интерфейсе для данной сети VLAN.

Отметим, что эти состояния STP не изменяют другую информацию, уже известную об интерфейсах коммутатора. Состояние интерфейса `connected/notconnect` не изменяется. Рабочее состояние интерфейса, доступа или магистрального канала не изменяется. Протокол STP добавляет свое дополнительное состояние, *состояние блокировки* (blocking state), просто отключая интерфейс.

Хоть и разными способами, но эти два последних параграфа подводят итог того, что делает протокол STP. Однако подробности того, как именно протокол STP осуществляет свою работу, могут потребовать длительного изучения и практики. Второй основной раздел этой главы начинается с объяснения необходимости в протоколе STP и фундаментальных идеях, благодаря которым протокол STP решает проблемы циклической передачи фреймов. Большая часть этого раздела посвящена выбору протоколом STP блокируемых портов коммутатора для решения своих задач.

Потребность в связующем дереве

Протокол STP предотвращает три общих проблемы локальных сетей Ethernet, возникающих при наличии в локальной сети избыточных каналов связи и отсутствии протокола STP. Фактически все три проблемы — это побочные эффекты циклической передачи некоторых фреймов Ethernet на протяжении довольно продолжительного времени (часов, дней или даже постоянно, пока не откажут устройства или каналы связи сети LAN).

Даже один фрейм, передаваемый в сети по кругу, может вызвать *широковещательный шторм* (broadcast storm). Широковещательный шторм происходит тогда, когда широковещательные, многоадресатные или одноадресатные фреймы для неизвестного получателя циклически передаются по сети LAN. Широковещательные штормы способны заполнить все каналы связи копиями этого одного фрейма, вытесняя полезные фреймы, а также значительно снижая производительность компьютера конечного пользователя, заставляя его обрабатывать слишком много широковещательных фреймов.

Чтобы помочь понять, как это происходит, на рис. 1.3 приведен пример сети, где компьютер Bob посылает широковещательный фрейм. Пунктирные линии показывают, как коммутаторы перенаправляют фрейм без протокола STP.

ВНИМАНИЕ!

Первоначальный широковещательный фрейм может быть также послан по кругу в противоположном направлении, когда коммутатор SW3 пошлет копию первоначального фрейма через свой порт Gi0/1. На рисунке это не показано, чтобы не загромождать его.

Помните описанную ранее логику сети LAN? Она требует от коммутатора передать широковещательный фрейм на все интерфейсы в той же сети VLAN, кроме того интерфейса, на который прибыл фрейм. Согласно рисунку, это означает, что коммутатор SW3 перенаправит фрейм, полученный с компьютера Bob, на коммутатор SW2, а он перенаправит фрейм на коммутатор SW1, который, в свою очередь, перенаправит его назад, на коммутатор SW3, а тот снова перенаправит его на коммутатор SW2.

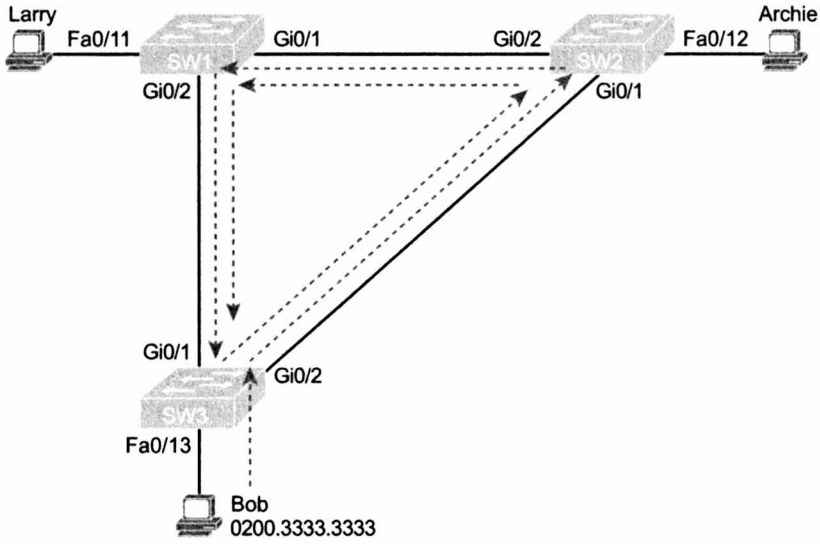


Рис. 1.3. Широковещательный шторм

Когда происходит широковещательный шторм, как на рис. 1.3, фреймы передаются бесконечно, пока что-то не изменится: отключится интерфейс, перезагрузится коммутатор или еще нечто нарушит цикл. Обратите также внимание, что все то же самое происходит и в противоположном направлении. Когда компьютер Bob передает первоначальный фрейм, коммутатор SW3 перенаправляет его копию и на коммутатор SW1, он — на коммутатор SW2 и т.д.

Циклическая передача фреймов вызывает также проблему неустойчивости таблицы MAC-адресов. Неустойчивость таблицы MAC-адресов означает, что информация таблицы MAC-адресов коммутатора постоянно изменяется, занося MAC-адрес отправителя циклически передаваемого фрейма. Например, коммутатор SW3

на рис. 1.3 начинает со следующий записи таблицы MAC-адресов для компьютера Bob (см. рис. 1.3, *снизу*):

```
0200.3333.3333   Fa0/13   VLAN 1
```

Теперь рассмотрим процесс обучения коммутатора, происходящий при передаче циклического фрейма на коммутатор SW2, затем на коммутатор SW1, а затем назад, на интерфейс Gi0/1 коммутатора SW3. Коммутатор SW3 думает так: "Хм ... MAC-адрес отправителя 0200.3333.3333, а фрейм поступил на мой интерфейс Gi0/1. Изменю свою таблицу MAC-адресов!" и создает следующую запись:

```
0200.3333.3333   Gi0/1   VLAN 1
```

На настоящий момент коммутатор SW3 сам не может правильно доставить фрейм по MAC-адресу компьютера Bob. Если на коммутатор SW3 поступает фрейм, предназначенный для компьютера Bob (другой фрейм, а не передаваемый по кругу и приведшей к проблеме), коммутатор SW3 ошибочно направит его через интерфейс Gi0/1 на коммутатор SW1.

Циклические фреймы создают и третью проблему: к месту назначения прибывает несколько копий фрейма. Рассмотрим случай, когда компьютер Bob передает фрейм на компьютер Larry, но ни одни из коммутаторов не знает MAC-адрес компьютера Larry. Коммутаторы лавинно рассылают фреймы, посланные на неизвестный одноадресатный MAC-адрес. Когда компьютер Bob посылает фрейм на MAC-адрес компьютера Larry, коммутатор SW3 посылает его копию и коммутатору SW1, и коммутатору SW2. Коммутаторы SW1 и SW2 также лавинно рассылают фрейм, запуская копии фрейма по кругу. Коммутатор SW1 отсылает также копию каждого фрейма на интерфейс Fa0/11 компьютеру Larry. В результате компьютер Larry получает несколько копий фрейма, что может привести к отказу приложения, если оно неустойчиво к проблемам сети.

Три класса основных проблем, вызванных отсутствием протокола STP в избыточных сетях LAN, представлены в табл. 1.1.

Таблица 1.1. Три класса проблем, вызываемых отсутствием протокола STP в избыточных локальных сетях

Ключевая тема

Проблема	Описание
Широковещательный шторм	Перенаправление фрейма повторяется на тех же каналах связи, растрачивая существенную часть их пропускной способности
Неустойчивость таблицы MAC-адресов	Реагируя на циклические фреймы, коммутатор непрерывно заносит в таблицу MAC-адресов неправильные записи, приводящие к передаче фреймов в неправильном направлении
Передача нескольких фреймов	Побочный эффект циклической передачи фреймов, когда хосту доставляется несколько копий одного фрейма, нарушая его работу

Что делает связующее дерево IEEE 802.1D

Протокол STP предотвращает циклы, переводя каждый порт коммутатора либо в состояние перенаправления, либо в состояние блокировки. Интерфейсы в состоянии перенаправления действуют как обычно, перенаправляя и получая фреймы. Но интерфейсы в блокированном состоянии не обрабатывают никаких фреймов, кроме

сообщений протокола STP (и некоторых других служебных сообщений). Блокированные интерфейсы не перенаправляют пользовательские фреймы, не изучают MAC-адреса полученных фреймов и не обрабатывают полученные пользовательские фреймы.

На рис. 1.4 приведено простое дерево STP, решающее представленную на рис. 1.3 проблему за счет перевода одного порта коммутатора SW3 в состояние блокировки.

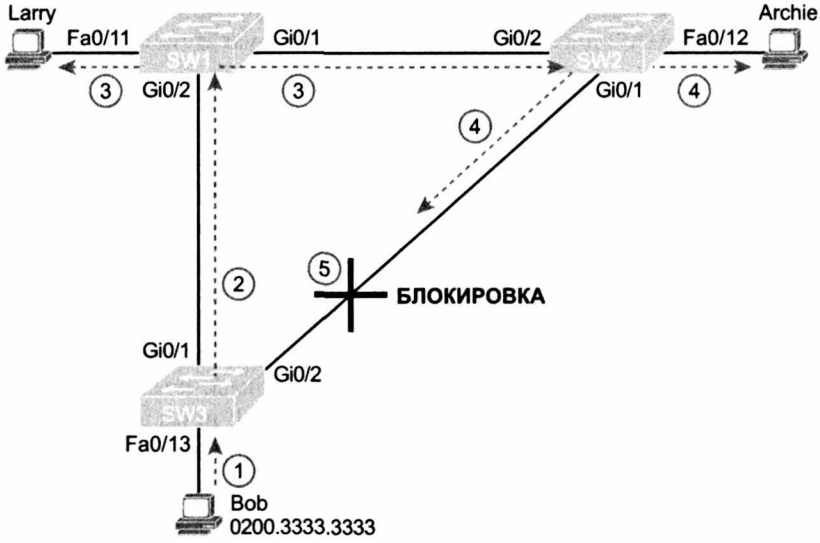


Рис. 1.4. Протокол STP блокирует порт, чтобы разорвать круг

Теперь, когда компьютер Bob посылает широковещательный фрейм, он не передается по кругу. На рисунке показаны следующие этапы.

Этап 1 Компьютер Bob посылает фрейм коммутатору SW3

Этап 2 Коммутатор SW3 перенаправляет фрейм только коммутатору SW1, но не через интерфейс Gi0/2 коммутатору SW2, поскольку этот интерфейс находится в состоянии блокировки

Этап 3 Коммутатор SW1 рассылает фрейм на интерфейсы Fa0/11 и Gi0/1

Этап 4 Коммутатор SW2 рассылает фрейм на интерфейсы Fa0/12 и Gi0/1

Этап 5 Физически коммутатор SW3 получает фрейм, но игнорирует его, поскольку его интерфейс Gi0/2 находится в блокированном состоянии

В представленной на рис. 1.4 сети коммутаторы просто не используют канал связи между коммутаторами SW2 и SW3 для трафика этой сети VLAN, что является незначительным отрицательным побочным эффектом протокола STP. Но при отказе любого из двух других каналов связи конвергенция протокола STP сработает так, что коммутатор SW3 переведет свой интерфейс Gi0/2 из состояния блокировки в состояние перенаправления.

ВНИМАНИЕ!

Термин *конвергенция STP* (STP convergence) описывает процесс, когда все коммутаторы понимают, что в топологии LAN что-то изменилось и, возможно, следует изменить состояние блокированных и перенаправляющих портов.

На этом завершается обсуждение того, что делает протокол STP, переводя каждый порт в состояние перенаправления или блокировки. Однако куда интереснее и труднее другие вопросы: как и почему протокол STP делает свой выбор? Как протокол STP блокирует интерфейс коммутатора? Как конвергенция изменяет состояние блокировки на перенаправление, чтобы использовать избыточные каналы при отказе сетевых соединений? На эти вопросы отвечают следующие разделы.

Как работает связующее дерево

Алгоритм STP создает связующее дерево интерфейсов, передающих фреймы. Древовидная структура перенаправляющих интерфейсов формирует только один путь к каждому каналу связи Ethernet и от него (точно так же, как и у живого дерева можно проследить только один путь от корня к каждому листу).

ВНИМАНИЕ!

Протокол STP был создан задолго до появления коммутаторов LAN. В те времена протокол STP использовал мосты Ethernet. Сегодня роль мостов играют коммутаторы, реализуя ту же концепцию STP. Однако многие термины протокола STP все еще относятся к мостам, поэтому в данной главе термины *мост* (bridge) и *коммутатор* (switch) можно считать синонимами.

Принимая решение о переводе интерфейса в состояние перенаправления, протокол STP руководствуется тремя критериями.

- Протокол STP выбирает корневой коммутатор. Все рабочие интерфейсы корневого коммутатора переводятся в состояние перенаправления.
- Каждый некорневой коммутатор считает, что у одного из его портов есть наименьшая административная стоимость между ним и корневым коммутатором. Это *корневая стоимость* (root cost) данного коммутатора. Протокол STP переводит в состояние перенаправления *корневой порт* коммутатора (Root Port — RP), т.е. порт, являющийся частью пути с наименьшей корневой стоимостью.
- К тому же сегменту Ethernet может быть подключено много коммутаторов, но в современных сетях с каждым каналом связи связано обычно лишь два коммутатора. Коммутатор с самой низкой корневой стоимостью, по сравнению с другими коммутаторами, подключенными к тому же каналу связи, переводится в состояние перенаправления. Это *выделенный коммутатор* (designated switch), а присоединенный к этому сегменту интерфейс коммутатора — *выделенный порт* (Designated Port — DP).

ВНИМАНИЕ!

Реальная причина, по которой корневые коммутаторы переводят все рабочие интерфейсы в состояние перенаправления, заключается в том, что все они являются выделенными портами, но проще просто запомнить, что все рабочие интерфейсы всех корневых коммутаторов перенаправят фреймы.

Все другие интерфейсы переводятся в состояние блокировки. В табл. 1.2 приведены причины, по которым протокол STP переводит порт в состояние перенаправления или блокировки.

Ключевая тема

Таблица 1.2. STP: причины для перевода порта в состояние перенаправления или блокировки

Характеристика порта	Состояние STP	Описание
Все порты корневого коммутатора	Перенаправление	Корневой коммутатор всегда является выделенным для всех подключенных сегментов
Корневой порт каждого некорневого коммутатора	Перенаправление	Порт с наименьшей стоимостью для доступа к корневому коммутатору
Выделенный порт каждой сети LAN	Перенаправление	Коммутатор, перенаправляющий сообщения Hello в сегмент, с самой низкой корневой стоимостью, является выделенным коммутатором для этого сегмента
Все другие рабочие порты	Блокировка	Порт не используется ни для перенаправления пользовательских фреймов, ни для получения любых фреймов, предназначенных для перенаправления

ВНИМАНИЕ!

Протокол STP учитывает только рабочие интерфейсы (т.е. находящиеся в подключенном состоянии). Интерфейсы отключенные физически (например, без кабеля) или отключенные административно протокол STP переводит в блокированное состояние. Таким образом, в этом разделе используется термин *рабочий порт* (working port) для интерфейсов, способных перенаправлять фреймы, если бы протокол STP перевел интерфейс в состояние перенаправления.

Идентификатор моста STP и пакет BPDU Hello

Сначала протокол STP выбирает один коммутатор как корневой. Чтобы лучше понять процесс выбора, следует уяснить, какие сообщения STP передаются между коммутаторами, а также концепции и формат идентификатора, позволяющего однозначно определить каждый коммутатор.

Идентификатор моста STP (Bridge ID — BID) представляет собой 8-байтовое значение, уникальное для каждого коммутатора. Идентификатор моста состоит из 2-байтового поля *приоритета* (priority) и 6-байтового *системного идентификатора* (system ID), в основе которого лежит универсальный (прошитый) MAC-адрес каждого коммутатора. Использование прошитого MAC-адреса гарантирует, что идентификатор моста каждого коммутатора будет уникален.

Протокол STP определяет сообщения *модуля данных протокола моста* (Bridge Protocol Data Unit — BPDU), используемые коммутаторами для обмена информацией друг с другом. Наиболее распространенным сообщением BPDU является пакет Hello, содержащий много подробностей, включая идентификатор BID коммутатора. Передавая свои уникальные идентификаторы BID, коммутаторы способны

распознавать, кто какой пакет Hello передал. Часть ключевой информации пакета Hello приведена в табл. 1.3.

Таблица 1.3. Поля пакета Hello протокола STP



Поле	Описание
Идентификатор корневого моста	Отправивший это сообщение Hello коммутатор в настоящее время считает себя корневым
Идентификатор моста отправителя	Идентификатор моста коммутатора, отправившего это сообщение Hello
Корневая стоимость отправителя	Стоимость STP пути между этим коммутатором и текущим корневым
Значение таймера на корневом коммутаторе	Значения таймеров Hello, MaxAge и таймера задержки перенаправления

Сейчас основное внимание обратите лишь на первые три элемента табл. 1.3, поскольку в следующих разделах рассматривают три этапа выбора протоколом STP интерфейсов, переводимых в состояние перенаправления. Итак, рассмотрим три основных этапа процесса STP.

Выбор корневого коммутатора

Коммутаторы выбирают корневой коммутатор на основании идентификаторов BID в сообщениях BPDU. Корневой коммутатор — это коммутатор с самым низким числовым значением идентификатора BID. Поскольку идентификатор BID состоит из двух частей, начиная со значения приоритета, корневым, по существу, становится коммутатор с самым низким приоритетом. Например, если у одного коммутатора приоритет 4096, а у других — 8192, то победит коммутатор с приоритетом 4096, независимо от MAC-адреса, использованного для создания идентификатора BID каждого коммутатора.

Поскольку выбор происходит на основании части приоритета идентификатора BID, при равных приоритетах корневым станет коммутатор с самой низкой частью MAC-адреса. Никакой другой схемы разрешения конфликтов не нужно, поскольку во второй части своих идентификаторов BID коммутаторы используют собственные универсальные (прошитые) MAC-адреса. Если при равенстве приоритетов один коммутатор использует как часть BID MAC-адрес 0200.0000.0000, а другой 0911.1111.1111, то корневым станет первый коммутатор (MAC-адрес 0200.0000.0000).

Выборы корневого коммутатора протоколом STP проходят совсем не так, как политические выборы. Процесс начинается с передачи сообщений BPDU Hello всеми коммутаторами, которые собираются стать корневыми. Собственный идентификатор BID коммутатора в этих сообщениях заявлен как корневой BID. Если коммутатор получает сообщение Hello с лучшим (более низким) идентификатором BID, он прекращает анонсировать себя как корневой и начинает перенаправлять сообщение Hello лучшее, чем у него. Сообщение Hello, посланное лучшим коммутатором, содержит идентификатор BID лучшего коммутатора в качестве корневого. Это как в предвыборной кампании, когда менее популярный кандидат сдается и, прекращая собственную кампанию, оказывает поддержку более популярному кандидату. В конечном счете все соглашаются, что у некого коммутатора наилучший

(самый низкий) идентификатор BID, и поддерживают избранный коммутатор, а аналогия с политической предвыборной кампанией на этом заканчивается.

ВНИМАНИЕ!

Смысл лучшего сообщения Hello в том, что указанный в нем идентификатор BID корневого коммутатора лучше (в цифровой форме ниже). Это *наилучшее сообщение Hello* (superior Hello). У худшего сообщения Hello идентификатор BID корневого коммутатора не так хорош (в цифровой форме больше). Это *не наилучшее сообщение Hello* (inferior Hello).

На рис. 1.5 представлено начало процесса выборов корневого коммутатора. В данном случае коммутатор SW1 анонсировал себя корневым, как и коммутаторы SW2 и SW3. Но коммутатор SW2 теперь полагает, что коммутатор SW1 лучший корневой коммутатор, поэтому он теперь перенаправляет сообщения Hello, посланные коммутатором SW1. Таким образом, на настоящий момент на рисунке показан коммутатор SW1, передающий сообщения Hello, с заявкой на роль корневого; коммутатор SW2 соглашается с этим и перенаправляет сообщение коммутатора SW1 с заявкой на роль корневого; но коммутатор SW3 все еще утверждает, что был бы лучшим, посылая собственное сообщение BPDU Hello, содержащее идентификатор BID коммутатора SW3 как корневого.

На рис. 1.5 все еще есть два кандидата: коммутаторы SW1 и SW3. Так кто же победит? Конечно, коммутатор, идентификатор BID которого содержит самый низкий приоритет; если приоритеты равны, победит обладающий меньшим значением MAC-адреса. Как показано на рисунке, у коммутатора SW1 идентификатор BID (32769:0200.0001.0001) ниже, чем у коммутатора SW3 (32769:0200.0003.0003), поэтому побеждает коммутатор SW1, а коммутатор SW3 теперь также полагает, что он лучший коммутатор. На рис. 1.6 представлены результирующие сообщения Hello, посланные коммутаторами.

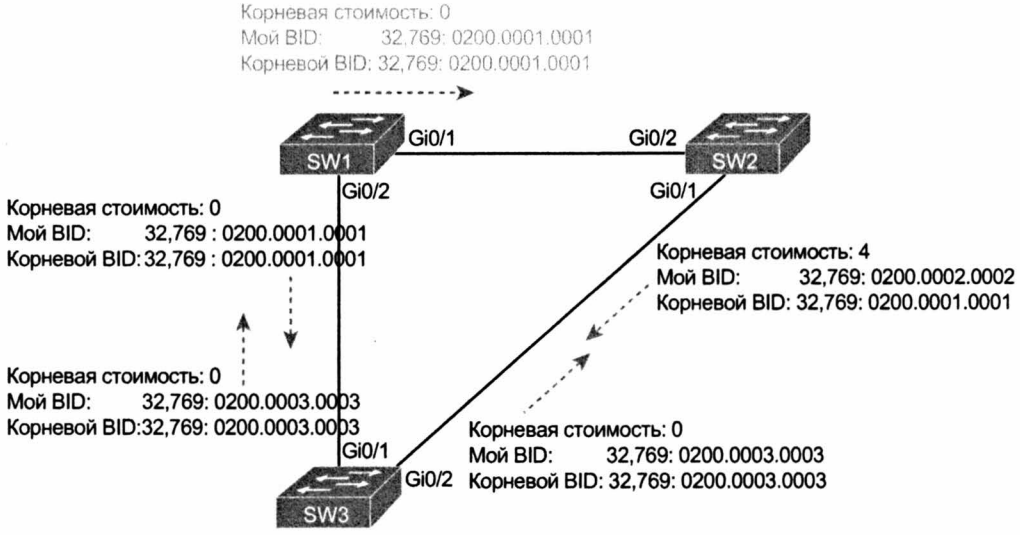


Рис. 1.5. Начало процесса выборов корневого коммутатора

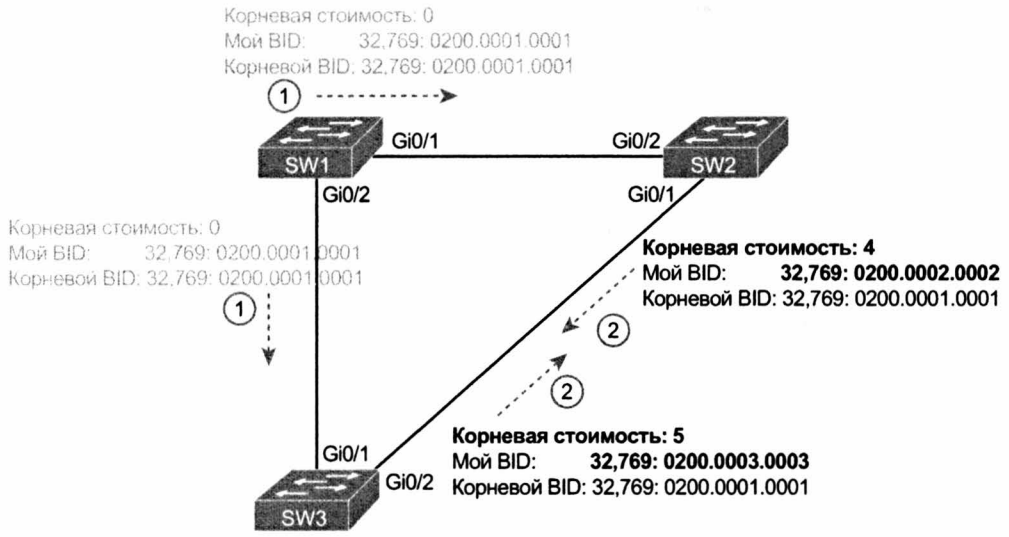


Рис. 1.6. Коммутатор SW1 побеждает на выборах

По завершении выборов только корневой коммутатор продолжает передавать сообщения Hello. Другие коммутаторы получают сообщения Hello, изменяют поле BID отправителя (и поле корневой стоимости), а затем перенаправляют их на другие интерфейсы. Рисунок отражает тот факт, что на этапе 1 коммутатор SW1 посылает сообщения Hello, а коммутаторы SW2 и SW3 независимо перенаправляют их на другие интерфейсы (этап 2).

Таким образом, выборы корневого коммутатора происходят на каждом коммутаторе, претендующем на роль корневого, а наилучшим считается коммутатор с самым низким (в цифровой форме) идентификатором BID. При разделении идентификатора BID на компоненты сравнение осуществляется так.

Логика выбора корневого коммутатора

Ключевая тема

- Самый низкий идентификатор моста.
- При равенстве самый низкий MAC-адрес коммутатора.

Выбор корневого порта каждого коммутатора

Вторая часть процесса STP — это выбор каждым некорневым коммутатором одного и только одного *корневого порта* (Root Port — RP). Корневой порт коммутатора — это интерфейс с наименьшей стоимостью STP для доступа к корневому коммутатору.

Идея стоимости доступа к корневому коммутатору легко понятна: посмотрите на схему сети, где представлен корневой коммутатор и связанная с каждым портом коммутатора стоимость STP, а также некий рассматриваемый коммутатор. Конечно, коммутаторы используют совсем не такой процесс, как на рисунке, но он облегчает описание идеи.

На рис. 1.7 представлена именно такая схема с теми же тремя коммутаторами, что и на нескольких предыдущих рисунках. Коммутатор SW1 уже выиграл выборы как корневой, и на рисунке рассматривается стоимость с точки зрения коммутатора SW3.

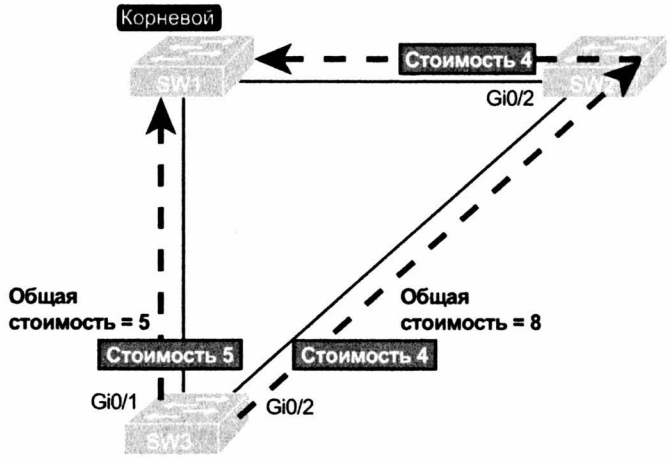


Рис. 1.7. Как человек мог бы вычислить стоимость STP от коммутатора SW3 до корневого коммутатора (SW1)

У коммутатора SW3 есть два возможных физических пути для передачи фреймов на корневой коммутатор: прямой путь (слева) и обходной (справа, через коммутатор SW2). *Стоимость* (cost) — это сумма стоимостей всех *портов, покидаемых фреймом*, если бы он следовал по этому пути. (Входящие порты вычисление игнорирует.) Как можно заметить, общая стоимость прямого пути через порт G0/1 коммутатора SW3 составляет 5, а общая стоимость другого пути — 8. Коммутатор SW3 выбирает свой порт G0/1 как корневой, поскольку он является частью пути с наименьшей стоимостью для передачи фреймов на корневой коммутатор.

Коммутаторы приходят к тому же выводу, но в ходе другого процесса. Вместо этого они добавляют стоимость STP своего локального интерфейса к корневой стоимости, указанной в каждом полученном пакете BPDU Hello. Стоимость STP маршрута через порт — это целочисленное значение, присвоенное каждому интерфейсу каждой сети VLAN для обеспечения объективного измерения, позволяющее протоколу STP выбрать, какие интерфейсы добавить в топологию STP. Коммутаторы учитывают также корневую стоимость своего соседа, анонсируемую в каждом полученном от каждого соседа пакете BPDU Hello.

На рис. 1.8 приведен пример вычисления коммутаторами своей лучшей корневой стоимости и последующего выбора корневого порта, с использованием той же топологии и стоимостей STP, что и на рис. 1.7. Протокол STP на коммутаторе SW3 вычисляет свою стоимость доступа к корневому коммутатору по двум возможным путям с добавлением анонсируемой (в сообщениях Hello) стоимости к стоимости интерфейса, приведенного на рисунке.

Сначала рассмотрим сам процесс. Корневой коммутатор посылает сообщения Hello с указанной корневой стоимостью 0. Идея в том, что стоимость корневого коммутатора для доступа к себе самому составляет 0.

Теперь рассмотрим левую часть рисунка. Коммутатор SW3 берет стоимость (0), полученную в сообщении Hello, посланном коммутатором SW1, добавляет стоимость (5) интерфейса, на котором было получено сообщение Hello. Коммутатор SW3 вычисляет стоимость доступа к корневому коммутатору через этот порт (G0/1) и получает 5.

В правой части рисунка коммутатор SW2 вычислил, что его лучшая стоимость доступа корневого коммутатора составляет 4. Таким образом, когда коммутатор SW2 перенаправляют пакет Hello коммутатору SW3, он указывает корневую стоимость 4. Стоимость маршрута коммутатора SW3 через порт G0/2 составляет 4, поэтому коммутатор SW3 определяет общую стоимость доступа к корневому коммутатору через порт G0/2 как 8.

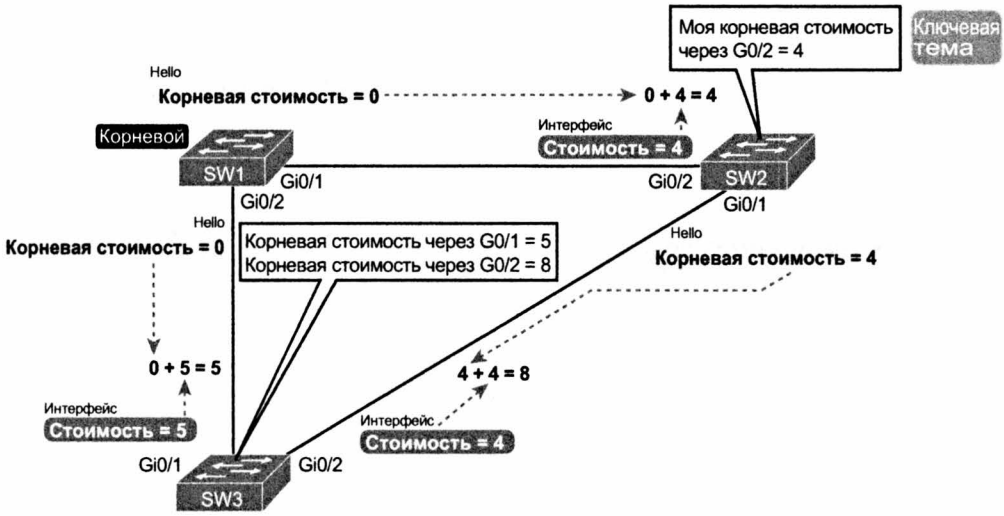


Рис. 1.8. Так протокол STP фактически вычисляет стоимость от коммутатора SW3 до корневого коммутатора (SW1)

В результате изображенного на рис. 1.8 процесса коммутатор SW3 выбирает свой порт Gi0/1 как корневой (Root Port — RP), поскольку стоимость доступа к корневому коммутатору через него составляет 5, что ниже, чем у альтернативы (стоимость через порт Gi0/2 = 8). Точно так же коммутатор SW2 выбирает свой порт Gi0/2 как порт RP со стоимостью 4 (коммутатор SW1 анонсировал стоимость 0 плюс стоимость 4 интерфейса Gi0/2 коммутатора SW2). Каждый коммутатор переводит свой корневой порт в состояние перенаправления.

В более сложной топологии выбор корневого порта не будет столь очевиден. Более подробная информация по этой теме и более сложные примеры, включая схемы разрешения конфликтов при совпадении корневых стоимостей, приведены в главе 2.

Выбор выделенного порта на каждом сегменте LAN

Заключительный этап процесса STP по выбору топологии подразумевает выбор выделенного порта на каждом сегменте сети LAN. *Выделенный порт* (Designated Port — DP) сегмента LAN — это порт коммутатора, анонсирующий в сегмент LAN сообщения Hello с самой низкой стоимостью. Когда некорневой коммутатор перенаправляет сообщения Hello, он записывает в поле корневой стоимости сообщения стоимость доступа к корневому коммутатору. В результате коммутатор с самой низкой стоимостью доступа к корневому коммутатору из всех коммутаторов сегмента становится портом DP на этом сегменте.

Например, на рис. 1.6 полужирным шрифтом выделены части сообщений Hello от коммутаторов SW2 и SW3, определяющих выбор порта DP на данном сегменте. Обратите внимание, что оба коммутатора, SW2 и SW3, имеют свою стоимость доступа к корневому коммутатору (4 у SW2 и 5 у SW3 соответственно). У коммутатора SW2 стоимость ниже, поэтому его порт Gi0/1 становится выделенным портом на этом сегменте LAN.

Все порты DP переводятся в состояние перенаправления; таким образом, интерфейс Gi0/1 коммутатора SW2 в данном случае будет в состоянии перенаправления.

Если анонсируемые стоимости совпадают, выбирается коммутатор с более низким идентификатором BID. В данном случае снова победил бы коммутатор SW2, его идентификатор BID 32769:0200.0002.0002 против 32769:0200.0003.0003 у коммутатора SW3.

ВНИМАНИЕ!

В некоторых случаях необходимы две дополнительные схемы разрешения конфликтов, хотя сегодня они маловероятны. Один коммутатор может быть подключен через концентратор двумя или более интерфейсами к тому же домену коллизий. В этом случае коммутатор получает собственное сообщение BPDU. Поскольку в этом случае коммутатор сыграет вничью сам с собой, используются две дополнительные схемы разрешения конфликтов: по самому низкому приоритету STP интерфейса, а если они совпадают — то по самому низкому номеру внутреннего интерфейса.

Единственный интерфейс, которому нет причин оставаться в состоянии перенаправления на трех коммутаторах в примерах на рис. 1.5–1.8, — это порт Gi0/2 коммутатора SW3. Итак, процесс STP завершен. В табл. 1.4 приведены состояния каждого порта и причины его нахождения в этом состоянии.

Таблица 1.4. Состояние каждого интерфейса

Интерфейс коммутатора	Состояние	Причина нахождения в состоянии перенаправления
SW1, Gi0/1	Перенаправление	Интерфейс находится на корневом коммутаторе, поэтому он становится портом DP на этом канале связи
SW1, Gi0/2	Перенаправление	Интерфейс находится на корневом коммутаторе, поэтому он становится портом DP на этом канале связи
SW2, Gi0/2	Перенаправление	Корневой порт коммутатора SW2
SW2, Gi0/1	Перенаправление	Выделенный порт сегмента LAN на коммутаторе SW3
SW3, Gi0/1	Перенаправление	Корневой порт коммутатора SW3
SW3, Gi0/2	Блокировка	Не корневой и не выделенный порт

Влияние и изменение топологии STP

Коммутаторы не используют протокол STP только один раз и больше никогда. Коммутаторы отслеживают изменения непрерывно. Причиной этих изменений может стать отказ канала связи или коммутатора, либо может появиться новый канал связи, доступный для использования. Топологию STP может изменить смена кон-

фигурации. В данном разделе коротко рассматриваются факторы, способные изменить топологию STP либо при смене конфигурации, либо при изменении состояния каналов связи или устройств LAN.

Внесение изменений в конфигурацию влияет на топологию STP

Сетевые инженеры вполне могут изменить параметры STP, что повлияет на результаты выборов в данной сети LAN. Для изменения идентификатора моста и стоимости маршрута через порт STP инженеру доступны два основных инструмента.

Коммутатор способен создать стандартный идентификатор BID из стандартного значения приоритета и уникального MAC-адреса, прошитого на коммутаторе при изготовлении. Но инженеры обычно сами выбирают, какой коммутатор станет корневым. В главе 2 описана настройка коммутатора Cisco и переопределение его стандартного идентификатора BID так, чтобы он стал корневым.

Стоимости маршрута через порт также имеют стандартные значения по каждому порту и сети VLAN. Эти стоимости маршрута через порт также можно настроить или можно использовать стандартные значения. В табл. 1.5 приведены стоимости маршрута через порт согласно стандарту IEEE; компания Cisco использует эти же значения.

Таблица 1.5. Стандартные стоимости маршрута через порт согласно IEEE

Ключевая тема

Скорость Ethernet	Стоимость IEEE
10 Мбит/с	100
100 Мбит/	19
1 Гбит/с	4
10 Гбит/с	2

При включенном протоколе STP все рабочие интерфейсы коммутатора находятся либо в состоянии STP перенаправления, либо блокировки, даже порты доступа. Если интерфейсы коммутатора подключены к хостам или маршрутизаторам, не использующим протокол STP, коммутатор продолжает перенаправлять пакеты Hello на эти интерфейсы. Чтобы стать единственным устройством, посылающим пакеты Hello в этом сегменте LAN, коммутатор посылает пакеты Hello с наименьшей стоимостью на этот сегмент LAN, позволяя коммутатору стать выделенным портом на этом сегменте сети LAN. Таким образом, протокол STP переводит рабочие интерфейсы доступа в состояние перенаправления в ходе части процесса STP, относящейся к выделенному порту.

Реакция на изменение состояния влияет на топологию STP

Как только инженер закончит настройку протокола STP, топология STP должна перейти в стабильное состояние и не изменяться, по крайней мере, до изменения топологии сети. В данном разделе рассматривается работа протокола STP в то время, когда сеть стабильна, а затем при переходе на новую топологию, когда что-то изменяется.

Стандартно корневой коммутатор посылает новые сообщения BPDU Hello каждые 2 секунды. Каждый некорневой коммутатор перенаправляет сообщения Hello

на все выделенные порты (DP), но только после изменяющихся элементов, выведенных в сообщениях Hello. Коммутатор вносит корневую стоимость в вычисляемую корневую стоимость локального коммутатора. Коммутатор устанавливает также в поле идентификатора моста отправителя собственный идентификатор моста. (Поле идентификатора моста корневого коммутатора не изменяется.)

При перенаправлении полученного (и измененного) пакета Hello все выделенные порты (DP) всех коммутаторов продолжают получать сообщения Hello каждые 2 секунды. Ниже приведена последовательность действий при стабильной работе, когда в топологии STP ничего не изменяется.



Работа протокола STP в стабильных условиях

Этап 1 Корневой коммутатор создает и посылает сообщения BPDU Hello с корневой стоимостью 0 через все свои рабочие интерфейсы (находящиеся в состоянии перенаправления)

Этап 2 Некорневые коммутаторы получают сообщения Hello на своих корневых портах. После замены в сообщении Hello идентификатора BID отправителя на собственный и указания собственной корневой стоимости коммутатор перенаправляет сообщение Hello на все выделенные порты

Этап 3 Этапы 1 и 2 повторяются, пока что-то не изменится

Для контроля работоспособности пути к корневому коммутатору каждый коммутатор полагается на периодическое получение сообщений Hello от корневого коммутатора. Когда коммутатор прекращает получать сообщения Hello или получает сообщение Hello с другими подробностями, он понимает, что что-то отказало, и реагирует, запуская процесс изменения топологии распределенного связующего дерева.

Как коммутаторы реагируют на изменения топологи STP

По некоторым причинам процесс конвергенции требует использования трех таймеров. Все коммутаторы используют таймеры, как диктует корневой коммутатор, периодически передающий сообщения BPDU Hello. Таймеры описаны в табл. 1.6.

Таблица 1.6. Таймеры STP

Таймер	Описание	Стандартное значение
Hello	Период времени между передачей сообщений Hello корневым коммутатором	2 секунды
MaxAge	Как долго коммутатор должен ожидать после прекращения поступления сообщений Hello, прежде чем пытаться изменять топологию STP	10 периодов Hello
Задержка перенаправления	Задержка, влияющая на процесс, происходящий при изменении интерфейсом состояния с блокировки на перенаправление. На протяжении секунд, заданных таймером, задержки перенаправления порт остается в промежуточном состоянии прослушивания, а затем переходит в промежуточное состояние самообучения	15 секунд

Если коммутатор не получает ожидаемых сообщений BPDU Hello за период Hello, то продолжает работать как обычно. Но если сообщения Hello не поступают на протяжении периода MaxAge, то коммутатор реагирует действиями, изменяющими топологию STP. При стандартных настройках таймер MaxAge составляет 20 секунд (10 стандартных таймеров Hello по 2 секунды). Таким образом, коммутатор не будет реагировать 20 секунд, не получая сообщений Hello.

По истечении периода MaxAge коммутатор начинает, по существу, новые выборы STP на основании любых пакетов Hello, поступающих от других коммутаторов. В результате корневой коммутатор выбирается заново. Если локальный коммутатор не становится корневым, он выбирает свой корневой порт (RP). И это определяет, будут ли это выделенные порты (DP) на каждом из его других каналов связи. Лучше всего описать конвергенцию STP на примере, используя уже знакомую топологию. На рис. 1.9 представлена та же схема с интерфейсом Gi0/2 коммутатора SW3 в состоянии блокировки, но интерфейс Gi0/2 коммутатора SW1 только что отказал.

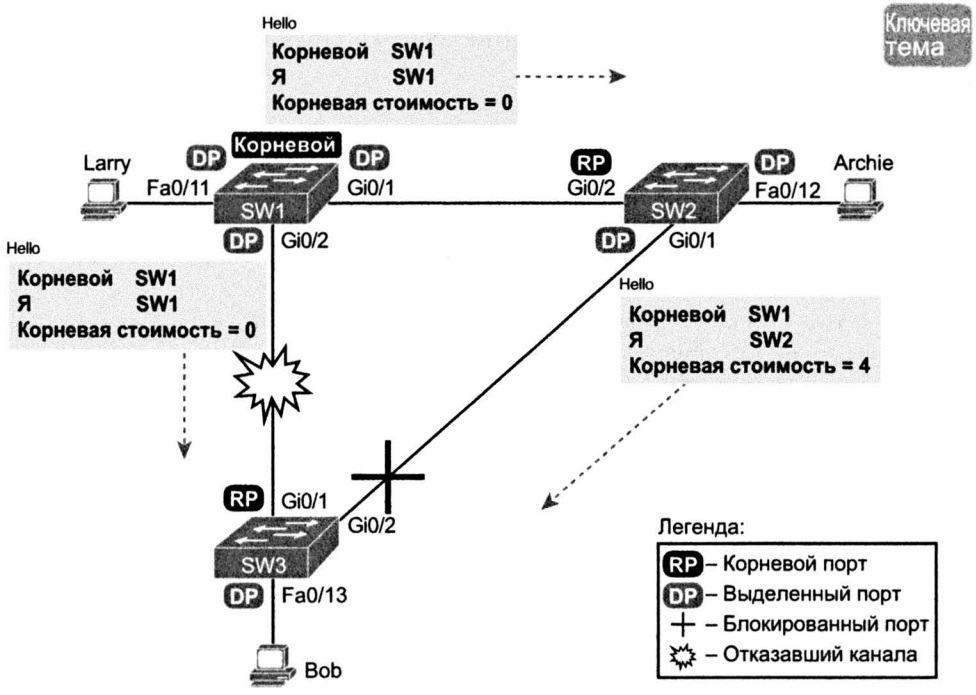


Рис. 1.9. Начальное состояние топологии STP перед отказом канала связи SW1–SW3

Коммутатор SW3 реагирует на изменения, поскольку не получает ожидаемые сообщения Hello на своем интерфейсе Gi0/1. Но коммутатор SW2 не должен реагировать, поскольку он продолжает регулярно получать сообщения Hello на своем интерфейсе Gi0/2. В данном случае коммутатор SW3 реагирует либо по истечении периода MaxAge без сообщений Hello, либо как только заметит, что его интерфейс Gi0/1 отказал. (Если интерфейс отказал, коммутатор может заметить, что сообщения Hello больше не поступают на этот интерфейс.)

Теперь, когда коммутатор SW3 может действовать, он начинает повторный процесс выбора корневого коммутатора. Коммутатор SW3 все еще получает сообщения Hello от коммутатора SW2, пересылаемые с корневого коммутатора (SW1). Идентификатор BID коммутатора SW1 все еще ниже, чем у коммутатора SW3; в противном случае коммутатор SW1 уже не был бы корневым. Таким образом, коммутатор SW3 решает, что коммутатор SW1 все еще лучший, а он сам не корневой.

Затем коммутатор SW3 переоценивает свой выбор корневого порта (RP). На настоящий момент коммутатор SW3 получает сообщения Hello только на одном интерфейсе: Gi0/2. Безотносительно вычисляемой корневой стоимости, интерфейс Gi0/2 становится новым корневым портом коммутатора SW3. (Он имел бы стоимость 8, подразумевая, что стоимости STP не изменились с момента, изображенного на рис. 1.7 и 1.8.)

Затем коммутатор SW3 переоценивает свою роль выделенного порта (DP) на любых других интерфейсах. В этом примере никаких изменений быть не должно. Коммутатор SW3 уже был выделенным портом на интерфейсе Fa0/13 и остается им, поскольку никакие другие коммутаторы не соединены с этим портом.

Изменение состояния интерфейса

Протокол STP использует концепции ролей и состояний. Роли корневого и выделенного портов относятся к тому, как протокол STP анализирует топологию сети LAN. Состояния перенаправления и блокировки указывают коммутатору, нужно ли передавать и получать фреймы. При конвергенции STP коммутатор выбирает новые роли для порта, а роли порта определяют состояние (перенаправления или блокировки).

Коммутаторы способны практически мгновенно перейти из состояния блокировки в состояние перенаправления, но для смены состояния им нужно дополнительное время. Например, если прежде коммутатор использовал свой порт G0/1 как корневой (роль RP), он находился в состоянии перенаправления. После конвергенции порт G0/1 может и не остаться ни корневым, ни выделенным; коммутатор может немедленно перевести его в состояние блокировки.

При переводе порта из состояния блокировки в состояние перенаправления коммутатор сначала помещает порт в два промежуточных состояния. Эти временные состояния позволяют предотвратить временные циклы.

Ключевая тема

Определения происходящего в состояниях прослушивания и самообучения

- *Прослушивание* (listening). Как и в состоянии блокировки, интерфейс не перенаправляет фреймы. Коммутатор удаляет устаревшие (неиспользуемые) записи таблицы MAC-адресов, для которых (или от которых) за данный период не было получено фреймов. Устаревшие записи таблицы MAC-адресов могут стать причиной временных циклов.
- *Самообучение* (learning). Интерфейсы в этом состоянии все еще не перенаправляют фреймы, но коммутатор начинает изучать MAC-адреса фреймов, полученных на интерфейсе.

Протокол STP переводит интерфейс из состояния блокировки в состояние прослушивания, затем в состояние самообучения, потом в состояние перенаправления. Протокол STP оставляет интерфейс в каждом из промежуточных состояний на время, равное периоду задержки перенаправления (стандартно 15 секунд). В результате событие конвергенции, переводящее интерфейс из состояния блокировки в состояние перенаправления, требует 30 секунд. Кроме того, коммутатору, возможно, придется выждать период MaxAge, прежде чем перейти к выборам.

Например, рассмотрим происходящее с начальной топологией STP, показанной на рис. 1.5–1.8, при отказавшем канале связи SW1–SW3 (см. рис. 1.9). Если коммутатор SW1 просто перестанет посылать сообщения Hello на коммутатор SW3, но канал связи между ними будет исправен, то прежде чем реагировать, коммутатор SW3 выждет период MaxAge (стандартно 20 секунд). Фактически коммутатор SW3 довольно быстро выбрал бы роли STP своих портов, но затем он ожидал бы по 15 секунд в состояниях прослушивания и самообучения на интерфейсе Gi0/2, что привело бы к суммарной задержке конвергенции в 50 секунд.

Таблица 1.7. Состояния распределенного связующего дерева по стандарту IEEE 802.1D

Ключевая тема

Состояние	Перенаправляет ли фреймы?	Изучает MAC-адреса на основании полученных фреймов?	Стабильное или промежуточное?
Блокирования	Нет	Нет	Стабильное
Прослушивания	Нет	Нет	Промежуточное
Прослушивания	Нет	Да	Промежуточное
Перенаправления	Да	Да	Стабильное
Отключения	Нет	Нет	Стабильное

Дополнительные средства протокола STP

Протокол STP существует более тридцати лет, хотя использовался даже раньше, чем *Институт инженеров по электротехнике и электронике* (Institute of Electrical and Electronic Engineers — IEEE) приступил к разработке стандартов Ethernet для Xerox и других производителей. Впервые IEEE стандартизировал протокол STP как стандарт IEEE 802.1D в 1980-х годах. Ныне коммутаторы Cisco все еще используют протокол STP. Кроме изменений стандартных значений стоимости, описание протокола STP в этой главе до сих пор относилось к оригинальному протоколу STP, созданному многие годы назад.

Даже при такой удивительно долгой продолжительности существования (несколько десятилетий) протокол STP претерпел несколько изменений, больших и маленьких. Например, компания Cisco добавила в протокол STP несколько собственных усовершенствований. В некоторых случаях IEEE добавил эти усовершенствования в последующий стандарт, например 802.1D, или оформил как дополнительный стандарт. У протокола STP есть новая версия с улучшенной конвергенцией — *ускоренный протокол распределенного связующего дерева* (Rapid Spanning Tree Protocol — RSTP), первоначально определенный в стандарте IEEE 802.1w.

В заключительном разделе данной главы кратко рассматриваются основы некоторых из необязательных средств, не входящих в базовые концепции протокола STP стандарта 802.1D, включая канал EtherChannel, режим PortFast и службу BPDU Guard.

Канал EtherChannel

Один из наилучших способов снижения времени конвергенции STP заключается в том, чтобы вообще избежать конвергенции. Канал EtherChannel позволяет избежать необходимости в конвергенции STP при отказе только одного порта или кабеля.

Канал EtherChannel объединяет несколько (до восьми) параллельных сегментов с равной скоростью между той же парой коммутаторов, связанных каналом EtherChannel. Коммутаторы рассматривают канал EtherChannel как единый интерфейс с точки зрения протокола STP. В результате при отказе одного из каналов связи, по крайней мере при наличии одного рабочего канала связи, конвергенция STP необязательна. На рис. 1.10 приведен пример знакомой сети с тремя коммутаторами, но теперь с двумя гигабитовыми соединениями Ethernet между каждой парой коммутаторов.

На каналах связи EtherChannel, состоящих из двух каналов связи Ethernet, протокол STP рассматривает каждый канал EtherChannel как единый канал связи. Другими словами, чтобы вызывать конвергенцию STP, отказать должны оба канала связи с тем же коммутатором. Без канала EtherChannel, если между двумя коммутаторами есть несколько параллельных каналов связи, протокол STP блокирует все каналы связи, кроме одного. При наличии канала EtherChannel все параллельные каналы связи могут работать одновременно, время конвергенции STP сокращается, что, в свою очередь, повышает доступность сети.

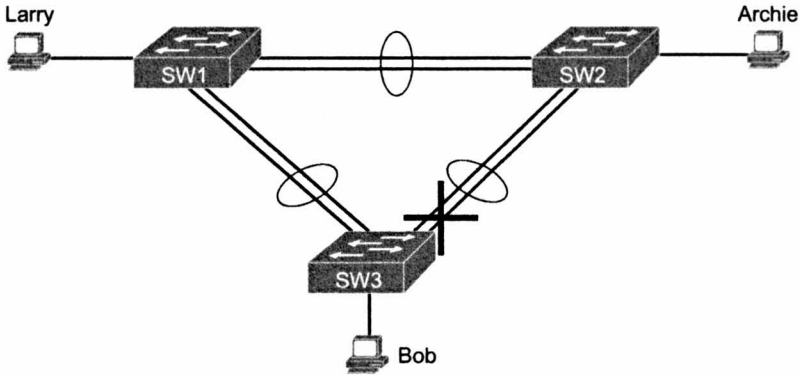


Рис. 1.10. Каналы EtherChannel с двумя сегментами между коммутаторами

Когда коммутатор принимает решение о перенаправлении фрейма по каналу EtherChannel, он должен предпринять дополнительный логический этап: на какой именно физический интерфейс передать фрейм? У коммутатора есть логика балансировки нагрузки, позволяющая ему выбрать интерфейс для каждого фрейма так, чтобы распределить нагрузку по всем активным каналам связи в канале EtherChannel. В результате сеть LAN, использующая каналы EtherChannel, много лучше использует доступную ширину полосы пропускания между коммутаторами, при сокращении времени конвергенции STP.

Режим PortFast

Режим PortFast позволяет коммутатору немедленно переходить из состояния блокировки в состояние перенаправления, в обход состояний прослушивания и самообучения. Однако единственные порты, на которых можно безопасно включить режим PortFast, — это порты, к которым гарантированно не подключены никакие мосты, коммутаторы или другие устройства STP. В противном случае режим PortFast способен создавать петли, во избежание которых предназначены состояния прослушивания и самообучения.

Режим PortFast лучше всего подходит для соединений с устройствами конечного пользователя. Если включить режим PortFast на портах, соединенных с устройствами конечного пользователя, при включении компьютера конечного пользователя порт коммутатора может перейти в состояние перенаправления STP и начать перенаправлять трафик, как только сетевая плата компьютера станет активной. Без режима PortFast каждый порт вынужден ждать, пока коммутатор подтвердит роль выделенного порта (DP), а затем подождет, пока интерфейс находится в промежуточных состояниях прослушивания и самообучения, прежде чем перейти в состояние перенаправления.

Служба BPDU Guard

Протокол STP открывает в сети LAN несколько брешей для нарушения ее безопасности. Например:

- Злоумышленник может подключиться к коммутатору через один из портов с низким значением приоритета STP и сделать его корневым коммутатором. У новой топологии STP может оказаться худшая производительность, чем у желательной топологии.
- Злоумышленник может включить несколько портов на нескольких коммутаторах, чтобы сделать свой коммутатор корневым, и фактически перенаправлять через него большую часть трафика сети LAN. Если сотрудники не воспрепятствуют, злоумышленник может использовать анализатор LAN для копирования фреймов данных, передаваемых по локальной сети.
- Пользователи по неосторожности могут повредить LAN, купив и подключив недорогой потребительский коммутатор LAN (неспособный использовать протокол STP). Такой коммутатор без функций STP не станет блокировать порты и, вероятно, создаст петли.

Служба Cisco BPDU Guard позволяет предотвратить эти проблемы, отключая порт, если на него поступает какое-нибудь сообщение BPDU. Это средство особенно полезно на тех портах, которые должны использоваться только как порты доступа и никогда не соединяться с другим коммутатором.

Кроме того, служба BPDU Guard позволяет предотвратить проблемы с режимом PortFast. Режим PortFast должен быть разрешен только на тех портах доступа, которые соединены с пользовательскими устройствами, но не с другими коммутаторами LAN. Использование службы BPDU Guard на тех же портах имеет смысл, поскольку при подключении к такому порту другого коммутатора локальный коммутатор может отключить порт прежде, чем образуется петля.

Протокол Rapid STP (IEEE 802.1w)

Как уже упоминалось в этой главе, IEEE определяет протокол STP в стандарте IEEE 802.1D. Улучшенная версия протокола, ускоренный протокол распределенного связующего дерева (RSTP), определена в стандарте IEEE 802.1w.

Протокол RSTP (802.1w) работает точно так же, как протокол STP (802.1D) в следующем.

- Выбирает корневой коммутатор, используя те же параметры и схемы разрешения конфликтов.
- Выбирает корневой порт на некорневых коммутаторах по тем же правилам.
- Выбирает выделенные порты на каждом сегменте LAN по тем же правилам.
- Переводит все порты в состояние перенаправления или блокировки, хотя в протоколе RSTP состояние блокировки называется *состоянием игнорирования* (discarding state).

Протокол RSTP может быть развернут параллельно с традиционным протоколом STP (802.1D), включая средства RSTP, работающие на коммутаторах, поддерживающих его, и традиционные средства протокола STP (802.1D), работающие на коммутаторах с поддержкой только протокола STP.

При всех этих сходствах может возникнуть вопрос: почему IEEE потрудился создать протокол RSTP? Причина в конвергенции. Конвергенция протокола STP занимает относительно много времени (50 секунд, со стандартными настройками). Протокол RSTP улучшает конвергенцию сети при изменении топологии; обычно она занимает несколько секунд, а в самых плохих случаях порядка 10 секунд.

В реальной жизни большинство корпоративных локальных сетей использует проекты сетей, требующих применения протокола STP, а большинство из них предпочитает использовать протокол RSTP из-за лучшей конвергенции. Однако на данном экзамене компания Cisco уделяет больше внимания протоколу RSTP, чем на экзамене CCNP. Тем, кто по работе связан с коммутацией LAN, имеет смысл изучить работу и реализацию протокола 802.1w/RSTP на коммутаторах вашей сети.

Обзор

Резюме

- В локальной сети Ethernet есть три базовых компонента: устройства с платой сетевого интерфейса Ethernet, коммутаторы LAN Ethernet и кабели, соединяющие устройства.
- Коммутация LAN порождает проблему широковещательных штормов, когда MAC-адрес не обнаруживается в таблице MAC-адресов.
- Протокол распределенного связующего дерева переводит некоторые порты коммутатора в состояние блокировки, а другие в состояние перенаправления, чтобы предотвратить петли коммутации и широковещательные штормы.
- Алгоритм распределенного связующего дерева выбирает интерфейсы, подлежащие переводу в состояние перенаправления.
- Блокированный канал связи не перенаправляет фреймы, но остается активным, чтобы передавать управляющие сообщения STP.
- Принимая решение о переводе интерфейса в состояние перенаправления, протокол STP руководствуется тремя критериями.
- При выборе корневого коммутатора используются идентификаторы BID и сообщения Hello.
- Порт, получающий сообщение Hello с самой низкой стоимостью, отмечается как корневой.
- Если у какого-нибудь сегмента есть коммутаторы, анонсирующие одинаковую стоимость, побеждает коммутатор с наиболее низким идентификатором BID, а его порты становятся выделенными.
- Канал EtherChannel объединяет несколько параллельных сегментов в единый канал связи.
- Режим PortFast позволяет подключенному к хосту порту немедленно перейти в состояние перенаправления.
- Служба BPDU Guard отключает порт доступа, если получает сообщение BPDU.
- Протокол Rapid STP улучшает конвергенцию, устраняя или сокращая период ожидания.

Контрольные вопросы

Ответьте на эти вопросы. Ответы можно найти на последней странице главы. Полное объяснение ответов приведено в приложении B на веб-сайте.

1. Что из следующего истинно о логике перенаправления фреймов коммутатором SW1?

   A) Перенаправление на основании записи в таблице MAC-адресов для порта F0/1 доступа к сети VLAN.

Б) Перенаправление на основании записи в таблице MAC-адресов для порта F0/2 доступа к сети VLAN.

В) Перенаправление на основании записи в таблице MAC-адресов для порта F0/1 собственной сети VLAN.

Г) Перенаправление на основании записи в таблице MAC-адресов для всех сетей VLAN.

2. Рассмотрим следующий вывод команды:

```
SW1# show interfaces f0/11 status

Port  Name  Status  Vlan Duplex Speed Type
Fa0/11      connected 3   a-full 100  10/100BaseTX
```

Фрейм поступает на тот же порт (F0/1) доступа к сети VLAN 3. Фрейм предназначен для MAC-адреса FFFF.FFFF.FFFF. Что из следующего является истиной, на основании информации о порте F0/11 в выводе команды `show` и о том, перенаправит ли коммутатор SW1 фрейм через порт F0/11?

А) Вывод подтверждает, что коммутатор SW1 определенно перенаправит фрейм через порт F0/11.

Б) Вывод подтверждает, что коммутатор SW1 определенно не будет перенаправлять фрейм через порт F0/11.

В) Вывод подтверждает, что коммутатор SW1 может перенаправить фрейм через порт F0/11, но не обязательно.

3. Какие из следующих состояний порта по стандарту IEEE 802.1D являются стабильными состояниями, используемыми после завершения конвергенции в ходе работы протокола STP? (Выберите два ответа.)

А) Блокирования.

Б) Перенаправления.

В) Прослушивания.

Г) Самообучения.

Д) Игнорирования.

4. Какие из следующих состояний порта по стандарту IEEE 802.1D являются переходными, используемыми только в процессе конвергенции при работе протокола STP? (Выберите два ответа.)

А) Блокирования.

Б) Перенаправления.

В) Прослушивания.

Г) Самообучения.

Д) Игнорирования.

5. Какой из следующих идентификаторов мостов был бы выбран в качестве корневого, при условии, что коммутаторы с этими идентификаторами мостов находятся в одной и той же сети?

А) `32769:0200.1111.1111`.

Б) `32769:0200.2222.2222`.

В) `4097:0200.1111.1111`.

Г) 4097:0200.2222.2222.

Д) 40961:0200.1111.1111.

6. Какой из следующих фактов позволяет определить, насколько часто некорневой мост или коммутатор отправляет сообщения Hello BPDU протокола STP по стандарту 802.1d?

   А) Настройка конфигурации таймера Hello на этом коммутаторе.

   Б) Настройка конфигурации таймера Hello на корневом коммутаторе.

   В) Это сообщение всегда передается через каждые 2 секунды.

   Г) Коммутатор реагирует на модули BPDU, полученные от корневого коммутатора, посылая другой модуль BPDU через 2 секунды после получения модуля BPDU корневого коммутатора.

7. Какое средство протокола STP вынуждает интерфейс перейти в состояние пересылки, как только интерфейс становится физически активным?

   А) Протокол STP.

   Б) Канал EtherChannel.

   В) Функция Root Guard.

   Г) Режим PortFast.

Ключевые темы

Повторите все ключевые темы данной главы, отмеченные пиктограммой "Ключевая тема". Ключевые темы и соответствующие им страницы перечислены в табл. 1.8.

Таблица 1.8. Ключевые темы главы 1

Элемент	Описание	Страница
Список	Резюме по логике перенаправления коммутатора LAN	56
Табл. 1.1	Три класса проблем, вызываемых отсутствием протокола STP в избыточных локальных сетях	63
Табл. 1.2	STP: причины для перевода порта в состояние перенаправления или блокировки	66
Табл. 1.3	Поля пакета Hello протокола STP	67
Список	Логика выбора корневого коммутатора	69
Рис. 1.8	Так протокол STP фактически вычисляет стоимость от коммутатора SW3 до корневого коммутатора	71
Табл. 1.5	Стандартные стоимости маршрута через порт согласно IEEE	73
Список	Работа протокола STP в стабильных условиях	74
Табл. 1.6	Таймеры STP	74
Список	Определения происходящего в состояниях прослушивания и самообучения	76
Табл. 1.7	Состояния распределенного связующего дерева по стандарту IEEE 802.1D	77

Заполните таблицы и списки по памяти

Распечатайте приложение Г с веб-сайта или его раздел, относящийся к этой главе, и заполните таблицы и списки по памяти. В приложении Д приведены заполненные таблицы и списки для самоконтроля.

Ключевые термины

После первого прочтения главы попытайтесь дать определения следующим ключевым терминам. Но не расстраивайтесь, если не все получится сразу, в главе 22 описано, как использовать эти термины на завершающем этапе подготовки к экзамену.

состояние блокирования (blocking state), служба BPDU Guard (BPDU Guard), идентификатор моста (bridge ID), модуль данных протокола моста (Bridge Protocol Data Unit — BPDU), выделенный порт (designated port), канал EtherChannel (EtherChannel), задержка передачи данных (forward delay), состояние перенаправления (forwarding state), пакет Hello BPDU (Hello BPDU), стандарт IEEE 802.1d (IEEE 802.1d), состояние самообучения (learning state), таймер устаревания информации (MaxAge), режим PortFast (PortFast), корневой порт (root port), корневой коммутатор (root switch), корневая стоимость (root cost), протокол распределенного связующего дерева (Spanning Tree Protocol — STP)

Ответы на контрольные вопросы:

1 А. 2 В. 3 А и Б. 4 В и Г. 5 В. 6 Б. 7 Г.

Глава 2

Реализация протокола распределенного связующего дерева

Изначально коммутаторы Cisco LAN разрешают выполнение протокола распределенного связующего дерева (STP) на всех интерфейсах в каждой сети VLAN. Но сетевые инженеры средних и крупных локальных сетей Ethernet обычно желают изменить по крайней мере некоторые параметры протокола STP, чтобы повлиять на его выбор. Например, сетевой инженер настраивает его так, чтобы при работе всех коммутаторов и каналов связи он знал, какой коммутатор корневой и какие порты блокированы. Конфигурация может быть также настроена так, чтобы при отказе канала связи или коммутатора инженер мог предсказать новую топологию STP.

В этой главе обсуждаются параметры настройки протокола STP с учетом использования коммутаторами STP 802.1D. Первый главный раздел посвящен изменению различных параметров каждой сети VLAN, а также командам `show`, демонстрирующим текущее состояние протокола STP, на которое воздействует каждая команда конфигурации. Во втором главном разделе рассматривается поиск и устранение неисправностей протокола STP, включая углубленный анализ правил STP, обсуждавшихся в главе 1, а также продолжено описание различных команд `show` коммутатора.

В этой главе рассматриваются следующие экзаменационные темы
Технологии коммутации сетей LAN
Настройка и проверка работы PVSTP
Описание выбора корневого моста
Режим связующего дерева
Поиск и устранение неисправностей
Поиск и устранение неисправностей в работе RST
Корневой коммутатор
Приоритет
Правильный режим
Состояние порта
Поиск и устранение проблем EtherChannel

Основные темы

Настройка и проверка протокола STP

Обычно коммутаторы Cisco изначально используют протокол STP (IEEE 802.1D). Вполне можно купить коммутаторы Cisco, подключить их кабелями Ethernet к избыточной топологии, и протокол STP гарантирует передачу фреймов без петель, при этом даже не придется заботиться об изменении каких-либо параметров!

Хотя протокол STP работает без настройки, большинство сетей среднего и крупного размера извлекут выгоду из некоторой настройки конфигурации STP. При всех стандартных значениях коммутаторы выбирают корневой коммутатор на основании самого низкого прошитого MAC-адреса, поскольку изначально все они используют одинаковый приоритет STP. Однако лучше настроить коммутаторы так, чтобы корневой коммутатор был предсказуем.

Например, на рис. 2.1 представлен типичный проект LAN с двумя коммутаторами уровня распределения (D1 и D2). В проекте может быть множество коммутаторов уровня доступа, соединенных с конечными пользователями; на рисунке показаны только три коммутатора доступа (A1, A2 и A3). Большинство сетевых инженеров выбирают корневыми коммутаторы уровня распределения по множеству причин. Например, настройка может сделать коммутатор D1 корневым, обладающим самым низким приоритетом, а коммутатор D2 — следующим, с достаточно низким приоритетом, чтобы при отказе коммутатора D1 он стал корневым.

Ключевая тема

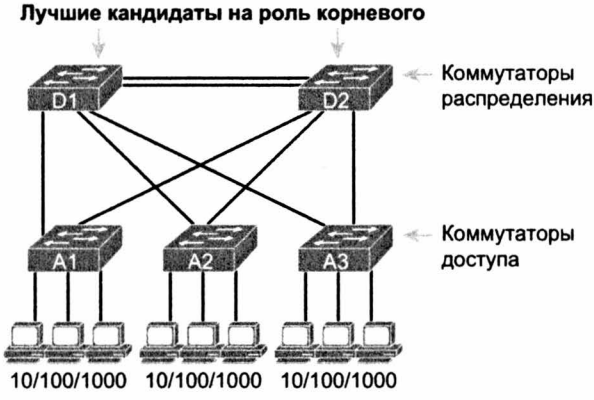


Рис. 2.1. Типичный выбор конфигурации: корневым стоит сделать коммутатор распределения

В данном разделе рассматривается множество тем, так или иначе касающихся конфигурации STP. Сначала рассмотрим параметры настройки STP как способ связи концепции из главы 1 с выбором конфигурации в этой главе. В следующем разделе рассматриваются некоторые из команд `show`, позволяющих подтвердить наличие стандартных параметров STP перед любыми изменениями конфигурации. В этом разделе приведены примеры настройки базовых и дополнительных средств протокола STP.

Установка режима STP

В главе 1 описана работа STP 802.1D в одной сети VLAN, а в настоящей главе речь пойдет о конфигурации протокола STP в коммутаторах Cisco. Один из главных вопросов: какой вид протокола STP предполагается использовать в сети LAN? Для ответа на этот вопрос необходимо обладать достаточной подготовкой.

Впервые IEEE стандартизировал протокол STP как стандарт IEEE 802.1D в 1990 году. В это время компания Cisco еще не продавала коммутаторы LAN и виртуальных локальных сетей еще не существовало. В результате с появлением коммутаторов, сетей VLAN и других передовых технологий LAN протокол STP претерпел несколько существенных изменений.

Ныне коммутаторы Cisco LAN позволяют использовать один из трех режимов протокола STP, отражающих его историю. Например, один из обсуждаемых в этой главе режимов, Per-VLAN Spanning Tree Plus (PVST+, или PVSTP), является собственной модификацией Cisco стандарта STP 802.1D. Часть *per-VLAN* (по каждой сети VLAN) в названии описывает основную задачу: протокол PVST+ создает разные топологии STP для каждой сети VLAN, тогда как стандарт 802.1D этого не предусматривает. В протоколе PVST+ также введен режим PortFast.

Со временем IEEE усовершенствовал стандарт STP 802.1D до Rapid STP (802.1w). Затем компания Cisco усовершенствовала этот стандарт, создав другой режим на коммутаторах Cisco: PVST+ (быстрый PVST+), или просто RPVST+. Он имеет все преимущества более нового стандарта IEEE per-VLAN.

Эта книга сосредоточена только на одном режиме: PVST+. Стандартно коммутаторы Cisco используют протокол PVST+. Для перевода коммутатора в этот режим можно использовать глобальную команду `spanning-tree mode pvst`. Кроме того, команда `spanning-tree mode rapid-pvst` позволяет использовать на коммутаторе режим RPVST+, а команда `spanning-tree mode mst` — режим MST (Multiple Spanning Tree — *множественное связующее дерево*). Все примеры в этой главе используют коммутатор 2960 со стандартным режимом PVST+.

Соотнесение концепций STP с параметрам настройки

Если вернуться к описанным в главе 1 подробностям работы протокола STP, то для принятия большинства решений он использует два типа чисел: идентификаторы BID и стоимости маршрута через порт. Остановимся на этих двух типах чисел и рассмотрим, что протокол STP делает внутренне.

- Использует BID для выбора корневого коммутатора. Побеждает коммутатор с наименьшим значением BID.
- Когда каждый некорневой коммутатор выбирает свой корневой порт (RP), он использует полную стоимость STP на каждом пути к корневому коммутатору.
- Когда коммутаторы выбирают, какой из портов станет выделенным (DP) на каждом сегменте LAN, используется корневая стоимость каждого коммутатора, которая, в свою очередь, вычисляется на основании стоимостей маршрута через порт STP.

Поэтому неудивительно, что коммутаторы Cisco позволяют задать части BID коммутатора и стоимости маршрута через порт STP, что, в свою очередь, влияет на выбор, осуществляемый каждым коммутатором STP.

Параметры конфигурации по каждой сети VLAN

Кроме настройки BID и стоимостей маршрута через порт STP, коммутаторы Cisco позволяют настраивать оба эти параметра по каждой сети VLAN. Обычно коммутаторы Cisco используют стандарт IEEE 802.1D, а не RSTP (802.1w), с собственным средством Cisco Per-VLAN Spanning Tree Plus (PVST+). Стандарт PVST+ (или просто PVST) позволяет создать индивидуальный экземпляр STP для каждой сети VLAN. Таким образом, перед рассмотрением настраиваемых параметров STP имеет смысл получить представление о фундаментальных концепциях протокола PVST+, поскольку параметры конфигурации для каждого экземпляра STP могут отличаться.

Основная идея представлена на рис. 2.2, где коммутатор SW3 перенаправляет трафик VLAN с нечетными номерами по левому магистральному каналу (Gi0/1), а VLAN — с четными номерами по правому магистральному каналу (Gi0/2).

Ключевая тема

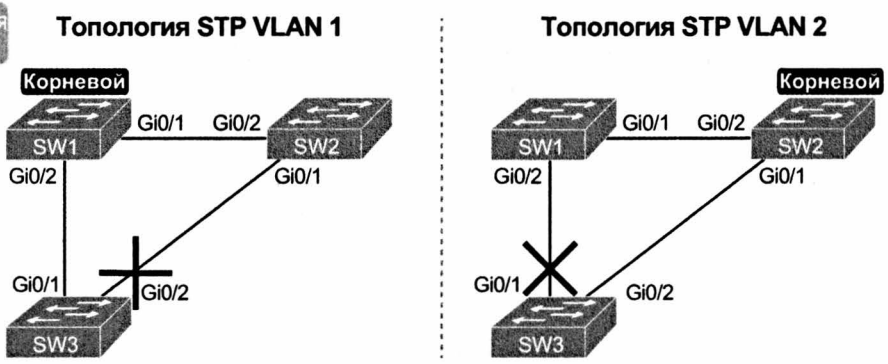


Рис. 2.2. Балансировка нагрузки при помощи протокола PVST+

Далее рассматривается изменение параметров BID и стоимости маршрута через порт STP по каждой VLAN с использованием стандартного режима PVST+.

Идентификатор моста и расширение системного идентификатора

Первоначально BID коммутатора формировался в результате объединения 2-байтового приоритета коммутатора и его 6-байтового MAC-адреса. Позже IEEE изменил правила, разделив первоначальное поле приоритета на два отдельных поля (рис. 2.3): 4-битовое поле приоритета и 12-битовое подполе *расширения системного идентификатора* (system ID extension), представляющего идентификатор VLAN.

Коммутаторы Cisco позволяют изменять только приоритетную часть BID. Коммутатор использует свой универсальный (прошитый) MAC-адрес как системный идентификатор. Он также включает идентификатор VLAN в 12-битовое поле расширения системного идентификатора. Единственная перестраиваемая сетевым инженером часть конфигурации — это 4-битовое поле приоритета.

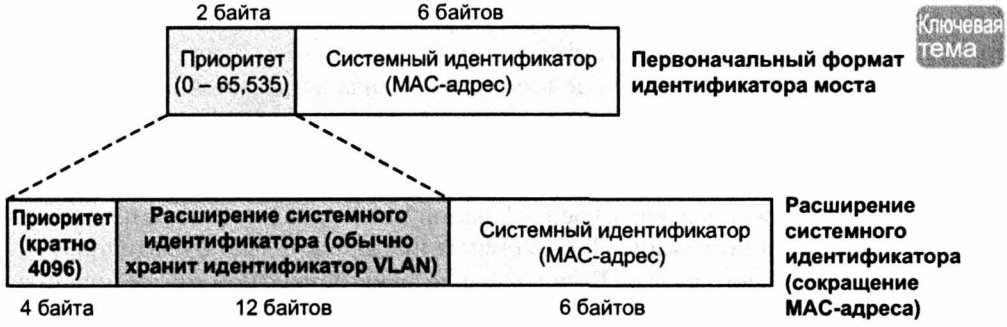


Рис. 2.3. Расширение системного идентификатора STP

Настройка значений, добавляемых в поле приоритета, вероятно, является одной из самых странных вещей, настраиваемых на маршрутизаторе или коммутаторе Cisco. Как показано на рис. 2.3, *сверху*, первоначально поле приоритета было 16-битовым числом, представляющим десятичное значение от 0 до 65 535. Из-за этого исторического факта нынешней команде конфигурации (`spanning-tree vlan` *`идентификатор_vlan`* `priority` *`x`*) требуется десятичное число от 0 до 65 535. И не просто любое число в этом диапазоне, а кратное 4096, т.е. 0, 4096, 8192, 12288 и так далее до 61 440.

Коммутатор все еще устанавливает первые 4 бита BID на основании заданного значения. Кроме того, 16 допустимых кратных 4096 значений от 0 до 61 440 имеют разные двоичные значения в первых 4 битах: 0000, 0001, 0010 и так далее до 1111. Коммутатор устанавливает истинный 4-битовый приоритет на основании первых 4 битов заданного значения.

Хотя исторические и конфигурационные подробности могут сделать идею приоритета BID немного замысловатой, наличие дополнительного 12-битового поля в идентификаторе BID на практике работает очень хорошо, поскольку оно применимо для идентификации VLAN. Идентификаторы VLAN находятся в диапазоне от 1 до 4094 и требуют 12 битов. Коммутаторы Cisco помещают идентификатор VLAN в поле расширения системного идентификатора, таким образом, у каждого коммутатора есть индивидуальный BID на каждую VLAN.

Например, коммутатор с настроенными сетями VLAN 1–4 со стандартным базовым приоритетом 32 768 имеет стандартный приоритет STP 32 769 для VLAN 1, 32 770 — для VLAN 2, 32 771 — для VLAN 3 и т.д. Таким образом, 16-разрядный приоритет можно рассматривать как базовый (заданный командой `spanningtree vlan` *`идентификатор_vlan`* `priority` *`x`*) плюс идентификатор VLAN.

Стоимость маршрута через порт по каждой VLAN

Стандартные значения интерфейсов коммутатора, согласно рекомендациям IEEE, приведены в табл. 1.6 главы 1. На интерфейсах, поддерживающих несколько скоростей, коммутаторы Cisco базируют стоимость на текущей фактической скорости. Таким образом, если интерфейс договорился об использовании более низкой скорости, стандартная стоимость STP отразит эту более низкую скорость. Если интерфейс договорился об использовании другой скорости, коммутатор динамически изменяет стоимость маршрута через этот порт STP.

В качестве альтернативы стоимость маршрута через порт STP коммутатора можно настроить подкомандой интерфейса `spanning-tree [vlan идентификатор_vlan] cost стоимость`. Чаще всего эта команда встречается на магистральных каналах, поскольку параметр стоимости на магистральных каналах оказывает влияние на корневую стоимость коммутатора, а параметр стоимости STP на портах доступа — нет.

Сама команда может включить идентификатор VLAN, а может и не включить. Для установки стоимости по каждой VLAN команда нуждается только в параметре `vlan` на портах магистрального канала. Если в команде на магистральном канале отсутствует параметр `vlan`, она устанавливает стоимость STP для всех VLAN, стоимость которых не установлена командой `spanning-tree vlan x cost` для данной VLAN.

Параметры настройки STP

В табл. 2.1 приведены стандартные настройки BID, стоимости маршрута через порт и необязательные команды конфигурации, рассматриваемые в этой главе.

Ключевая тема **Таблица 2.1. Стандартные значения STP и возможности для настройки**

Параметр	Стандартное значение	Команда, изменяющая стандартное значение
Приоритет BID	Базовое: 32 768	`spanning-tree vlan идентификатор_vlan root {primary | secondary}` `spanning-tree vlan идентификатор_vlan priority приоритет`
Стоимость интерфейса	От 100 до 10 Мбит/с От 19 до 100 Мбит/с От 4 до 1 Гбит/с От 2 до 10 Гбит/с	`spanning-tree vlan идентификатор_vlan cost стоимость`
PortFast	Не разрешено	`spanning-tree portfast`
BPDU Guard	Не разрешено	`spanning-tree bpduguard enable`

В следующем разделе описана проверка работы протокола STP в простой сети, наряду с изменением необязательных параметров.

Проверка работы STP

Прежде чем приступить к изменению конфигурации, рассмотрим несколько команд проверки STP. Это поможет закрепить знание стандартных параметров STP. В частности, примеры данного раздела используют сеть, представленную на рис. 2.4.

Пример 2.1 начинается с весьма полезной команды: `show spanning-tree vlan 10`, которая идентифицирует корневой коммутатор и выводит параметры локального коммутатора. Пример 2.1 демонстрирует вывод этой команды на коммутаторах SW1 и SW2.

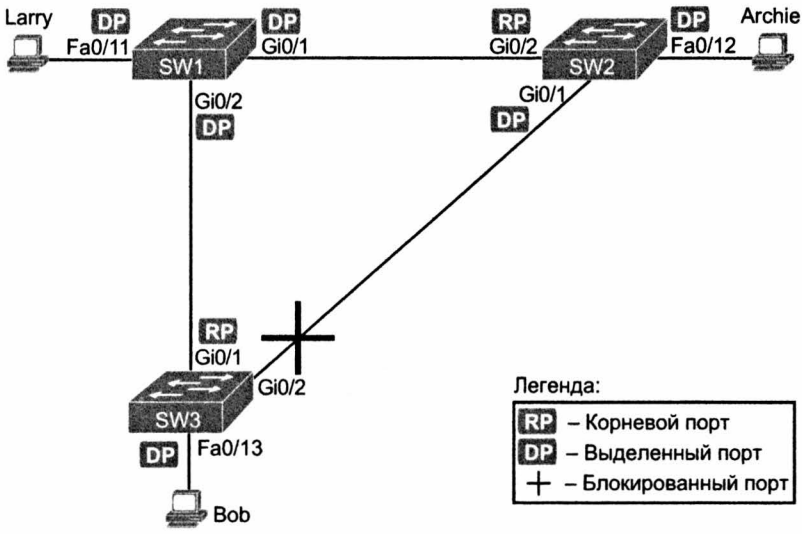


Рис. 2.4. Сеть LAN для примеров настройки и проверки STP

Пример 2.1. Состояние STP со стандартными параметрами на коммутаторах SW1 и SW2

```
SW1# show spanning-tree vlan 10

VLAN0010
  Spanning tree enabled protocol ieee
  Root ID     Priority    32778
              Address     1833.9d7b.0e80
              This bridge is the root
              Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

  Bridge ID   Priority    32778 (priority 32768 sys-id-ext 10)
              Address     1833.9d7b.0e80
              Hello Time  2 sec Max Age 20 sec Forward Delay 15 sec
              Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------
Fa0/11              Desg FWD 19        128.11   P2p Edge
Gi0/1               Desg FWD 4         128.25   P2p
Gi0/2               Desg FWD 4         128.26   P2p


SW2# show spanning-tree vlan 10

VLAN0010
  Spanning tree enabled protocol ieee
  Root ID     Priority    32778
              Address     1833.9d7b.0e80
              Cost        4
              Port        26 (GigabitEthernet0/2)
              Hello Time  2 sec Max Age 20 sec Forward Delay 15 sec
```

```
  Bridge ID  Priority    32778 (priority 32768 sys-id-ext 10)
             Address     1833.9d7b.1380
             Hello Time  2 sec Max Age 20 sec Forward Delay 15 sec
             Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------
Fa0/12              Desg FWD 19        128.12   P2p
Gi0/1               Desg FWD 4         128.25   P2p
Gi0/2               Root FWD 4         128.26   P2p
```

Пример 2.1 начинается с вывода команды `show spanning-tree vlan 10` на коммутаторе SW1. Сначала команда выводит три главных группы сообщений: о корневом и локальном коммутаторах, а также о ролях интерфейсов и их состоянии. В данном случае коммутатор SW1 выводит как идентификатор корневого коммутатора собственный BID, сопровождая его однозначным утверждением "This bridge is the root" ("Этот мост корневой"), подтверждающим, что коммутатор SW1 теперь корневой для сети VLAN 10 топологии STP.

Теперь сравним выделенные строки той же команды на коммутаторе SW2 в нижней части примера. Коммутатор SW2 выводит BID коммутатора SW1 как корневого; другими словами, коммутатор SW2 соглашается, что коммутатор SW1 победил на выборах корневого. Коммутатор SW2 не выводит фразу "This bridge is the root". Затем, после BID корневого коммутатора, коммутатор выводит подробности о собственном BID.

Вывод подтверждает также несколько стандартных значений. В первую очередь, каждый коммутатор выводит приоритетную часть BID как отдельное число: 32778. Это значение получается из стандартного приоритета 32768, плюс VLAN 10, что дает в общей сложности 32778. Вывод демонстрирует также стоимости 19 и 4 для интерфейсов Fast Ethernet и Gigabit Ethernet соответственно.

И наконец, внизу вывода команды `show spanning-tree` указаны все интерфейсы в VLAN, включая магистральные каналы, их роли STP и состояния. Например, на коммутаторе SW1 представлены три интерфейса с ролью `Desg`, т.е. выделенного порта (DP), и состоянием `FWD`, т.е. перенаправления. Коммутатор SW2 представляет три интерфейса: два DP и один корневой порт (все три в состоянии `FWD`).

В примере 2.1 приведено много полезной информации STP, но две другие команды, представленные в примере 2.2, выводят информацию о BID в более короткой форме. Первая команда, `show spanning-tree root`, выводит BID корневого коммутатора для каждой сети VLAN. Кроме того, она выводит также другие подробности, включая корневую стоимость локального коммутатора и корневой порт. Другая команда, `show spanning-tree vlan 10 bridge`, разделяет BID на составные части. В данном примере демонстрируется приоритет SW2 как стандартное значение 32768, идентификатор VLAN 10 и MAC-адрес.

Пример 2.2. Вывод корневого коммутатора и BID локального коммутатора на коммутаторе SW2

```
SW2# show spanning-tree root
                                        Root      Hello Max Fwd
Vlan             Root ID                Cost      Time  Age Dly Root Port
---------------- ---------------------- --------- ----- --- --- ------------
VLAN0001         32769 1833.9d5d.c900 23          2   20  15 Gi0/1
VLAN0010         32778 1833.9d7b.0e80  4          2   20  15 Gi0/2
VLAN0020         32788 1833.9d7b.0e80  4          2   20  15 Gi0/2
VLAN0030         32798 1833.9d7b.0e80  4          2   20  15 Gi0/2
VLAN0040         32808 1833.9d7b.0e80  4          2   20  15 Gi0/2

SW2# show spanning-tree vlan 10 bridge
Hello Max Fwd
Vlan             Bridge ID                          Time  Age Dly Protocol
---------------- ---------------------------------- ----- --- --- --------
VLAN0010         32778 (32768, 10) 1833.9d7b.1380      2   20  15 ieee
```

Обратите внимание: у обеих команд в примере 2.2 есть параметр VLAN: `show spanning-tree [vlan x] root` и `show spanning-tree [vlan x] bridge`. Без указания VLAN каждая команда выводит по одной строке на каждую VLAN; при указании VLAN выводится та же информация, но только для одной указанной сети VLAN.

Настройка стоимости маршрута через порт STP

Для изменения стоимости маршрута через порт STP достаточно простой подкоманды интерфейса `spanning-tree [vlan x] cost x`. Чтобы показать, как это работает, рассмотрим следующий пример изменения в сети, представленной на рис. 2.4.

Ранее на рис. 2.4 при стандартных настройках коммутатор SW1 был корневым, а коммутатор SW3 блокировал свой интерфейс G0/2. Для доступа к корневому коммутатору так, как показано на рис. 2.5, исходя из стандартной стоимости STP 4 для гигабитового интерфейса, коммутатор SW3 должен выбрать между путями со стоимостями 4 и 8.

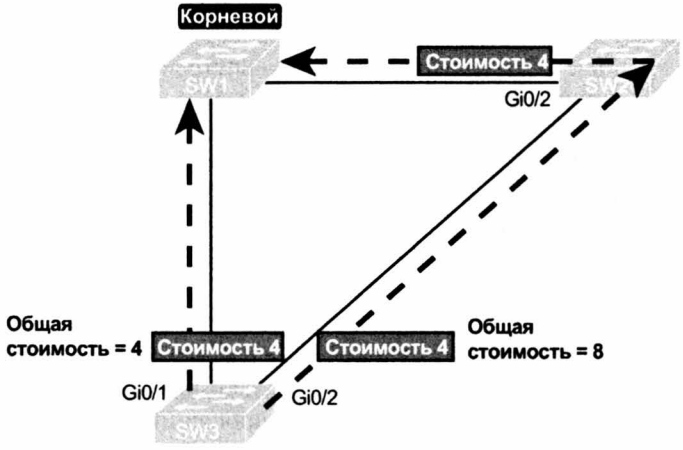


Рис. 2.5. Анализ текущей корневой стоимости коммутатора SW3 со стандартным значением 4

Для того чтобы показать результат изменения стоимости маршрута через порт, в следующем примере стоимость маршрута через порт G0/1 коммутатора SW3 устанавливается выше, чтобы лучший путь к корневому коммутатору проходил через порт G0/2. В примере 2.3 приведено также несколько других интересных последствий.

Пример 2.3. Изменение стоимости маршрута через порт STP и переход в состояние перенаправления

```
Spanning Tree event debugging is on
SW3# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW3(config)# interface gigabitethernet0/1
SW3(config-if)# spanning-tree vlan 10 cost 30
SW3(config-if)# ^Z
SW3#
*Mar 11 06:28:00.860: STP: VLAN0010 new root port Gi0/2, cost 8
*Mar 11 06:28:00.860: STP: VLAN0010 Gi0/2 -> listening
*Mar 11 06:28:00.860: STP: VLAN0010 sent Topology Change Notice on Gi0/2
*Mar 11 06:28:00.860: STP[10]: Generating TC trap for port GigabitEther-
net0/1
*Mar 11 06:28:00.860: STP: VLAN0010 Gi0/1 -> blocking
*Mar 11 06:28:15.867: STP: VLAN0010 Gi0/2 -> learning
*Mar 11 06:28:30.874: STP[10]: Generating TC trap for port GigabitEther-
net0/2
*Mar 11 06:28:30.874: STP: VLAN0010 sent Topology Change Notice on Gi0/2
*Mar 11 06:28:30.874: STP: VLAN0010 Gi0/2 -> forwarding
```

Пример начинается с команды `debug spanning-tree events` на коммутаторе SW1. Эта команда требует от коммутатора выдавать регистрационные сообщения отладки при каждом изменении роли интерфейса STP или его состояния. В примере эти сообщения отображаются в ходе изменения конфигурации.

Далее в примере показано изменение стоимости маршрута через порт SW3 в сети VLAN 10 на 30 при помощи подкоманды интерфейса `spanning-tree vlan 10 cost 30`. Согласно рисунку, корневая стоимость через порт G0/1 коммутатора SW3 составит теперь 30 вместо 4. В результате лучшей стоимостью от коммутатора SW3 до корневого коммутатора будет 8, а его порт G0/2 станет корневым.

Отладочные сообщения извещают о том, что внутренне делает протокол STP на коммутаторе SW3, причем с временны*ми* метками. Обратите внимание, что первые пять отладочных сообщений, отображенных непосредственно после выхода пользователя из режима конфигурации, создаются в данном случае одновременно (в течение той же миллисекунды). А именно: интерфейс G0/1, находившийся в состоянии перенаправления, немедленно переходит в состояние блокировки. Интерфейс G0/2, который был блокирован, переходит не в состояние перенаправления, а в состояние прослушивания (по крайней мере, согласно этому сообщению).

Теперь найдите отладочное сообщение, отображающее переход интерфейса G0/2 в состояние самообучения, за ним находится следующее, демонстрирующее переход интерфейса в состояние перенаправления. Сколько времени прошло между сообщениями? В каждом случае временны*е* метки сообщений свидетельствуют о 15 секундах. В данном случае коммутаторы использовали стандартное значение таймера задержки пересылки (15 секунд). Таким образом, эти отладочные сообщения под-

тверждают этапы перехода интерфейса STP из состояния блокировки в состояние перенаправления.

Если отладка при настройке стоимости не была включена, то впоследствии можно использовать команду `show` для подтверждения выбора коммутатором SW3 порта G0/2 в качестве своего RP. Команда `show spanning-tree vlan 10` в примере 2.4 демонстрирует новое значение стоимости маршрута через порт STP на коммутаторе SW3, а также новый корневой порт и корневую стоимость. Обратите внимание, что интерфейс G0/2 теперь указывается как корневой порт. Вверху вывода указана корневая стоимость коммутатора SW3, равная 8, что согласуется с результатом анализа, представленным на рис. 2.5.

Пример 2.4. Новое состояние и параметры STP на коммутаторе SW3

```
SW3# show spanning-tree vlan 10

VLAN0010
  Spanning tree enabled protocol ieee
  Root ID     Priority    32778
              Address     1833.9d7b.0e80
              Cost        8
              Port        26 (GigabitEthernet0/2)
              Hello Time  2 sec Max Age 20 sec Forward Delay 15 sec

  Bridge ID   Priority    32778 (priority 32768 sys-id-ext 10)
              Address     f47f.35cb.d780
              Hello Time  2 sec Max Age 20 sec Forward Delay 15 sec
              Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------
Fa0/23              Desg FWD 19        128.23   P2p
Gi0/1               Altn BLK 30        128.25   P2p
Gi0/2               Root FWD 4         128.26   P2p
```

Влияние изменения приоритета на выбор корневого коммутатора

Еще один настраиваемый параметр STP — приоритет коммутатора — позволяет влиять на выбор корневого коммутатора. Приоритет может быть установлен явно при помощи глобальной команды конфигурации `spanning-tree vlan` *`идентификатор_vlan`* `priority` *`значение`*, устанавливающей базовый приоритет коммутатора. (Значение параметра этой команды должно быть кратно 4096.)

Однако компания Cisco предоставляет и лучший способ задания конкретного значения приоритета. В большинстве сетей инженеры выбирают на роль корневого два коммутатора: один основной и второй, который станет корневым, если откажет первый. Операционная система коммутатора предоставляет для этого команды `spanning-tree vlan` *`идентификатор_vlan`* `root primary` и `spanning-tree vlan` *`идентификатор_vlan`* `root secondary`.

Команда `spanning-tree vlan` *`идентификатор_vlan`* `root primary` указывает коммутатору установить свой приоритет достаточно низким, чтобы стать корневым прямо сейчас. Коммутатор выявляет текущий корневой коммутатор в этой

VLAN и его приоритет. Затем локальный коммутатор выбирает такое значение приоритета, которое сделает его корневым.

С учетом того, что коммутаторы Cisco используют стандартный базовый приоритет 32 768, эта команда выбирает базовый приоритет следующим образом:

Ключевая тема **Две ветви логики выбора нового базового приоритета STP командой `spanning-tree root primary`**

- Если базовый приоритет нынешнего корневого коммутатора выше 24 576, *локальный коммутатор использует базовый приоритет 24 576.*
- Если базовый приоритет нынешнего корневого коммутатора составляет 24 576 или ниже, локальный коммутатор устанавливает свой базовый приоритет в самое высокое кратное 4096 значение, все еще позволяющее локальному коммутатору стать корневым.

Для коммутатора, предназначенного на роль корневого, если первый корневой коммутатор откажет, используется команда `spanning-tree vlan` *идентификатор_vlan* `root secondary`. Эта команда очень похожа на команду `spanning-tree vlan` *идентификатор_vlan* `root primary`, но со значением приоритета хуже, чем у первичного корневого коммутатора, но лучше, чем у всех других коммутаторов. Эта команда устанавливает базовый приоритет коммутатора в 28 672 независимо от текущего значения приоритета текущего корневого коммутатора.

Например, на рис. 2.4-2.5 коммутатор SW1 был корневым, и, как свидетельствуют различные команды, все три коммутатора использовали стандартный базовый приоритет 32 768. Пример 2.5 демонстрирует конфигурацию, делающую первичным корневым коммутатор SW2, а коммутатор SW1 — вторичным корневым, только чтобы продемонстрировать их обмен ролями. В результате выполнения этих команд коммутатор SW2 получает базовый приоритет 24 576, а SW1 — 28 672.

Пример 2.5. Как сделать коммутатор SW2 первичным корневым, а SW1 — вторичным корневым

```
! Сначала на SW2:
SW2# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW2(config)# spanning-tree vlan 10 root primary
SW2(config)# ^Z


! Теперь SW1 настраивается как резервный
SW1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW1(config)# spanning-tree vlan 10 root secondary
SW1(config)# ^Z
SW1#

! Следующая команда демонстрирует BID локального коммутатора (SW1)
SW1# show spanning-tree vlan 10 bridge

                                                Hello Max Fwd
Vlan            Bridge ID                       Time  Age Dly Protocol
```

```
---------------- ---------------------------------- ------ --- --- --------
VLAN0010         28682 (28672, 10) 1833.9d7b.0e80    2    20  15 ieee

! Следующая команда демонстрирует BID корневого коммутатора (SW2)
SW1# show spanning-tree vlan 10 root

                                        Root      Hello Max Fwd
Vlan             Root ID                Cost      Time  Age Dly Root Port
---------------- -------------------- --------- ----- --- --- -----------
VLAN0010         24586 1833.9d7b.1380     4        2    20  15 Gi0/1
```

Вывод двух команд show однозначно указывает установленные на каждом коммутаторе значения приоритетов. Первая команда, show spanning-tree bridge, выводит информацию о BID локального коммутатора, а команда show spanning-tree root о BID корневого коммутатора, о корневой стоимости локального коммутатора и о корневом порте (если это не корневой коммутатор). Таким образом, коммутатор SW1 выводит собственный BID с приоритетом 28 682 (базовый 28 672, для VLAN 10) согласно команде show spanning-tree bridge, а также приоритет корневого коммутатора как 24 586 для VLAN 10, т.е. базовые 24 576 плюс 10 для VLAN 10, согласно команде show spanning-tree root.

Заметим, что в качестве альтернативы можно задать конкретное значение приоритета. На коммутаторе SW1 можно использовать команду spanning-tree vlan 10 priority 28672, а на коммутаторе SW2 — команду spanningtree vlan 10 priority 24576. В данном случае обе возможности привели бы к тому же результату.

Настройка режима PortFast и службы BPDU Guard

Режим PortFast и службу BPDU Guard можно легко разрешить на любом интерфейсе, причем двумя способами. Один лучше подходит для разрешения этих средств на некоторых портах, а другой — для разрешения этих средств почти на каждом порте доступа.

Чтобы разрешить средство только на одном порте за раз, используйте подкоманды интерфейса spanning-tree portfast и spanning-tree bpduguard enable. В примере 2.6 представлен процесс разрешения обоих средств на интерфейсе F0/4 коммутатора SW3. (Обратите также внимание на длинное предупреждающее сообщение, выдаваемое операционной системой IOS при разрешении режима PortFast; использование режима PortFast на порту, подключенном к другим коммутаторам, может действительно создать серьезные проблемы.)

Пример 2.6. Разрешение режима PortFast и службы BPDU Guard на одном интерфейсе

```
SW3# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW3(config)# interface fastEthernet 0/4
SW3(config-if)# spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
  host. Connecting hubs, concentrators, switches, bridges, etc... to this
  interface when portfast is enabled, can cause temporary bridging loops.
  Use with CAUTION
```

```
%Portfast has been configured on FastEthernet0/4 but will only
  have effect when the interface is in a non-trunking mode.

SW3(config-if)# spanning-tree bpduguard ?
  disable Disable BPDU guard for this interface
  enable Enable BPDU guard for this interface

SW3(config-if)# spanning-tree bpduguard enable
SW3(config-if)# ^Z
SW3#
*Mar 1 07:53:47.808: %SYS-5-CONFIG_I: Configured from console by console
SW3# show running-config interface f0/4
Building configuration...

Current configuration : 138 bytes
!
interface FastEthernet0/4
  switchport access vlan 104
  spanning-tree portfast
  spanning-tree bpduguard enable
end

SW3# show spanning-tree interface fastethernet0/4 portfast
VLAN0104            enabled
```

Вторая половина примера подтверждает конфигурацию на интерфейсе и состояние режима PortFast. Команда `show running-config` просто подтверждает, что коммутатор записал две команды конфигурации. Команда `show spanning-tree interface fastethernet0/4 portfast` выводит состояние интерфейса PortFast (если режим PortFast включен и интерфейс работает, состояние отображается как просто разрешенное).

Когда в режиме PortFast и службе BPDU Guard нуждается большинство портов коммутатора, лучше подходит альтернативная конфигурация. Стандартно оба средства на каждом интерфейсе коммутатора отключены. Альтернативный способ настройки позволяет изменить стандартные значения режима PortFast и службы BPDU Guard, которые будут разрешены на каждом интерфейсе. Впоследствии можно отключить эти средства на соответствующих портах.

Чтобы изменить стандартные значения, используйте эти две глобальные команды:

- `spanning-tree portfast default`
- `spanning-tree portfast bpduguard default`

Затем, чтобы переопределить стандартные значения или отключить эти средства, используйте следующие подкоманды интерфейса:

- `spanning-tree portfast disable`
- `spanning-tree bpduguard disable`

Настройка канала EtherChannel

Как упоминалось в главе 1, два соседних коммутатора могут рассматривать несколько параллельных каналов связи между ними как один логический канал связи — *EtherChannel*. Протокол STP работает с каналом EtherChannel в целом, а не

с отдельными физическими каналами связи, поэтому он блокирует или разблокирует весь логический канал EtherChannel к определенной сети VLAN. В результате находящийся в состоянии перенаправления коммутатор способен балансировать трафик, распределяя его по всем физическим каналам связи в канале EtherChannel. Без канала EtherChannel только одному из параллельных каналов между двумя коммутаторами было бы позволено перенаправлять трафик, а остальные каналы протокол STP блокировал бы.

Канал EtherChannel может быть одним из наиболее сложных средств коммутатора. Во-первых, есть несколько параметров настройки, поэтому следует помнить об их совместимости. Во-вторых, коммутаторам требуется также множество других параметров всех интерфейсов канала связи, поэтому следует знать и эти параметры.

Данный раздел посвящен правильной конфигурации канала EtherChannel. Последующий раздел, "Поиск и устранение неисправностей канала EtherChannel", посвящен большинству потенциальных проблем канала EtherChannel, а также проверке коммутатором всех этих параметров конфигурации, прежде чем он позволит работать каналу EtherChannel.

Настройка канала EtherChannel вручную

Самый простой способ настройки канала EtherChannel заключается в добавлении правильной команды конфигурации `channel-group` с ключевым словом `on` на каждый физический интерфейс каждого коммутатора. Ключевое слово `on` указывает коммутатору присоединить физический интерфейс к каналу EtherChannel.

Но перед переходом к настройке и проверке необходимо заметить, что термины *канал EtherChannel*, *интерфейс PortChannel* и *группа Channel-group* являются синонимами. Как ни странно, операционная система IOS использует команду конфигурации `channel-group`, но затем, отображая ее состояние, использует команду `show etherchannel`. Затем вывод команды `show` использует термины "EtherChannel" и "Channel-group" вместо термина "PortChannel". Таким образом, обратите особое внимание на эти три термина в примере.

Для настройки канала EtherChannel вручную необходимо предпринять следующее.

Ключевая тема

Этапы настройки канала EtherChannel вручную

Этап 1 Добавьте подкоманду интерфейса `channel-group` *значение* `mode on` на каждый физический интерфейс, который должен быть частью канала

Этап 2 Используйте то же значение для всех команд на том же коммутаторе, но значение команды `channel-group` на соседнем коммутаторе может отличаться

В примере 2.7 показана сеть с двумя каналами связи между коммутаторами SW1 и SW2 (рис. 2.6). Две команды `show` отображают для коммутатора SW1 два интерфейса, помещенных в группу канала 1.

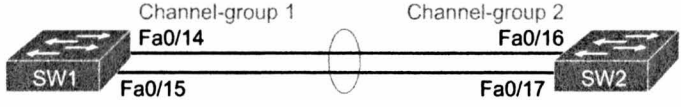


Рис. 2.6. Пример сети LAN, использующей канал EtherChannel

Пример 2.7. Настройка и мониторинг канала EtherChannel

```
SW1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW1(config)# interface fa 0/14
SW1(config-if)# channel-group 1 mode on
SW1(config)# interface fa 0/15
SW1(config-if)# channel-group 1 mode on
SW1(config-if)# ^Z

SW1# show spanning-tree vlan 3

VLAN0003
  Spanning tree enabled protocol ieee
  Root ID     Priority    28675
              Address     0019.e859.5380
              Cost        12
              Port        72 (Port-channel1)
              Hello Time  2 sec Max Age 20 sec Forward Delay 15 sec

  Bridge ID   Priority    28675 (priority 28672 sys-id-ext 3)
              Address 0019.e86a.6f80
              Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
              Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Po1              Root FWD 12        128.64   P2p Peer(STP)

SW1# show etherchannel 1 summary
Flags: D - down P - bundled in port-channel
       I - stand-alone s - suspended
       H - Hot-standby (LACP only)
       R - Layer3 S - Layer2
       U - in use f - failed to allocate aggregator

       M - not in use, minimum links not met
       u - unsuitable for bundling
       w - waiting to be aggregated
       d - default port

Number of channel-groups in use:  1
Number of aggregators:            1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1(SU)         -          Fa0/14(P) Fa0/15(P)
```

Уделим некоторое время рассмотрению вывода двух командах `show` в примере. Сначала команда `show spanning-tree` выводит как интерфейс Po1 — сокращение от PortChannel1. Этот интерфейс существует благодаря команде `channel-group` с параметром `1`. Протокол STP больше не используется на физических интерфейсах F0/14 и F0/15, вместо этого он работает на интерфейсе PortChannel1, поэтому в выводе отображается только этот интерфейс.

Теперь обратите внимание на вывод команды `show etherchannel 1 summary`. Под заголовком `Port-channel` она выводит канал Po1. Она также выводит в списке портов интерфейсы F0/14 и F0/15, с пометкой (P) возле каждого. Метка `P` означает, что порты объединены в канале портов, а следовательно, они прошли все проверки конфигурации и допустимы для включения в канал.

Настройка канала EtherChannel динамически

Коммутаторы Cisco поддерживают два протокола, позволяющих коммутаторам вести переговоры о том, станет ли конкретный канал связи частью канала EtherChannel или нет. Как правило, конфигурация разрешает использование протокола для группы каналов с конкретным номером. В этом случае коммутатор может использовать протокол для обмена сообщениями между соседними коммутаторами, позволяющий проверить все параметры конфигурации. Если данный физический канал связи подходит, он добавляется к каналу EtherChannel и используется; в противном случае он отключается и не используется, пока несогласованность конфигурации не будет устранена.

В данном разделе говорится в основном о том, как заставить работать канал EtherChannel, а конкретные параметры, способные привести к его отказу, рассматриваются ниже, в разделе "Поиск и устранение неисправностей канала EtherChannel".

Коммутаторы Cisco поддерживают собственный *протокол объединения портов* (Port Aggregation Protocol — PAgP) и стандартизированный IEEE *протокол управления объединением каналов* (Link Aggregation Control Protocol — LACP), созданный на основании стандарта IEEE 802.3ad. Хотя между ними и есть различие, оба они выполняют одну задачу: проведение переговоров, гарантирующих фактическое использование в канале EtherChannel только каналов связи, прошедших проверку конфигурации.

Для настройки любого протокола коммутатор использует команды конфигурации `channel-group` на каждом коммутаторе, но с ключевым словом, означающим либо "использовать этот протокол и начать переговоры", либо "использовать этот протокол и ожидать начала переговоров от другого коммутатора". Как показано на рис. 2.7, ключевые слова `desirable` и `auto` разрешают протокол PAgP, а ключевые слова `active` и `passive` — протокол LACP. При этих параметрах по крайней мере одна из сторон должна начать переговоры. Другими словами, при использовании протокола PAgP по крайней мере на одной из этих двух сторон должен быть использован параметр `desirable`, а при протоколе LACP — параметр `active`.



Рис. 2.7. Правильные комбинации параметров в конфигурации канала EtherChannel

ВНИМАНИЕ!

Не используйте параметр `on` на одном конце и параметр `auto` или `desirable` (либо `active` или `passive` в случае LACP) на соседнем коммутаторе. Параметр `on` не использует ни протокол PAgP, ни протокол LACP, поэтому использующая его на другом конце конфигурация, будь то протокол PAGP или LACP, не сможет сформировать работоспособный канал EtherChannel.

Например, можно было бы изменить конфигурацию в примере 2.7 командами `channel-group 1 mode desirable` на обоих интерфейсах при помощи команды `channel-group 2 mode auto` на коммутаторе SW2.

Поиск и устранение неисправностей STP

Заключительный раздел этой главы посвящен применению информации, представленной в главе 1 и в первой половине данной главы. Хотя этот раздел и поможет в поиске и устранении проблем STP в реальных сетях, его основная задача — подготовить к ответам на вопросы об STP на экзаменах CCNA.

Затруднения с вопросами о протоколе STP испытывают многие экзаменуемые. Протокол STP использует множество правил, иногда конфликтующих друг с другом. Не обладая достаточным практическим опытом работы с протоколом STP, люди обычно не доверяют собственным ответам. Кроме того, работающим с реальными сетями, вероятно, не часто приходится искать и устранять проблемы протокола STP, поскольку он запущен изначально и хорошо работает со стандартными параметрами конфигурации в малых и средних сетях. Поэтому, прежде чем приступать к сложным вопросам по протоколу STP, следует выработать хорошую стратегию поиска и устранения неисправностей.

Данный раздел содержит обзор правил STP, подчеркивая некоторые важные моменты поиска и устранения неисправностей. В частности, здесь более подробно рассматриваются схемы разрешения конфликтов, используемые протоколом STP при принятии решения. Кроме того, даны некоторые практические рекомендации по ответам на такие экзаменационные вопросы, как "Какой коммутатор является корневым?"

Определение корневого коммутатора

Определить корневой коммутатор STP очень просто, если известны BID всех коммутаторов: достаточно выбрать самое низкое значение. Если приоритеты и MAC-адреса в вопросе указаны отдельно, как это обычно бывает в выводе некоторых команд `show`, выберите коммутатор с самым низким приоритетом или, в ином случае, с наиболее низким значением MAC-адреса.

Для полной ясности скажем, что протокол STP не использует и не нуждается в схеме разрешения конфликтов для выбора корневого коммутатора. Для последних 48 битов идентификатора BID коммутатор использует свой уникальный MAC-адрес. Поскольку MAC-адреса уникальны, одинаковых BID тоже никогда не будет, следовательно, нет необходимости в схеме разрешения конфликтов.

Экзаменационный вопрос о корневом коммутаторе не может быть столь простым, как список идентификаторов BID, из которых следует выбрать "лучший". Вероятней всего, это будет симлет, подразумевающий ввод любых команд `show` по вашему выбо-

ру или вопрос с несколькими вариантами ответов, содержащих вывод одной или двух команд. Для выяснения остального следует применить алгоритм STP.

Встретив экзаменационный вопрос об использовании эмулятора или содержащий строки вывода, используйте следующую простую стратегию исключения коммутаторов.

Стратегия поиска корневого коммутатора для экзаменационных вопросов



Этап 1 Начните со списка или с диаграммы коммутаторов, считая их все возможными корневыми

Этап 2 Исключите все коммутаторы, у которых есть корневой порт (`show spanning-tree`, `show spanning-tree root`), поскольку у корневых коммутаторов их нет

Этап 3 Всегда используйте команду `show spanning-tree`, поскольку она способна непосредственно идентифицировать локальный коммутатор как корневой: сообщение "`This switch is the root`" в пятой строке вывода

Этап 4 Всегда используйте команду `show spanning-tree root`, поскольку она способна косвенно идентифицировать локальный коммутатор как корневой: если локальный коммутатор является корневым, столбец `RP` пуст

Этап 5 В случае симлета, вместо беспорядочных попыток опроса коммутаторов, проследите корневые порты. Например, если начать с коммутатора SW1 и если его порт G0/1 является корневым, стоит опросить коммутатор на другом конце канала, подключенного к порту G0/1

Этап 6 В случае симлета используйте команду `show spanning-tree vlan` *x* на нескольких коммутаторах и запишите корневой коммутатор, а порты RP и DP позволят быстро выяснить большинство фактов о протоколе STP. Если возможно, используйте эту стратегию

Один из этапов этого списка, исключение коммутаторов, обладающих RP, зачастую игнорируют. У корневых коммутаторов нет корневых портов, поэтому любой коммутатор с портом RP может быть исключен из списка возможных корневых коммутаторов данной VLAN. Пример 2.8 демонстрирует две команды на коммутаторе SW2 в некой локальной сети, подтверждающие наличие у него порта RP. Следовательно, коммутатор SW2 не является корневым.

Пример 2.8. Исключение коммутатора из возможных корневых на основании наличия корневого порта

```
SW2# show spanning-tree vlan 20 root

                                        Root        Hello Max Fwd
Vlan             Root ID                Cost        Time  Age Dly Root Port
---------------- ---------------------- ----------- ----- --- --- -----------
VLAN0020         32788 1833.9d7b.0e80    4          2      20  15 Gi0/2

SW2# show spanning-tree vlan 20

VLAN0020
  Spanning tree enabled protocol ieee
  Root ID     Priority    32788
              Address     1833.9d7b.0e80
              Cost        4
```

```
            Port         26 (GigabitEthernet0/2)
            Hello Time   2 sec Max Age 20 sec Forward Delay 15 sec

  Bridge ID Priority     32788 (priority 32768 sys-id-ext 20)
            Address      1833.9d7b.1380
            Hello Time   2 sec Max Age 20 sec Forward Delay 15 sec
            Aging Time   15 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------
Gi0/1               Desg FWD 4         128.25   P2p
Gi0/2               Root FWD 4         128.26   P2p
```

Обе команды идентифицируют порт G0/2 коммутатора SW2 как его порт RP, поэтому, следуя рекомендациям, попробуйте опросить следующий коммутатор на другом конце интерфейса G0/2.

Определение корневого порта на некорневых коммутаторах

Определение корневого порта коммутатора в выводе команды `show` относительно просто. Как показано в примере 2.7, обе команды, `show spanning-tree` и `show spanning-tree root`, указывают корневой порт локального коммутатора, подтверждая, что это некорневой коммутатор. Куда сложней экзаменационный вопрос, требующий определить, как коммутаторы выбирают порт RP на основании корневой стоимости каждого пути к корневому коммутатору с применением схем разрешения конфликтов.

Напомним, что у каждого некорневого коммутатора есть один и только один порт RP для каждой VLAN. Для его выбора коммутатор прослушивает поступающие сообщения Hello *модуля данных протокола моста* (Bridge Protocol Data Unit — BPDU). Для каждого полученного сообщения Hello коммутатор добавляет указанную в нем стоимость к стоимости входящего интерфейса (интерфейса, на котором было получено сообщение Hello). Это суммарное значение — корневая стоимость по данному пути. Побеждает самая низкая корневая стоимость, и локальный коммутатор использует свой локальный порт с наименьшим значением стоимости корневого пути как корневой порт.

Хотя и более сложными словами, но это описание повторяет ту же концепцию, что и рис. 1.8 в главе 1.

Если в экзаменационном вопросе есть схема сети LAN, то, как правило, лучше подходит немного иной способ решения проблемы. Вместо сообщений Hello и всего связанного с ними подойдите к вопросу с другой стороны: выясните сумму всех стоимостей исходящих маршрутов через порты между некорневым и корневым коммутаторами. Повторяя знакомый пример, но с некоторым изменением, рис. 2.8 демонстрирует вычисление корневой стоимости. Обратите внимание, что порт Gi0/1 коммутатора SW3 снова изменил значение стоимости.

Схемы разрешения конфликтов STP при выборе корневого порта

На рисунке представлен основной процесс выбора корневого порта коммутатора SW3 путем добавления стоимости исходящих портов, расположенных по всему маршруту от SW3 до корня (SW1). Здесь также представлено равенство стоимостей, чтобы рассмотреть схему разрешения конфликтов.

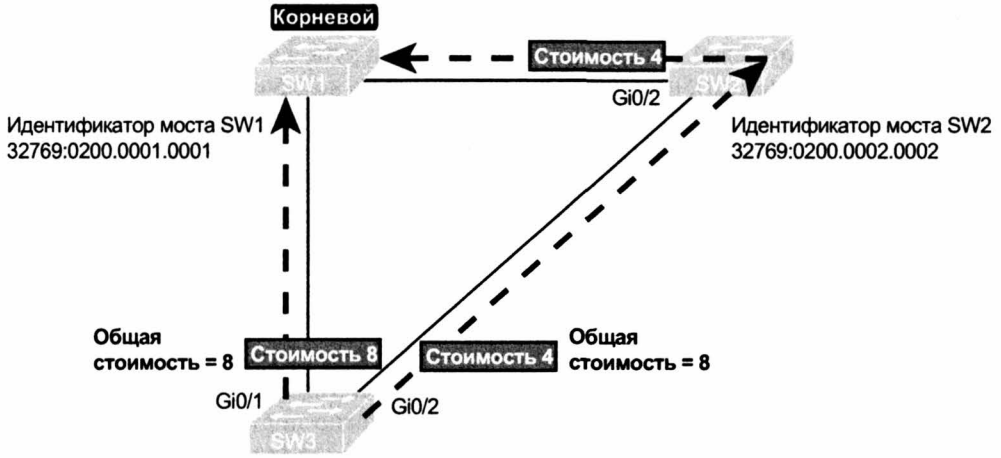


Рис. 2.8. Вычисление корневых стоимостей на коммутаторе SW3 заканчивается равенством

Когда коммутатор выбирает свой корневой порт, сначала он выбирает локальный порт с наименьшей корневой стоимостью. При равенстве стоимостей коммутатор выбирает порт, соединяющий с соседом, обладающим более низким значением BID. Эта схема разрешения конфликтов обычно нарушает равенство, но не всегда. Поэтому упомянем три схемы разрешения конфликтов в порядке их применения коммутатором.

1. Выбор на основании самого низкого идентификатора соседнего моста.
2. Выбор на основании самого низкого приоритета соседнего порта.
3. Выбор на основании самого низкого внутреннего номера соседнего порта.

(Обратите внимание, что коммутатор применяет эти схемы разрешения конфликтов только при равенстве корневых путей.)

Например, на рис. 2.8 показано, что коммутатор SW3 не является корневым и что есть два пути доступа к корневому коммутатору с равными корневыми стоимостями 8. Первая схема разрешения конфликтов по самому низкому BID соседа. Значение BID коммутатора SW1 ниже, чем у SW2, поэтому в данном случае коммутатор SW3 выбирает в качестве RP свой интерфейс G0/1.

Последние две схемы разрешения конфликтов RP применяются, только если два коммутатора соединены друг с другом несколькими каналами связи, как показано на рис. 2.9. В этом случае коммутатор получает сообщения Hello на нескольких портах от того же соседнего коммутатора, поэтому их BID совпадают.

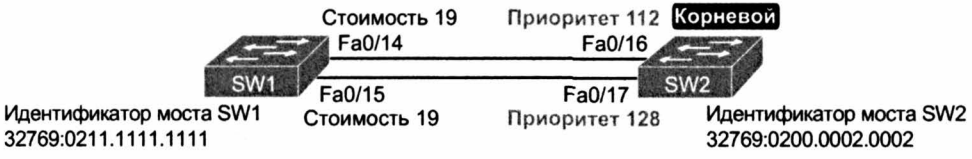


Рис. 2.9. Топология для двух последних схем разрешения конфликтов корневого порта

В данном конкретном случае корневым становится коммутатор SW2, а коммутатор SW1 должен выбрать свой порт RP. Стоимости маршрута через порты коммутатора SW1 равны (по 19 каждый), поэтому корневая стоимость коммутатора SW1 по каждому пути также будет равна 19. Коммутатор SW2 посылает сообщения Hello по каждому каналу связи с коммутатором SW1, поэтому коммутатор SW1 не может нарушить равенство на основании BID соседа, ведь в обоих случаях это BID коммутатора SW2. Поэтому коммутатор SW1 должен обратиться к двум другим схемам разрешения конфликтов.

ВНИМАНИЕ!

В реальной жизни большинство инженеров поместили бы эти два канала связи в канал EtherChannel.

Следующая схема разрешения конфликтов настраиваемая: по приоритету порта соседнего коммутатора каждого интерфейса. Стандартно порты коммутатора Cisco имеют значение 128, при диапазоне значений от 0 до 255 (как обычно, чем ниже, тем лучше). В этом примере сетевой инженер использовал для интерфейса F0/16 коммутатора SW2 команду `spanning-tree vlan 10 port-priority 112`. Теперь коммутатор SW1 знает, что у соседа есть порт с приоритетом 112 на верхнем канале связи и с приоритетом 128 на нижнем, таким образом, коммутатор SW1 использует свой верхний интерфейс (F0/14) как корневой.

Если приоритеты портов равны, что не редко бывает при стандартных значениях, протокол STP полагается на внутренний номер порта соседа. Для идентификации каждого интерфейса коммутаторы Cisco внутреннее используют номера. Некорневой коммутатор находит порт соседа с самым низким внутренним номером (указываемом в сообщениях Hello) и выбирает свой RP на основании самого низкого значения.

Коммутаторы Cisco используют вполне очевидную нумерацию, начиная с самого низкого номера, Fa0/1, затем Fa0/2, Fa0/3 и т.д. Так, на рисунке у интерфейса Fa0/16 коммутатора SW2 более низкий внутренний номер порта, чем у интерфейса Fa0/17; коммутатор SW1 узнал бы эти значения из сообщений Hello и использовал бы как RP свой порт Fa0/14.

Рекомендации по решению проблем корневого порта на экзамене

Экзаменационные вопросы о портах RP могут оказаться простыми, если знать, где искать, и если доступен вывод некоторых ключевых команд. Однако, чем более концептуален вопрос, тем чаще придется вычислять корневую стоимость по каждому пути, сопоставлять их с выводом различных команд `show` и объединять идеи. Вот несколько рекомендаций о том, как подходить к проблемам STP на экзамене.

Ключевая тема

Стратегия поиска корневого порта на некорневых коммутаторах для экзаменационных вопросов

1. Если возможно, просмотрите вывод команд `show spanning-tree` и `show spanning-tree root`. Обе выводят корневой порт и корневую стоимость (см. пример 2.8).
2. Команда `show spanning-tree` выводит стоимость в двух местах: корневая стоимость вначале, в разделе о корневом коммутаторе, и стоимость интерфейса внизу, в разделе интерфейса. Но будьте внимательны, стоимость внизу — это стоимость интерфейса, а не корневая стоимость!

3. Для задач, в которых придется вычислить корневую стоимость коммутатора.
   - Запомните стандартные значения стоимостей: 100 для 10 Мбит/с, 19 для 100 Мбит/с, 4 для 1 Гбит/с и 2 для 10 Гбит/с.
   - Ищите любые случаи команды конфигурации `spanning-tree cost` на интерфейсе, поскольку она переопределяет стандартную стоимость. Не рассчитывайте на то, что используется стандартная стоимость.
   - Если известно, что используется стандартная стоимость, то можно проверить также текущую фактическую скорость. Коммутаторы Cisco выбирают стандартные стоимости STP на основании текущей скорости, а не максимально возможную.

Определение выделенного порта на каждом сегменте LAN

У каждого сегмента сети LAN есть один коммутатор, действующий как *выделенный порт* (Designated Port — DP) этого сегмента. В сегментах, соединяющих коммутатор с устройством, не использующим протокол STP (например, сегменты, соединяющие коммутатор с компьютером или маршрутизатором), всегда побеждает коммутатор, поскольку это единственное устройство, посылающее в канал связи сообщения Hello. Однако каналы связи с двумя коммутаторами требуют немного больше усилий при обнаружении выделенного порта.

Стратегия поиска выделенного порта для экзаменационных вопросов



Этап 1 Для коммутаторов, подключенных к тому же сегменту LAN, выделенным портом (DP) на этом канале связи становится коммутатор с самой низкой стоимостью доступа к корневому коммутатору, содержащейся в сообщениях Hello, посылаемых в канал связи

Этап 2 В случае равенства стоимостей портом DP становится коммутатор с самым низким BID

Рассмотрим, например, рис. 2.10, где представлены корневой коммутатор, порты RP и DP, а также наименьшая для каждого коммутатора стоимость доступа к корневому коммутатору через его порт RP.

Коротко рассмотрим сегменты, соединяющие некорневые коммутаторы.

- **Сегмент SW2–SW4**. Коммутатор SW4 побеждает, поскольку его корневая стоимость, 19, ниже корневой стоимости 20 коммутатора SW2.
- **Сегмент SW2-SW3**. Коммутатор SW3 побеждает, поскольку его корневая стоимость, 19, ниже корневой стоимости 20 коммутатора SW2.
- **Сегмент SW3-SW4**. У коммутаторов SW3 и SW4 равная корневая стоимость, 19. Коммутатор SW3 выигрывает, поскольку значение его BID лучше (ниже).

Интересно, что коммутатор SW2 проигрывает выборы и не становится портом DP на каналах связи с коммутаторами SW3 и SW4, даже при том, что у него лучшее значение BID (самое низкое). Схема разрешения конфликтов DP действительно использует самый низкий BID, но главным критерием является самая низкая корневая стоимость, а корневая стоимость коммутатора SW2 выше, чем у коммутаторов SW3 и SW4.

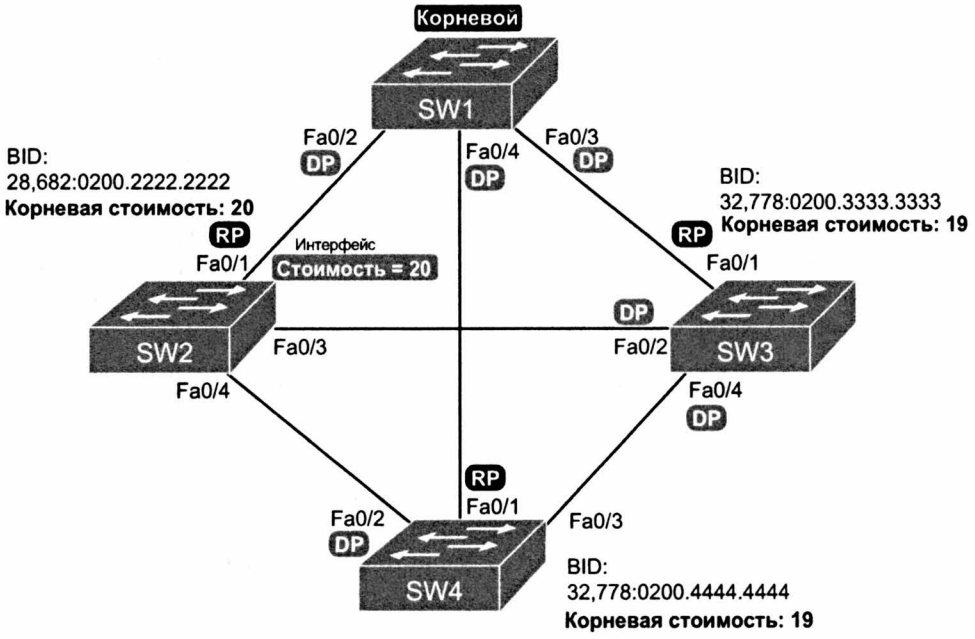


Рис. 2.10. Выборы выделенного порта

ВНИМАНИЕ!

Один коммутатор может быть подключен двумя или более интерфейсами к тому же домену коллизий и при использовании концентраторов конкурировать сам с собой на роль DP. В таких случаях при двух разных портах того же коммутатора (а следовательно, равенстве) порт DP выбирается с использованием тех же двух заключительных схем разрешения конфликтов, что и при выборе порта RP: самый низкий приоритет интерфейса STP, а при равенстве — самый низкий внутренний номер интерфейса.

Рекомендации по решению проблем выделенного порта на экзамене

Подобно экзаменационным вопросам о портах RP, вопросы о портах DP могут оказаться простыми, если знать, где искать, и если доступен вывод некоторых ключевых команд. Однако, чем более концептуален вопрос, тем чаще придется думать о критериях выбора порта DP: сначала корневая стоимость конкурирующих коммутаторов, затем лучший BID, если корневые стоимости равны.

Ниже приведено несколько рекомендаций, которые стоит иметь в виду при решении задач о портах DP. Часть рекомендаций совпадает с таковыми для задач о портах RP, но для завершенности они приведены тоже.

Ключевая тема **Рекомендации по решению задач о выделенных портахх**

1. Если возможно, просмотрите в конце вывода команд `show spanning-tree` список интерфейсов. В столбце `Role` ищите записи `Desg`, идентифицирующие все порты DP.

2. Выясните корневую стоимость коммутатора непосредственно, используя команду `show spanning-tree`. Но будьте внимательны! Стоимость упоминается в двух местах, и только вверху, в разделе о корневом коммутаторе, указана корневая стоимость.
3. Для задач, в которых придется вычислить корневую стоимость коммутатора.
   - Запомните стандартные значения стоимостей: 100 для 10 Мбит/с, 19 для 100 Мбит/с, 4 для 1 Гбит/с и 2 для 10 Гбит/с.
   - Ищите любые случаи команды конфигурации `spanning-tree cost` на интерфейсе, поскольку она переопределяет стандартную стоимость. Не рассчитывайте на то, что используется стандартная стоимость.
   - Если известно, что используется стандартная стоимость, то можно проверить также текущую фактическую скорость. Коммутаторы Cisco выбирают стандартные стоимости STP на основании текущей скорости, а не максимально возможную.

Конвергенция STP

Протокол STP переводит каждый порт RP и DP в состояние перенаправления, а другие порты, не являющиеся ни портом RP, ни DP, блокирует. В таком состоянии они могут оставаться многие дни, недели и месяцы. Но в один прекрасный момент некий коммутатор или канал связи отказывает, или канал связи изменяет скорость (изменяя стоимость STP), или изменяется конфигурация STP. Любое из этих событий может заставить коммутаторы снова запустить свой алгоритм STP, который, в свою очередь, может изменить порты RP и DP.

Причиной конвергенции STP является некое изменение, но не все порты должны изменить свое состояние. Например, перенаправляющий порт, если он все еще должен перенаправить, продолжает перенаправлять данные. Блокированный порт остается блокированным, если так и должно быть. Но когда порт должен изменить свое состояние, это происходит на основании следующих правил.

Действия при конвергенции STP



- У интерфейсов, остающихся в том же состоянии STP, ничего не изменяется.
- У интерфейсов, переходящих из состояния перенаправления в состояние блокировки, изменение происходит немедленно.
- У интерфейсов, переходящих из состояния блокировки в состояние перенаправления, сначала происходит переход в состояние прослушивания, затем в состояние самообучения, причем каждый на протяжении времени, определенного таймером задержки перенаправления (стандартно 15 секунд), и только затем интерфейс переходит в состояние перенаправления.

Поскольку переход из состояния блокировки в состояние перенаправления требует неких дополнительных этапов, следует быть готовым отвечать на концептуальные вопросы о переходе. Для этого можно вернуться к главе 1.

Поиск и устранение неисправностей канала EtherChannel

Поиск и устранение неисправностей каналов EtherChannel может оказаться особенно сложным по нескольким причинам. Во-первых, следует сделать все возможное для правильного выбора конфигурации, поскольку неправильных комбинаций конфигурационных параметров даже больше, чем правильных. Во-вторых, прежде чем коммутатор добавит физический канал связи в группу, должно совпасть множество параметров интерфейса и на физических каналах связи, и на локальном коммутаторе, и на соседнем. В данном разделе рассматриваются оба набора проблем.

Неправильные параметры команды `channel-group`

Ранее, в разделе "Настройка канала EtherChannel", был приведен небольшой набор рабочих параметров команды `channel-group`. Таким образом, для одиночного канала EtherChannel могут быть применены следующие правила.

Ключевая тема **Параметры интерфейса, которые должны совпадать с таковыми у других интерфейсов на том же коммутаторе для их включения в канал EtherChannel**

1. Все команды `channel-group` на локальном коммутаторе для всех физических интерфейсов должны использовать тот же номер группы канала.
2. Номер группы канала может отличаться на соседних коммутаторах.
3. Если используется ключевое слово `on`, оно должно использоваться на соответствующих интерфейсах обоих коммутаторов.
4. Если на одном коммутаторе используется ключевое слово `desirable`, то коммутатор использует протокол PAgP; следовательно, другой коммутатор должен использовать ключевое слово `desirable` или `auto`.
5. Если на одном коммутаторе используется ключевое слово `active`, то коммутатор использует протокол LACP; следовательно, другой коммутатор должен использовать ключевое слово `active` или `passive`.

Эти правила обобщают правильные параметры настройки, но фактически остается еще много возможностей для неправильного выбора. В следующем разделе представлено несколько неправильных, но вполне допустимых коммутаторами конфигураций, хотя они и не позволят создать работоспособный канал EtherChannel. Список сравнивает конфигурацию на одном коммутаторе с другим на основании физической конфигурации интерфейса. Указаны также причины, по которым конфигурация является неправильной.

- На одном коммутаторе использовано ключевое слово `on`, а на другом — ключевое слово `desirable`, `auto`, `active` или `passive`. Ключевое слово `on` не включает ни протокол PAgP, ни протокол LACP, а другие параметры полагаются на работу протокола PAgP или LACP.
- Ключевое слово `auto` использовано на обоих коммутаторах. Оба используют протокол PAgP, но оба ожидают начала переговоров от другого коммутатора.
- Ключевое слово `passive` использовано на обоих коммутаторах. Оба используют протокол LACP, но оба ожидают начала переговоров от другого коммутатора.

- На одном коммутаторе использовано ключевое слово `active`, а на другом — ключевое слово `desirable` или `auto`. Ключевое слово `active` подразумевает протокол LACP, а другие ключевые слова — протокол PAgP.
- На одном коммутаторе использовано ключевое слово `desirable`, а на другом — ключевое слово `active` или `passive`. Ключевое слово `desirable` подразумевает протокол PAgP, а другие ключевые слова — протокол LACP.

Пример 2.9 демонстрирует последний случай в списке. В данном случае два порта (F0/14 и F0/15) коммутатора SW1 были настроены с использованием ключевого слова `desirable`, а соответствующие порты F0/16 и F0/17 коммутатора SW2 — с использованием ключевого слова `active`. Вывод в примере содержит достаточно информации о состоянии, чтобы сделать вывод о причине отказа.

Пример 2.9. Исключение коммутатора как корневого на основании наличия корневого порта

```
SW1# show etherchannel summary
Flags: D - down P - bundled in port-channel
       I - stand-alone s - suspended
       H - Hot-standby (LACP only)
       R - Layer3 S - Layer2
       U - in use f - failed to allocate aggregator

       M - not in use, minimum links not met
       u - unsuitable for bundling
       w - waiting to be aggregated
       d - default port
Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------
1      Po1(SD)         PAgP        Fa0/14(I) Fa0/15(I)

SW1# show interfaces status | include Po|14|15
Port      Name               Status       Vlan       Duplex  Speed  Type
Fa0/14                       connected    301        a-full  a-100  10/100BaseTX
Fa0/15                       connected    301        a-full  a-100  10/100BaseTX
Po1                          notconnect   unassigned   auto  auto
```

Начнем с легенды команды `show etherchannel summary` вверху вывода. Знак *D* означает, что сам канал отключен; знак *S* — что это канал EtherChannel уровня 2; знак *I* — что физический интерфейс работает независимо от интерфейса PortChannel (т.е. автономно). Далее в выводе команды интерфейс PortChannel (Po1) помечен как канал EtherChannel уровня 2 в остановленном состоянии (SD), а интерфейсы F0/14 и F0/15 — как автономные (I).

Как ни странно, проблема в ошибке конфигурации: два физических интерфейса продолжают работать независимо, как будто канала портов не существует. Это демонстрирует последняя команда в примере: хотя интерфейс PortChannel 1 отключен, оба физических интерфейса находятся во включенном состоянии.

ВНИМАНИЕ!

При решении на экзамене задач, связанных с каналом EtherChannel, рекомендуется запоминать не неправильные сочетания параметров, а сконцентрироваться на списке правильных, чтобы затем искать любые различия между конфигурацией, заданной в вопросе, и известными правильными сочетаниями.

Проверка конфигурации перед добавлением интерфейсов в канал EtherChannel

Даже когда все команды `channel-group` настроены правильно, проблемы могут вызвать и другие параметры конфигурации. Данный раздел посвящен этим параметрам конфигурации и их воздействию.

В первую очередь, локальный коммутатор проверяет каждый новый физический интерфейс, настраиваемый как часть канала EtherChannel, сравнивая новый канал с существующими. Параметры нового физического интерфейса должны совпадать с таковыми у существующих каналов связи; в противном случае коммутатор не добавит новый канал связи в список рабочих интерфейсов канала EtherChannel. Таким образом, физический интерфейс остается настроенным как часть канала портов, но в составе группы не используется, а зачастую переводится в некое нерабочее состояние.

Ниже приведен список элементов, проверяемых на коммутаторе.

- Скорость.
- Дуплекс.
- Состояние доступа или магистрали (все каналы должны быть в одинаковом состоянии).
- Если это порт доступа, то проверяется сеть VLAN.
- Если это порт магистрального канала, список разрешенных сетей VLAN (согласно команде `switchport trunk allowed`).
- Если это порт магистрального канала, то проверяется собственная сеть VLAN.
- Параметры интерфейса STP.

Кроме того, коммутаторы проверяют параметры на соседнем коммутаторе. Для этого они используют протокол PAgP или LACP (если он уже не используется) или, при настройке вручную, протокол обнаружения устройств Cisco (CDP). У соседа должны совпадать все параметры списка, кроме параметров STP.

Например, коммутаторы SW1 и SW2 снова используют два канала связи в одном канале EtherChannel. Прежде чем настроить канал EtherChannel, на интерфейсе F0/15 коммутатора SW1 была задана стоимость маршрута через порт STP, отличная от интерфейса F0/14. Пример 2.10 продолжает эту последовательность, но уже после ввода правильных команд `channel-group`, когда коммутатор решает, использовать ли интерфейс F0/14 и F0/15 в этом канале EtherChannel.

Пример 2.10. Отказ локальных интерфейсов в канале EtherChannel из-за несовпадения стоимостей STP

```
*Mar 1 23:18:56.132: %PM-4-ERR_DISABLE: channel-misconfig (STP) error de-
tected on Po1, putting Fa0/14 in err-disable state
*Mar 1 23:18:56.132: %PM-4-ERR_DISABLE: channel-misconfig (STP) error de-
```

```
tected on Po1, putting Fa0/15 in err-disable state
*Mar 1 23:18:56.132: %PM-4-ERR_DISABLE: channel-misconfig (STP) error de-
tected on Po1, putting Po1 in err-disable state
*Mar 1 23:18:58.120: %LINK-3-UPDOWN: Interface FastEthernet0/14,
changed state to down
*Mar 1 23:18:58.137: %LINK-3-UPDOWN: Interface Port-channel1,
changed state to down
*Mar 1 23:18:58.137: %LINK-3-UPDOWN: Interface FastEthernet0/15,
changed state to down

SW1# show etherchannel summary
Flags: D - down P - bundled in port-channel
       I - stand-alone s - suspended
       H - Hot-standby (LACP only)
       R - Layer3 S - Layer2
       U - in use f - failed to allocate aggregator

       M - not in use, minimum links not met
       u - unsuitable for bundling
       w - waiting to be aggregated
       d - default port


Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------
1      Po1(SD)           -          Fa0/14(D) Fa0/15(D)
```

Сообщение вверху примера, в частности, сообщает, что коммутатор делает при проверке совпадения параметров интерфейса. В данном случае коммутатор SW1 обнаруживает различие в стоимостях STP. Коммутатор SW1 не использует ни порт F0/14, ни порт F0/15, а переводит их в состояние блокировки из-за ошибки. Коммутатор переводит также в состояние блокировки из-за ошибки интерфейс PortChannel. В результате ни канал портов, ни физические интерфейсы работать не будут.

Для решения этой проблемы следует перенастроить физические интерфейсы так, чтобы использовать одинаковые параметры STP. Кроме того, для выхода из состояния блокировки из-за ошибки интерфейс PortChannel и физические интерфейсы должны быть отключены (`shutdown`), а затем снова включены (`no shutdown`). (Обратите внимание, что когда коммутатор применяет команды `shutdown` и `no shutdown` на канале портов, он применяет те же команды к физическим интерфейсам; поэтому достаточно ввести команды `shutdown`/`no shutdown` только на интерфейсе PortChannel.)

Обзор

Резюме

- Хотя протокол STP работает без настройки, большинство сетей среднего и крупного размера извлекут выгоду из некоторой настройки конфигурации STP.
- Коммутаторы Cisco LAN позволяют использовать один из трех режимов протокола STP.
- Стандарт Per-VLAN Spanning Tree Plus (PVST+, или просто PVST) позволяет создать индивидуальный экземпляр STP для каждой сети VLAN.
- Поле приоритета BID можно настраивать, чтобы инженер имел возможность контролировать выбор корневого моста.
- Настройка стоимостей маршрута через порт STP позволяет инженеру контролировать выбор корневого порта.
- Переговоры между коммутаторами о создании канала EtherChannel обеспечивают два разных протокола: PAgP и LACP.
- Если данный физический канал связи подходит, он добавляется к каналу EtherChannel и используется.
- Прежде чем приступать к сложным вопросам по протоколу STP, следует выработать хорошую стратегию поиска и устранения неисправностей.

Контрольные вопросы

Ответьте на эти вопросы. Ответы можно найти на последней странице главы. Полное объяснение ответов приведено в приложении B на веб-сайте.

1. Какие из следующих команд, применяемых в коммутаторах 2960, позволяют изменить значение идентификатора моста? (Выберите дав ответа.)

   А) `spanning-tree bridge-id` *значение*.

   Б) `spanning-tree vlan` *номер_vlan* `root {primary | secondary}`.

   В) `spanning-tree vlan` *номер_vlan* `priority` *значение*.

   Г) `set spanning-tree priority` *значение*.

2. Рассмотрите следующий фрагмент из результатов выполнения команды `show spanning-tree` на коммутаторе Cisco:

```
Bridge ID Priority 32771 (priority 32768 sys-id-ext 3)
    Address 0019.e86a.6f80
```

   Какой из следующих ответов является правильным по отношению к коммутатору, на котором был получен этот вывод команды?

   А) Эти сведения относятся к экземпляру STP для VLAN 1.

   Б) Эти сведения относятся к экземпляру STP для VLAN 3.

   В) Вывод команды подтверждает, что этот коммутатор, скорее всего, не может быть корневым.

   Г) Вывод команды подтверждает, что этот коммутатор в настоящее время является корневым.

3. Интерфейс G0/1 коммутатора поддерживает магистральный канал с сетями VLAN 1-10, он автоматически договорился о скорости 100 Мбит/с. Все настройки протокола STP у коммутатора в настоящее время стандартные. Какое из следующих действий приведет к использованию на коммутаторе стоимости STP 19 для интерфейса в VLAN 3? (Выберите два ответа).

   А) `spanning-tree cost 19`

   Б) `spanning-tree port-cost 19`.

   В) `spanning-tree vlan 3 port-cost 19`.

   Г) Никаких действий выполнять не нужно.

4. Инженер настроил коммутатор так, чтобы поместить интерфейсы G0/1 и G0/2 в тот же канал EtherChannel. Какие из следующих терминов используются в командах конфигурации?

   А) EtherChannel.

   Б) PortChannel.

   В) Ethernet-Channel.

   Г) Channel-group.

5. Коммутатор SW3 получает только два пакета Hello BPDU, и оба они поступают из одного и того же корневого коммутатора, причем получение происходит через два интерфейса, отображаемых в выводе команды следующим образом:

```
SW3 #show interfaces status

Port  Name Status  Vlan Duplex Speed Type
Fa0/13   connected 1  a-half a-100 10/100BaseTX
Gi0/1    connected 1  a-full a-1000 1000BaseTX
```

   В коммутаторе SW3 отсутствуют какие-либо команды конфигурации, относящиеся к протоколу STP. Для пакета Hello, полученного через интерфейс Fa0/13, указана стоимость 10, а для пакета Hello, полученного через интерфейс Gi0/1, — стоимость 20. Какое из следующих утверждений о применении протокола STP в коммутаторе SW3 является истинным?

   А) Коммутатор SW3 выберет Fa0/13 в качестве своего корневого порта.

   Б) Коммутатор SW3 выберет Gi0/1 в качестве своего корневого порта.

   В) Порт Fa0/13 коммутатора SW3 станет выделенным.

   Г) Порт Gi0/1 коммутатора SW3 станет выделенным.

6. Какие из следующих команд выводят корневую стоимость некорневого коммутатора? (Выберите два ответа.)

   А) `show spanning-tree root`.

   Б) `show spanning-tree root-cost`.

   В) `show spanning-tree bridge`.

   Г) `show spanning- tree`.

Ключевые темы

Повторите все ключевые темы данной главы, отмеченные пиктограммой "Ключевая тема". Ключевые темы и соответствующие им страницы перечислены в табл. 2.2.

Таблица 2.2. Ключевые темы главы 2

Элемент	Описание	Страница
Рис. 2.1	Типичный выбор конфигурации: корневым стоит сделать коммутатор распределения	86
Рис. 2.2	Балансировка нагрузки при помощи протокола PVST+	88
Рис. 2.3	Расширение системного идентификатора STP	89
Табл. 2.1	Стандартные значения STP и возможности для настройки	90
Список	Две ветви логики выбора нового базового приоритета STP командой spanning-tree root primary	96
Список	Этапы настройки канала EtherChannel вручную	99
Список	Стратегия поиска корневого коммутатора для экзаменационных вопросов	103
Список	Стратегия поиска корневого порта на некорневых коммутаторах для экзаменационных вопросов	106
Список	Стратегия поиска выделенного порта для экзаменационных вопросов	107
Список	Рекомендации по решению задач о выделенных портах	108
Список	Действия при конвергенции STP	109
Список	Параметры интерфейса, которые должны совпадать с таковыми у других интерфейсов на том же коммутаторе для их включения в канал EtherChannel	110

Ключевые термины

После первого прочтения главы попытайтесь дать определения следующим ключевым терминам. Но не расстраивайтесь, если не все получится сразу, в главе 22 описано, как использовать эти термины на завершающем этапе подготовки к экзамену.

связующее дерево с использованием сетей VLAN плюс (Per-VLAN Spanning Tree Plus — PVST+), быстрый PVST+ (Rapid PVST+), расширение системного идентификатора (system ID extension), протокол объединения портов (Port Aggregation Protocol — PAgP), протокол управления объединением каналов (Link Aggregation Control Protocol — LACP), интерфейс PortChannel (PortChannel), команда `channel-group`

Таблицы команд

Хоть и не обязательно заучивать информацию из таблиц данного раздела, ниже приведен список команд конфигурации и пользовательских команд, приведенных в главе. Фактически команды стоит запомнить, чтобы лучше понять содержимое главы и выполнить задания по подготовке к экзамену. Чтобы проверить, насколько хорошо вы запомнили команды, закройте левую колонку таблицы листом бумаги, читайте описания справа и пытайтесь вспомнить команду.

Таблица 2.3. Конфигурационные команды главы 2

Команда	Описание
`spanning-tree mode { pvst | rapid-pvst | mst }`	Глобальная команда конфигурации, устанавливающая режим STP
`spanning-tree vlan` *`номер_vlan`* `root primary`	Глобальная команда конфигурации, позволяющая назначить конкретный коммутатор для использования в качестве корневого. Приоритет этого коммутатора изменяется в меньшую сторону так, что становится либо равным 24 576, либо на 4096 меньшим по сравнению с приоритетом текущего корневого моста ко времени выполнения этой команды
`spanning-tree vlan` *`номер_vlan`* `root secondary`	Глобальная команда конфигурации, которая задает базовый приоритет протокола STP для рассматриваемого коммутатора, равный 28 672
`spanning-tree [vlan` *`идентификатор_vlan`*`] {priority` *`приоритет`*`}`	Глобальная команда конфигурации, которая позволяет изменить приоритет моста этого коммутатора для указанной сети VLAN
`spanning-tree [vlan` *`номер_vlan`*`] cost` *`стоимость`*	Команда интерфейса, позволяющая задать в конфигурации протокола STP указанное значение стоимости
`spanning-tree [vlan` *`номер_vlan`*`] port-priority` *`приоритет`*	Подкоманда интерфейса, изменяющая приоритет порта STP на заданной VLAN (от 0 до 240 с шагом 16)
`channel-group` *`номер`* `mode {auto | desirable | active | passive | on}`	Подкоманда интерфейса, включающая использование канала EtherChannel на интерфейсе
`spanning-tree portfast`	Подкоманда интерфейса, включающая использование режима PortFast на интерфейсе
`spanning-tree bpduguard enable`	Подкоманда интерфейса, позволяющая включить технологию BPDU Guard на интерфейсе
`spanning-tree portfast default`	Глобальная команда, изменяющая на интерфейсах доступа коммутатора стандартное для PortFast значение `disabled` на `enabled`
`spanning-tree portfast bpduguard default`	Глобальная команда, изменяющая на интерфейсах доступа коммутатора стандартное для службы BPDU Guard значение `disabled` на `enabled`
`spanning-tree portfast disable`	Подкоманда интерфейса, отключающая PortFast на интерфейсе
`spanning-tree bpduguard disable`	Подкоманда интерфейса, отключающая службу BPDU Guard на интерфейсе

Таблица 2.4. Команды EXEC главы 2

Команда	Описание
`show spanning-tree`	Получение подробных сведений о состоянии протокола STP на коммутаторе, включая состояние каждого порта
`show spanning-tree` *интерфейс идентификатор_интерфейса*	Получение информации протокола STP только для указанного порта
`show spanning-tree vlan` *идентификатор_vlan*	Получение информации протокола STP для указанной сети VLAN
`show spanning-tree [vlan` *идентификатор_vlan*`] root`	Получение информации о корневом коммутаторе каждой сети VLAN или только указанной сети VLAN
`show spanning-tree [vlan` *идентификатор_vlan*`] bridge`	Получение информации протокола STP о локальном коммутаторе для каждой сети VLAN или только для указанной сети VLAN
`debug spanning-tree events`	Переключение коммутатора в режим формирования информационных сообщений об изменениях в топологии STP
`show spanning-tree interface` *номер_типа* `portfast`	Выводит краткое сообщение о состоянии PortFast на заданном интерфейсе
`show etherchannel [`*номер_группы_каналов*`] {brief | detail | port | port-channel | summary}`	Получение информации о состоянии каналов EtherChannel в указанном коммутаторе

Ответы на контрольные вопросы:

1 Б и В. 2 Б. 3 А и Г. 4 Г. 5 Б. 6 А и Г.

ГЛАВА 3

Поиск и устранение неисправностей коммутации LAN

Цель этой главы, а также нескольких других глав и разделов по поиску и устранению неисправностей — помочь выработать навыки поиска и устранения неисправностей, необходимые для быстрого и уверенного ответа на определенные типы экзаменационных вопросов. В то же время благодаря этой главе вы должны улучшить подготовку в решении реальных сетевых проблем.

Главы и разделы по поиску и устранению неисправностей этой книги имеют несколько иную основную задачу, чем другие материалы. Проще говоря, они сосредоточены на конкретных средствах и фактах из области технологий поиска и устранения неисправностей и охватывают более широкий круг понятий. В частности, в главах о поиске неисправностей сетевая проблематика рассматривается в более широком аспекте, а основное внимание уделяется взаимодействию отдельных сетевых компонентов (считается, что читатель уже знает все необходимое о работе самих компонентов).

Одна из задач этой главы вполне очевидна, а другая — нет. В первую очередь обсуждается поиск и устранение неисправностей локальных сетей. Не столь очевидно то, что эта глава содержит также обзор большинства тем по LAN Ethernet этой книги. Обзор некоторых из тем этой главы приведен в главе 1.

Эта большая глава разделена на три раздела.

- Обобщенные методологии поиска неисправностей.
- Поиск неисправностей коммутации на уровне данных локальной сети.
- Примеры и упражнения на поиск и устранение неисправностей.

С учетом объема данной главы считайте каждый из трех главных разделов отдельной темой для чтения приблизительно по 10, 20 и 20 страниц соответственно. Все три раздела взаимосвязаны, поэтому они включены в одну главу, но второй раздел содержит основные темы по поиску и устранению неисправностей коммутаторов LAN. В первом разделе определены некоторые термины поиска и устранения неисправностей, а заключительный раздел — это, по существу, два длинных примера с большим количеством команд `show`. Эти довольно длинные примеры должны помочь выработать некоторые навыки и запомнить значение команд `show` на коммутаторах Cisco.

В этой главе рассматриваются следующие экзаменационные темы
Поиск и устранение неисправностей
Поиск и устранение наиболее распространенных проблем сети
Поиск и устранение проблем маршрутизации interVLAN
Собственная сеть VLAN
Состояние режима порта магистрального канала

Основные темы

Обобщенные методологии поиска неисправностей

ВНИМАНИЕ!

В данном разделе приведены общие стратегии и методы поиска неисправностей для изучения основного подхода к рассматриваемой теме. Но эти процессы не рассматриваются непосредственно на экзаменах, поэтому подробно их изучать или запоминать нет необходимости. Вместо этого описанные здесь процессы должны помочь выработать такой подход к решению задач, рассматриваемых на экзаменах, чтобы можно было отвечать на вопросы немного быстрее и чувствовать себя гораздо более уверенным.

Каждый, кто сталкивается с необходимостью устранить ту или иную сетевую проблему, вынужден использовать определенную методологию поиска неисправностей — формальную или неформальную. При этом одни начинают с проверки состояния физической кабельной системы и интерфейсов во всех физических каналах для определения того, что могло бы стать причиной нарушения в работе. Другие специалисты предпочитают прежде всего провести эхо-тестирование всех устройств, чтобы больше узнать о первоисточнике проблемы, а затем углубиться в изучение деталей. Есть и такие специалисты, которые пытаются просто выполнить все проверки, которые подсказывает им интуиция, пока не сложится общее понимание причин возникновения проблемы. Ни один из этих подходов, по сути, не является правильным или неправильным; автор испытал не только указанные подходы, но и многие другие, и в каждом случае так или иначе добивался успеха.

В целом следует отметить, что большинство специалистов постепенно вырабатывают наиболее приемлемые для себя навыки и стили поиска неисправностей на основе собственного опыта и с учетом своих сильных и слабых сторон, но существуют более систематизированные методологии поиска неисправностей, способные помочь любому, кто занимается устранением нарушений в работе, добиться большего успеха. В следующих разделах описана одна из таких систематизированных методологий поиска неисправностей, которая должна помочь лучше подготовиться к решению задач по устранению нарушений в работе сети на экзаменах CCNA.

Эту методологию поиска неисправностей можно разделить на три основных направления, которые обычно реализуются в указанной ниже последовательности.

- **Анализ и прогнозирование нормальной работы.** Данный этап отвечает на вопрос: что должно происходить в данной сети? Описание и прогнозирование деталей того, что должно происходить в процессе исправного функционирования сети, на основании документации, сведений о конфигурации, а также вывода команд `show` и `debug`.
- **Локализация проблемы.** Этот этап отвечает на тот же вопрос: что именно не работает? Если причиной нарушения в работе является определенная проблема, то для поиска компонентов, не функционирующих должным образом, используются документация, сведения о конфигурации и вывод команд `show` и `debug`.

- **Анализ первопричин.** Этот этап отвечает на вопрос: что можно исправить для решения проблемы? Выявление основных причин возникновения проблем, обнаруженных на предыдущем этапе, особенно тех, которые указывают на конкретные действия, позволяющие устранить текущие проблемы.

Выполнение этих трех этапов должно привести не только к пониманию инженером признаков нарушения в работе, но и к обнаружению способа устранения проблемы. В данной главе рассматриваются некоторые рекомендации по осуществлению каждого из указанных этапов в процессе поиска неисправностей.

Анализ и прогнозирование нормальной работы сети

Назначение любой сети — доставка данных от одного устройства конечного пользователя к другому. Чтобы успешно проводить анализ сети, инженер должен знать, какие действия осуществляются устройствами, следующими друг за другом, в ходе перенаправления данных на очередное устройство. Зная о том, что должно происходить в каждом устройстве, инженер может описать весь поток данных.

Под термином *уровень данных* (data plane) подразумевают все действия, выполняемые сетевым устройством для перенаправления отдельного фрейма или пакета. Чтобы перенаправить каждый фрейм или пакет, устройство применяет заложенные в нем логику уровня данных и процессы к фрейму или пакету. Например, после получения сетевым коммутатором фрейма через интерфейс, относящийся к сети VLAN 3, коммутатор принимает решение о перенаправлении на основе записей с данными сети VLAN 3 в таблице MAC-адресов и перенаправляет пакет. Все осуществляемые при этом действия составляют часть процесса обработки на уровне данных коммутатора.

Термином *уровень управления* (control plane) обозначают вспомогательные процессы, не воздействующие непосредственно на перенаправление отдельных фреймов или пакетов. Примерами процессов уровня управления является протокол распределенного связующего дерева (STP) и любой протокол маршрутизации IP.

Кроме того, некоторые процессы уровня управления даже косвенно не влияют на устройство перенаправления данных. Например, для подтверждения точности сетевой документации может применяться *протокол обнаружения устройств компании Cisco* (Cisco Discovery Protocol — CDP), но включение или выключение средств протокола CDP никак не влияет на процессы перенаправления уровня данных.

Чтобы иметь возможность прогнозировать ожидаемое функционирование сети или привести подробные сведения о том, как действует в данный момент правильно функционирующая сеть, следует начать с рассмотрения уровня управления или уровня данных. В настоящей главе в первую очередь рассматривается уровень данных, но в реальной обстановке может быть выбран тот или иной уровень с учетом того, какие признаки неисправности наблюдаются в настоящее время.

Анализ уровня данных

При поиске неисправностей на уровне данных последовательно рассматривается каждое устройство в предполагаемом пути перенаправления данных. Анализ начинается с хоста, на котором создаются исходные данные. Хост отправляет данные на другое устройство, которое передает данные еще на одно устройство, и так далее до достижения данными хоста назначения.

Процесс поиска неисправности уровня данных должен учитывать оба направления передачи данных между двумя устройствами. Когда одно устройство отправляет данные, получающий хост обычно передает своего рода ответ. Так, причиной проблемы "не могу связаться с сервером Server1" может быть проблема с пакетами, передаваемыми пользователями с сервера Server1. Однако причиной проблемы может быть и проблема с покидающими сервер Server1 пакетами, возвращаемыми пользователю. Таким образом, чтобы полностью понять происходящее при коммуникации, следует также анализировать и обратный процесс.

Во многих случаях о причинах возникновения конкретной проблемы можно судить непосредственно по ее признакам, а если это не удается сделать, то поиск причин нарушений в работе на уровне данных следует начинать с анализа работы уровня данных на уровне 3. Если анализ начинается с уровня 3, то появляется возможность следить за основными этапами передачи и получения данных, проходящих между двумя хостами. После этого можно более подробно изучить каждый этап перенаправления на уровне 3, рассматривая дополнительные сведения о нижележащих уровнях 1 и 2. В качестве примера на рис. 3.1 показаны шесть основных этапов перенаправления IP (forwarding) трафика (на уровне данных) в небольшой сети.

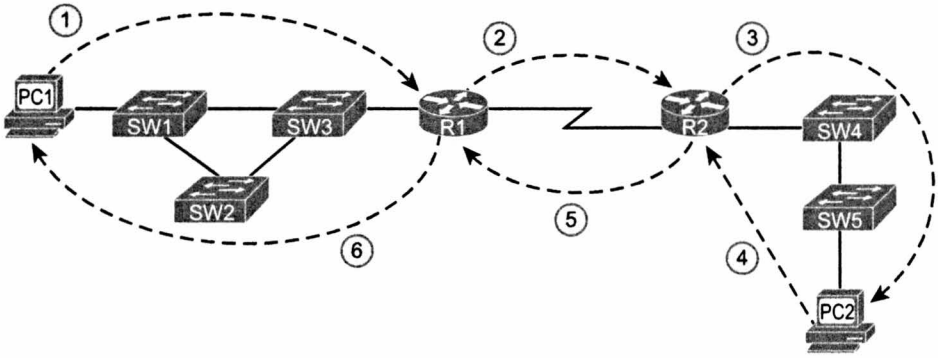


Рис. 3.1. Основные этапы перенаправления IP в рассматриваемом примере

Чтобы попытаться понять, в чем состоит ожидаемое поведение уровня 3 в этом случае, необходимо представить себе, как движутся пакеты в сети на рис. 3.1 слева направо, а затем — как в ответ им передаются пакеты справа налево. Используя указанные на рис. 3.1 шесть этапов, можно провести следующий анализ.

Этап 1 Узнать IP-адрес и маску компьютера PC1, IP-адрес и маску компьютера PC2, а также определить, какие действия выполняются в компьютере PC1 для выявления того, что компьютер PC2 находится в другой подсети. Получив указанные сведения, компьютер PC1 вынужден отправить пакет на стандартный шлюз (R1)

Этап 2 Рассмотреть, какие действия по перенаправлению выполняются на маршрутизаторе R1 для согласования IP-адреса получателя пакета с таблицей маршрутизации маршрутизатора R1, исходя из предположения, что после этого маршрутизатор R1 примет решение по отправке пакета на маршрутизатор R2

Этап 3 Применительно к маршрутизатору R2 рассмотреть те же действия по согласованию с таблицей маршрутизации, которые использовались маршрутизатором R1 на предыдущем этапе, применяя таблицу маршрутизации маршрутизатора R2.

Соответствующая запись должна показывать маршрут для устройства, подключенного к маршрутизатору R2

Этап 4 Этот этап относится к ответному пакету компьютера PC2, и при его осуществлении используется та же основная логика, что и на этапе 1. Происходит сравнение IP-адреса и маски компьютера PC2 с IP-адресом и маской компьютера PC1, а это позволяет обнаружить, что компьютеры находятся в разных подсетях. В результате этого компьютер PC2 должен передать пакет на свой стандартный шлюз, R2

Этап 5 Рассмотреть действия, выполняемые маршрутизатором R2 по перенаправлению пакетов, в которых в качестве IP-адреса назначения указан компьютер PC1, из чего следует, что применение согласованного маршрута должно привести к отправке маршрутизатором R2 полученных пакетов маршрутизатору R1

Этап 6 Конечный шаг маршрутизации, осуществляемый маршрутизатором R1, должен показать, что пакет, в котором в качестве IP-адреса назначения указан компьютер PC1, должен быть передан маршрутизатором R1 на это устройство, которое обозначено как подключенное; в результате этого маршрутизатор R1 передает пакет непосредственно по MAC-адресу компьютера PC1

Полностью разобравшись, в чем состоит ожидаемое поведение на каждом этапе, осуществляемом на уровне 3, можно перейти к более подробному изучению действий на уровне 2. Соблюдая такую же последовательность этапов, можно более внимательно рассмотреть этап 1 маршрутизации на уровне 3, который показан на рис. 3.1 (передача пакета компьютером PC1 маршрутизатору R1), и изучить подробные сведения об отправке компьютером PC1 фрейма на уровнях 1 и 2 для его доставки на маршрутизатор R1 (рис. 3.2).

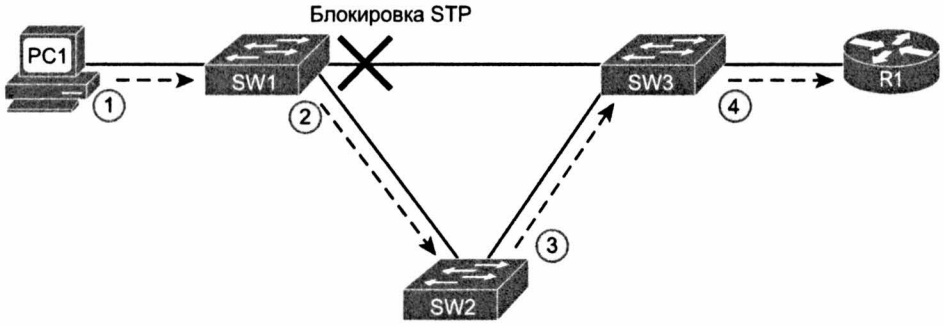


Рис. 3.2. Основные этапы в примере пересылки данных в процессе коммутации локальной сети

Для такого анализа необходимо было бы снова начать с компьютера PC1, но на этот раз рассматривать не фреймы и пакеты, а заголовки и концевики Ethernet, в частности MAC-адреса получателя и отправителя. После этого на этапе 2 необходимо было бы рассмотреть пересылку, осуществляемую коммутатором SW1, который сравнивает MAC-адрес получателя фрейма с таблицей MAC-адресов SW1 и определяет, что с коммутатора SW1 фрейм должен быть перенаправлен коммутатору SW2. На этапах 3 и 4 соответственно должны были бы повториться действия этапа 2, но пересылка происходит с коммутатора SW2 на коммутатор SW3.

Анализ уровня управления

Многие процессы уровня управления непосредственно затрагивают тот или иной процесс уровня данных. Например, маршрутизация IP не может осуществляться, если не выработаны соответствующие маршруты IP, поэтому обычно в маршрутизаторах для изучения этих маршрутов используется динамический протокол маршрутизации (протокол уровня управления). Протоколы маршрутизации отчасти рассматриваются как протоколы уровня управления, поскольку работу, проделанную с помощью такого протокола, не приходится выполнять снова и снова для каждого фрейма или пакета.

Хотя изучение процессов уровня данных позволяет тем или иным образом наметить универсальный процесс устранения нарушений в работе, основанный на изучении действий по пересылке данных, осуществляемых в каждом устройстве, процессы уровня управления слишком разнообразны, поэтому возможность предложить для них подобный обобщенный процесс поиска неисправностей отсутствует. Однако имеет смысл рассмотреть конкретный ряд этапов процедуры поиска неисправностей для каждого конкретного протокола уровня управления. В качестве примера отметим, что в главе 2 было показано, как подойти к устранению некоторых типов нарушений в работе протокола VTP.

Прогнозирование нормальной работы: сводные данные о выполняемом процессе

Для ответа на некоторые вопросы на экзаменах буквально необходимо проанализировать и спрогнозировать состояние нормальной работы сети. А в других случаях прогнозирование нормального поведения сети становится лишь первым шагом к локализации и устранению проблемы. Но в любой ситуации, если в самом вопросе отсутствуют конкретные подсказки о том, на изучении какой части сети следует сосредоточиться в поисках решения, можно воспользоваться следующей процедурой.

Этап 1 Изучить уровень данных, как описано ниже.

A. Определить основные действия, осуществляемые на уровне 3 по передаче данных в обоих направлениях, включая то, в какой стандартный маршрутизатор направляет трафик хост-отправитель, какие маршрутизаторы используются в пути для передачи данных и какой маршрутизатор становится последним на маршруте к хосту получателя.

B. Для каждой сети уровня 2 между хостом и маршрутизатором или между двумя маршрутизаторами проанализировать действия по пересылке данных, осуществляемые применительно к каждому устройству

Этап 2 Изучить уровень управления, как описано ниже.

A. Определить наиболее важные и используемые протоколы уровня управления, от которых полностью зависит осуществление процесса перенаправления.

B. Изучить каждый важный протокол уровня управления с точки зрения того, правильно ли он действует; подробности такого изучения зависят от конкретного протокола.

C. Отложить анализ тех протоколов уровня управления, от которых не зависит правильная организация работы уровня данных, до того времени, пока не будет явно обнаружена необходимость изучить работу того или иного протокола для поиска ответа на поставленный вопрос (в качестве примера можно указать протокол CDP)

Локализация проблемы

Процесс поиска и устранения неисправностей подразумевает нахождение первопричины проблемы и ее исправление. Процесс поиска первопричины начинается с локализации проблемы. Локализация проблемы переводит нас от общих представлений о проблеме к конкретным представлениям о ее причинах следующим образом.

Перед локализацией проблемы. Причина неизвестна, есть лишь некие общие признаки неисправности.

После локализации проблемы. Понятно, что именно не работает, известно, как это должно работать и какое устройства должно функционировать иначе.

В качестве примера еще раз рассмотрим рис. 3.1, демонстрирующий доставку пакета в прямом направлении, от компьютера PC1 к компьютеру PC2, за шесть этапов маршрутизации. Но в данном случае вместо нормального протекания процесса обнаруживается, что пакет поступает в маршрутизатор R2, но не передается компьютеру PC2. Поэтому имеет смысл обратить более пристальное внимание на третий этап процесса маршрутизации, между маршрутизатором R2 и компьютером PC2, чтобы еще более локализовать проблему. Процесс сужения пространства, где может находиться причина проблемы, называется *локализацией проблемы* (problem isolation).

Иными словами, проведена локализация причин возникновения нарушений в работе и обнаружен этап процесса пересылки трафика IP (см. рис. 3.1), на котором возникают проблемы, поэтому появляется возможность сосредоточиться на изучении конкретной ситуации и определить именно те компоненты, функционирование которых требует вмешательства. Например, если пакет поступает в маршрутизатор R2, но не передается на компьютер PC2, то проблема может заключаться в том, что нарушена работа маршрутизатора R2, коммутатора SW4, коммутатора SW5, компьютера PC2, есть проблемы в кабельной системе или, возможно, неисправно какое-либо устройство, не указанное в сетевой документации из-за случайного упущения.

Для дальнейшей локализации причин проблемы обычно требуется рассматривать функционирование почти всех уровней модели OSI, а также выполнение устройствами функций на уровне управления и на уровне данных. Продолжая рассмотрение того же примера сценария возникновения проблемы, отметим, что маршрутизатор R2 может перенаправлять пакеты на компьютер PC2 лишь в том случае, если в его таблицах имеется MAC-адрес компьютера PC2, полученный с помощью протокола ARP (Address Resolution Protocol — *протокол преобразования адресов*). Если обнаруживается, что в таблицах маршрутизатора R2 отсутствует запись ARP, относящаяся к компьютеру PC2, это может стать основанием для вывода, что имеет место проблема, связанная с нарушением работы протокола IP.

В действительности первопричина могла бы быть любой из следующих:

- обрыв магистрального канала между коммутаторами SW4 и SW5;
- неисправность кабеля между коммутатором SW5 и компьютером PC2;
- конфигурация IPv4 на компьютере PC2 не имеет правильного IP-адреса;
- сервер DHCP, протокола динамического конфигурирования хоста, мог бы быть настроен неправильно, поэтому компьютер PC2 не изучал адрес DHCP.

Локализация проблемы начинается с общего представления, становясь впоследствии все более конкретной. В данном примере проблема была изолирована до точ-

ки, где стало понятно, что запрос ARP маршрутизатора R2 к компьютеру PC2 потерпел неудачу, но, как уже упоминалось, конкретная причина проблемы доставки запросов ARP еще не была определена.

Иногда подсказка, с помощью которой можно определить, с чего начать изучение проблемы, находится в самом экзаменационном вопросе; в противном случае следует руководствоваться описанным ниже процессом, который воплощает в себе удобную общую стратегию локализации проблемы.

Этап 1 Начните с исследования уровня данных на уровне 3 (пересылка данных IP), сравнивая полученные результаты с ожидаемым нормальным поведением до тех пор, пока не обнаружится первый важный этап маршрутизации, на котором возникает нарушение

Этап 2 Проведите дальнейшую локализацию проблемы, чтобы ограничить потенциальный участок сети, подлежащий рассмотрению, до минимально возможного количества компонентов, как описано ниже.

A. Исследуйте функционирование сети на всех уровнях (и особенно на уровнях 1–3).

B. Исследуйте функционирование сети на уровне управления и уровне данных

В процессе решения экзаменационных задач следует помнить, что оценки выставляются с учетом конечных результатов, и при этом не учитывается, насколько подходящим был метод поиска неисправностей, поэтому достаточно найти ответ любым возможным путем, даже если для этого придется принять дополнительные предположения в контексте самого вопроса. Например, на этапе 2 предложенного выше процесса необходимо сосредоточиться на изучении функционирования уровней 1–3, причем эта рекомендация исходит из того факта, что на экзаменах CCNA основное внимание уделяется трем указанным уровням. Но сказанное не означает, что необходимо строго придерживаться рекомендуемого процесса, поэтому всегда следует использовать всю информацию, представленную в вопросе, для максимально быстрого поиска решения.

Анализ основной причины

Этап анализа основной причины является последним из трех рекомендуемых этапов процесса поиска неисправностей и предназначен для обнаружения конкретных устройств и функций, которые требуют внесения исправлений. Только что устраненная причина проблемы в сети решает, по крайней мере, часть первоначальной проблемы.

Обнаружить основную причину чрезвычайно важно, поскольку по определению именно с ней связано конкретное решение, позволяющее устранить нарушения в работе, тогда как все прочие проблемы, обнаруженные в процессе локализации неисправностей, такой особенностью не обладают. В качестве примера продолжим рассмотрение той же проблемы, обусловленной отсутствием возможности передачи пакетов из маршрутизатора R2 на компьютер PC2, и предположим, что в ходе ее локализации обнаружены указанные ниже нарушения в работе.

- Маршрутизатор R2 не может перенаправлять пакеты на компьютер PC2.
- Маршрутизатор R2 не получает ответы ARP от компьютера PC2.

- Интерфейс коммутатора SW4, относящийся к магистральному каналу между коммутаторами SW4 и SW5, находится в состоянии "down/down" (не работает).
- Между коммутаторами SW4 и SW5 проложен кабель, в котором неправильно расположены выводы кабельной разводки.

Каждый из этих фактов может оказаться формулировкой основной причины в условиях того или иного конкретного проявления проблемы, но только последний факт имеет очевидное осуществимое решение (замена кабеля с учетом правильного расположения выводов). Следует также отметить, что все прочие приведенные выше утверждения являются действительными и важными фактами, обнаруженными в процессе локализации проблемы, но на их основании нельзя определить, что именно следует сделать для устранения проблемы. Таким образом, можно сделать вывод, что этап анализа основной причины должен осуществляться в соответствии с двумя приведенными ниже простыми рекомендациями.

Этап 1 Продолжайте процесс локализации проблемы до тех пор, пока не будет обнаружена истинная основная причина, которая, в свою очередь, имеет очевидное решение

Этап 2 Если в процессе изучения проблемы не удается свести ее до истинной основной причины, то следует исключить из рассмотрения максимально возможное количество факторов, не относящихся к этой проблеме, а также попытаться внести в сеть какое-то изменение в расчете на то, что изменятся наблюдаемые признаки неисправности, благодаря чему появится возможность более успешно выявить основную причину

Сравнение задач реальной сети с экзаменационными

В экзаменационных задачах есть намеки на то, что должно стать основным предметом рассмотрения при поиске решения, и решение следует искать в самой формулировке задачи. Например, если в задаче приведена схема сети, аналогичная представленной на рис. 3.1, и дано несколько вариантов ответов, причем во всех ответах упоминаются сети VLAN и протокол VTP, то следует начинать с рассмотрения среды локальной сети. Однако и в этом случае могут потребоваться дополнительные сведения об уровнях 1–3, а также об уровне данных и уровне управления, чтобы было проще найти ответ.

ВНИМАНИЕ!

Настоящий раздел посвящен общей процедуре поиска причин неисправностей, но приведен он только в данной главе, поскольку она является первой из всех глав этой книги, в которых рассматривается процесс устранения неисправностей в работе сетей.

На этом завершается введение в методы поиска и устранения неисправностей. Теперь обратим внимание на некоторых специфические особенности поиска и устранения неисправностей практически всех тем по коммутаторам LAN на экзамене ICND1.

Поиск неисправностей коммутации на уровне данных локальной сети

ВНИМАНИЕ!

Вот несколько советов по изучению начала второго раздела этой главы. Отдохните, отдышитесь и приготовьтесь. Следующий раздел довольно длинен, как и раздел "Основные темы" большинства других глав. Если необходимо прервать чтение до завершения этого длинного раздела, постарайтесь дочитать до следующего заголовка, начинающегося с "Этап 1", "Этап 2" и т.д.

Согласно общей стратегии поиска неисправностей, описанной выше, изучение причин нарушений в работе сети следует начинать с процесса маршрутизации IP на уровне 3. Если инженер сумеет определить, на каком именно этапе в процессе пересылки данных IP возникает проблема, то сможет перейти к следующему этапу, занявшись более подробным изучением данного этапа маршрутизации, включая анализ состояния функционирования сети на уровнях 1 и 2. Если тот этап маршрутизации осуществляется по сети LAN, подробности данного раздела применимы для локализации проблемы и поиска первопричины.

Здесь начинается второй из трех главных разделов этой главы, подробно рассматривающий инструментальные средства и процедуры, применяемые для устранения нарушений в работе процессов уровня данных локальной сети на уровнях 1 и 2. В оставшейся части главы предполагается, что какие-либо нарушения в работе на уровне 3 отсутствуют; процедура поиска неисправностей на уровне 3 рассматривается в главах 4, 5 и 11. В этой главе встречаются также упоминания протокола уровня управления, а именно протокола распределенного связующего дерева (STP), но он был подробно описан в двух предыдущих главах. Таким образом, эти разделы посвящены специально уровню данных коммутаторов LAN.

Настоящий раздел охватывает пять основных тем. Сначала рассмотрим процессы перенаправления в сетевом коммутаторе, в связи с чем дается вводное описание четырех основных этапов процесса устранения нарушений в работе средств коммутации локальной сети, в той степени, в какой эта тематика относится к данной главе. Затем подробно остановимся на четырех указанных этапах. И наконец, рассмотрим пример использования описанного процесса поиска неисправностей.

Краткий обзор нормального процесса перенаправления на сетевом коммутаторе

Обзор логики использования коммутатора LAN при перенаправлении фреймов приведен в главе 1, но без логики STP. Ниже приведены этапы процесса, описывающие логику, с дополнительными примечаниями, основное внимание которых уделено влиянию протокола STP на процесс перенаправления коммутатора.

Этап 1 Определите сеть VLAN, в которую должен быть перенаправлен фрейм, как указано ниже.

A. Если фрейм поступает в интерфейс доступа, то используется сеть доступа VLAN, относящаяся к интерфейсу.

B. Если фрейм поступает на магистральный канал, то используется сеть VLAN, указанная в заголовке магистрального соединения фрейма

Этап 2 Если интерфейс, через который поступает фрейм, находится в состоянии самообучения STP или пересылки в той же сети VLAN, то следует добавить MAC-адрес отправителя в таблицу MAC-адресов, указав в формируемой записи входной интерфейс и идентификатор сети VLAN (если соответствующая запись еще не находится в таблице)

Этап 3 Если интерфейс, через который поступает фрейм, не находится в состоянии пересылки STP в этой сети VLAN, то фрейм должен быть отброшен

Этап 4 Выполните поиск MAC-адреса получателя фрейма в таблице MAC-адресов, но только для записей с данными о сети VLAN, выявленной на этапе 1. В зависимости от того, найден ли MAC-адрес получателя, устройство должно выполнить указанные ниже действия.

A. MAC-адрес найден. Перенаправить фрейм только через тот интерфейс, который указан в соответствующей записи таблицы адресов.

B. MAC-адрес не найден. Передать фрейм по принципу лавинной рассылки через все прочие порты доступа в той же сети VLAN, находящиеся в состоянии пересылки протокола STP, и через все магистральные порты, по отношению к которым эта сеть VLAN является полностью поддерживаемой (активной, находящейся в списке разрешенных сетей, не подвергнутой отсечению и находящейся в состоянии пересылки STP)

Чтобы перенаправить фрейм, коммутатор должен сначала определить, в какую сеть VLAN его перенаправить (этап 1), в случае необходимости внести MAC-адрес отправителя в таблицу адресов (этап 2), а затем определить, куда должен быть перенаправлен фрейм. Исключительно для того, чтобы убедиться в полном понимании этого процесса, рассмотрим с помощью рис. 3.3 пример, в котором компьютер PC1 передает фрейм через свой стандартный шлюз, маршрутизатор R1; при этом используются MAC-адреса, показанные на этом рисунке.

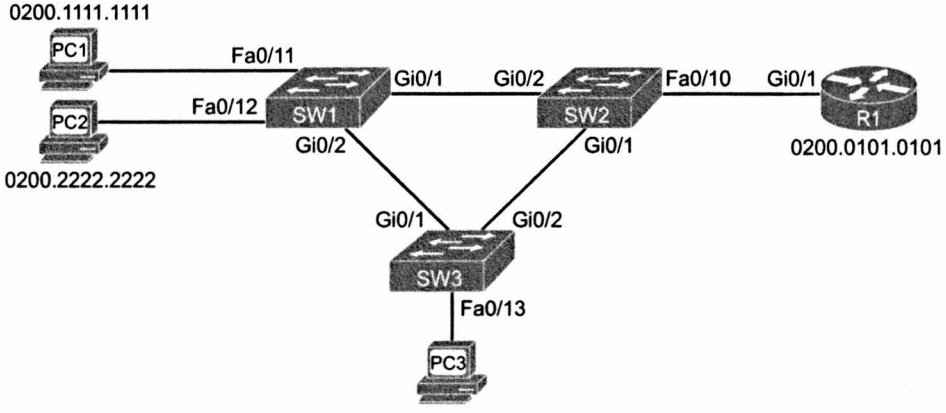


Рис. 3.3. Коммутируемая сеть, используемая в ходе анализа уровня данных в этой главе

В рассматриваемом примере предположим, что фрейм передается от компьютера PC1 (MAC-адрес отправителя — 0200.1111.1111) к маршрутизатору R1 (MAC-адрес получателя — 0200.0101.0101). Ниже приведены подробности каждого этапа логики коммутации.

- Коммутатор SW1, используя этап 1 описанной выше сводной процедуры перенаправления, определяет, применяется ли интерфейс Fa0/11 в качестве интерфейса доступа или магистрального интерфейса. В данном случае рассматриваемый интерфейс является интерфейсом доступа, назначенным в сеть VLAN 3.
- После перехода к этапу 2 коммутатор SW1 добавляет запись в свою таблицу MAC-адресов, указывая MAC-адрес 0200.1111.1111, интерфейс Fa0/11 и сеть VLAN 3.
- На этапе 3 коммутатор SW1 проверяет, находится ли интерфейс, через который поступил фрейм, Fa0/11, в состоянии пересылки STP.
- На этапе 4 коммутатор SW1 находит запись с MAC-адресом 0200.0101.0101, относящуюся к сети VLAN 3. Если бы коммутатор SW1 обнаружил запись, в которой указан интерфейс Gigabit 0/1, то перенаправил бы фрейм только на интерфейс Gi0/1. Если выходной интерфейс (Gi0/1) является магистральным интерфейсом, то коммутатор SW1 добавляет заголовок создания магистрали VLAN, в котором указана сеть VLAN 3, т.е. указан идентификатор сети VLAN, определенной на этапе 1.

Рассмотрим еще один пример, немного отличающийся от предыдущего, в котором рассматривается широковещательное сообщение, передаваемое компьютером PC1. Этапы 1–3 осуществляются, как и прежде, но на этапе 4 коммутатор SW1 передает фрейм по принципу лавинной рассылки. Но коммутатор SW3 рассылает этот фрейм только через порты доступа в сети VLAN 3 и магистральные порты, которые поддерживают сеть VLAN 3, с тем ограничением, что коммутатор SW1 не будет перенаправлять копию фрейма через порты, не находящиеся в состоянии пересылки STP.

Безусловно, эта логика перенаправления относительно проста, но в процессе поиска причин нарушений в работе приходится рассматривать почти все относящиеся к локальным сетям понятия, которые приведены в обоих томах (ICND1 и ICND2), а также обращаться к другим разделам. Например, поскольку известно, что компьютер PC1 вначале передает фреймы на коммутатор SW1, имеет смысл проверить состояние интерфейса, убедиться в том, что его состоянием является "`up/up`", и устранить нарушения в работе интерфейса, если в действительности он находится в другом состоянии. Иногда в ходе поиска причин возникновения определенной проблемы приходится выполнять проверку буквально по десяткам отдельных позиций. Поэтому в настоящей главе предлагается к рассмотрению процесс поиска неисправностей на уровне данных в локальной сети, согласно которому все необходимые действия организованы в виде четырех основных этапов, указанных ниже.

Этап 1 Проверить правильность схем сети с использованием протокола CDP

Этап 2 Локализовать проблемы с интерфейсами

Этап 3 Локализовать проблемы фильтрации и безопасности портов

Этап 4 Локализовать проблемы сетей VLAN и магистральных каналов

В следующих четырех подразделах рассматриваются и уточняются понятия и инструментальные средства, необходимые для выполнения каждого из этих четырех этапов. Разумеется, определенные факты и сведения в этих подразделах будут приведены

в данной книге впервые, но большинство конкретных основополагающих понятий уже рассматривались в других источниках, в том числе и в томе 1, а также в главах 1 и 2 настоящей книги. Основное назначение последующих подразделов — ознакомить читателя со всеми необходимыми понятиями, изложенными в одном контексте, что позволяет тратить меньше времени на анализ уникальных сценариев, но с большими шансами на успех (в соответствии с экзаменационными требованиями).

Этап 1. Проверка правильности схемы сети с использованием протокола CDP

Протокол обнаружения устройств компании Cisco (Cisco Discovery Protocol — CDP) может оказаться полезным средством проверки правильности информации, приведенной в схеме сети, а также восполнить недостающую необходимую информацию об устройствах и топологии. В ходе реальной эксплуатации сети ее схемы часто оказываются неактуальными и устаревшими, поэтому могут возникать проблемы, например, связанные с тем, что кто-то из инженеров переустановил некоторые кабели и не исправил в связи с этим схемы. Автор сомневается в том, что корпорация Cisco когда-либо включит в экзаменационное задание вопрос, в котором намеренно приведена неточная информация на прилагаемом к нему рисунке, но вполне может оказаться так, что на экзамене встретится вопрос с прилагаемой схемой сети, на которой не приведена вся необходимая информация, поэтому при поиске ответа на вопрос приходится использовать протокол CDP для выявления недостающих подробностей. Поэтому в настоящем подразделе рассматриваются протокол CDP и наиболее приемлемый этап 1 в процессе поиска причин нарушений в работе на уровне данных локальной сети, как описано ниже.

Этап 1 Проверить точность и полноту информации, приведенной на схеме сети, с помощью протокола CDP

ВНИМАНИЕ!

В настоящей главе этапы поиска неисправностей, касающихся средств коммутации локальной сети, пронумерованы начиная с этапа 1. Сами этапы и их номера на экзаменах не упоминаются; они пронумерованы в данной главе лишь для того, чтобы было проще ссылаться на определенный этап.

В маршрутизаторах, коммутаторах и других устройствах Cisco протокол CDP используется по многим причинам, но в маршрутизаторах и коммутаторах он применяется для передачи в виде анонсов основной информации о себе соседним устройствам, в частности — имени хоста, типа устройства, версии операционной системы IOS и номеров интерфейсов. При этом особое значение имеют три команды, позволяющие ознакомиться с информацией CDP, полученной от соседних устройств, которые перечислены в табл. 3.1. Фактически, даже если схема сети вообще отсутствует, инженер может легко создать схему маршрутизаторов и коммутаторов, используя вывод команды `show cdp`.

Таблица 3.1. Команды группы `show cdp`, позволяющие получить информацию о соседних устройствах

Команда	Описание
`show cdp neighbors [тип номер]`	Выводит одну итоговую строку с информацией о каждом соседнем устройстве или только о том соседнем устройстве, которое подключено к конкретному интерфейсу, если указан этот интерфейс
`show cdp neighbors detail`	Выводит большой объем информации о каждом соседнем устройстве (состоящей приблизительно из 15 строк), представляя отдельно каждое соседнее устройство
`show cdp entry название`	Выводит ту же информацию, что и команда `show cdp neighbors detail`, но только для одного указанного соседнего устройства

Вывод команд CDP может быть немного непонятен, поскольку не очевидно, находится ли указанный интерфейс на локальном устройстве или на соседнем. Читая слева направо, вывод обычно сообщает имя хоста соседнего устройства в разделе `Device ID` (идентификатор устройства), следующий раздел, `Local Intrfce` (локальный интерфейс), содержит имя и номера интерфейса локального устройства. Сами сведения об имени/номере интерфейса соседнего устройства находятся в правой части вывода команды в разделе "`Port ID`" (идентификатор порта).

В примере 3.1 приведен образец вывода команды `show cdp neighbors`, относящийся к коммутатору SW2, показанному на рис. 3.3. Найдите время, чтобы сравнить затененные части вывода этой команды с подробными сведениями, приведенными на рис. 3.3, и узнать, в каких полях перечисляются интерфейсы, относящиеся к каждому устройству.

Пример 3.1. Пример вывода команды `show cdp`

```
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, D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID  Local Intrfce  Holdtme  Capability  Platform    Port ID
SW1        Gig 0/2        154      S I         WS-C2960-   Gig 0/1
SW3        Gig 0/1        170      S I         WS-C2960-   Gig 0/2
R1         Fas 0/10       134      R S I       CISCO2901   Gig 0/1
```

Но после ввода протокола CDP в действие безопасность сети подвергается риску. Чтобы предотвратить угрозу, связанную с тем, что потенциальный нарушитель может получить подробные сведения о каждом коммутаторе, можно разрешить использование протокола CDP лишь там, где это необходимо. Компания Cisco рекомендует запретить использование протокола CDP во всех интерфейсах, кроме тех, в которых без него нельзя обойтись. С наибольшей вероятностью интерфейсами, в которых потребуется применение протокола CDP, окажутся интерфейсы, подключенные к другим маршрутизаторам и коммутаторам Cisco, а также интерфейсы, подключенные к IP-телефонам компании Cisco. Во всех прочих случаях может по-

требоваться запретить использование протокола CDP с помощью подкоманды интерфейса `no cdp enable`. (Подкоманда интерфейса `cdp enable` позволяет вновь разрешить использование протокола CDP.) Еще один вариант состоит в том, что можно применить глобальную команду `no cdp run` для запрета использования протокола CDP во всем коммутаторе или глобальную команду `cdp run`, позволяющую вновь ввести протокол CDP в действие глобально для всего коммутатора.

Этап 2. Локализация проблем с интерфейсом

Интерфейс коммутатора Cisco должен находиться в рабочем состоянии, поскольку лишь при этом условии коммутатор может обрабатывать фреймы, полученные через интерфейс, или передавать фреймы из интерфейса. Поэтому вполне очевидный этап 1 процедуры поиска неисправностей должен предусматривать проверку состояния каждого интерфейса, особенно если предполагается, что интерфейс будет использоваться для перенаправления фреймов, и определения того, находится ли интерфейс в исправном и рабочем состоянии.

В настоящем разделе рассмотрены возможные состояния интерфейса коммутаторов на основе системы Cisco IOS, перечислены основные причины перехода в нерабочие состояния и приведены сведения о том, каковы наиболее часто обнаруживаемые проблемы, которые имеют место даже в тех случаях, когда, на первый взгляд, интерфейс должен находиться в рабочем состоянии. На этом этапе решаются конкретные задачи, которые можно кратко описать в виде приведенных ниже этапов процедуры поиска неисправностей.

Этап 2 Проверить, имеют ли место проблемы с интерфейсами, как описано ниже.

A. Определить коды состояний интерфейса для каждого требуемого интерфейса и, если интерфейс не находится в состоянии "`connected`" или "`up/up`", устранять нарушения в работе до тех пор, пока интерфейс не достигнет этих состояний.

B. Применительно к интерфейсам в состоянии "`connected`" ("`up/up`") проверить, наблюдаются ли симптомы двух других проблем: несоответствие режимов передачи и целенаправленное уничтожение фреймов в связи с применением некоторых разновидностей средств защиты портов (т.е. эффект режима безопасности порта)

Коды состояния интерфейса и причины возникновения нерабочих состояний

В коммутаторах Cisco используются два набора кодов состояния: один набор состоит из двух кодов (слов), в которых используются такие же соглашения, как и в кодах состояний интерфейса маршрутизатора, а другой набор включает один код (слово). Оба набора кодов состояния позволяют определить, работает ли интерфейс.

Команды коммутатора `show interfaces` и `show interfaces description` выводят информацию о состоянии с применением двух кодов, как и команды маршрутизатора. Два кода указывают состояние канала и состояние протокола, поэтому по этим кодам, вообще говоря, можно судить о том, работают ли средства уровней 1 и 2 соответственно. В интерфейсах сетевого коммутатора состояние обычно отображается с обоими кодами, одновременно равными "`up`" или "`down`", поскольку во всех интерфейсах коммутатора используются одни и те же протоколы уровня передачи данных Ethernet, а это означает, что в работе отдельно взятого протокола уровня передачи данных никогда не должны возникать проблемы.

ВНИМАНИЕ!

В настоящей книге два указанных кода состояния обозначаются сокращенно последовательным указанием двух кодов, разделенных косой чертой, например "up/up".

В выводе команды show interfaces status отображается единственный код состояния интерфейса. Такие однокомпонентные коды состояния интерфейса соответствуют различным комбинациям традиционных двухкомпонентных кодов состояния интерфейса и могут быть легко сопоставлены с ними. Например, в выводе команды show interfaces status состояние "connected" указано для рабочих интерфейсов, что соответствует состоянию "up/up", отображаемому в выводе команд show interfaces и show interfaces description.

Если в выводе команды показано любое состояние интерфейса, отличное от "connected" или "up/up", значит, коммутатор не может перенаправлять или получать фреймы через интерфейс. С каждым нерабочим состоянием интерфейса связан небольшой набор основных причин его возникновения. Кроме того, следует отметить, что на экзаменах вполне может встретиться вопрос, в котором указан код состояния лишь одного или другого типа, поэтому при подготовке к экзаменам необходимо изучить, что означают коды состояния интерфейса, относящиеся к обоим наборам. В табл. 3.2 перечислены комбинации кодов и указаны некоторые основные причины, из-за которых может быть вызван переход интерфейса в данное конкретное состояние.

Ключевая тема

Таблица 3.2. Коды состояния интерфейса сетевого коммутатора

Состояние канала	Состояние протокола	Состояние интерфейса	Типичная основная причина
admin. down	down	disabled	В конфигурации интерфейса указана команда shutdown
down	down	notconnect	Кабель не подключен; кабель неисправен; расположение выводов кабеля является неправильным; скорости двух подключенных устройств не соответствуют друг другу; устройство на другом конце кабеля выключено или остановлен интерфейс этого устройства
up	down	notconnect	Это состояние в интерфейсах сетевого коммутатора практически не встречается
down	down (err-disabled)	err-disabled	Интерфейс заблокирован с помощью средств обеспечения безопасности порта. Канал EtherChannel использует это состояние для интерфейсов на канале, конфигурация которого не соответствует другим интерфейсам на канале
up	up	connected	Интерфейс работает

Состояние "notconnect" и варианты расположения выводов кабельной разводки

В табл. 3.2 перечислены причины, по которым интерфейс коммутатора может находиться в состоянии "notconnect". Большинство из указанных причин не требует более подробного объяснения, чем приведено в таблице. Например, если интерфейс связан кабелем с другим коммутатором, но находится в состоянии "notconnect", необходимо проверить другой коммутатор, чтобы узнать, не был ли его интерфейс остановлен. Но одна из причин обнаружения состояния "notconnect" (неправильная распайка выводов кабеля) заслуживает большего внимания, поскольку ошибка, связанная с применением неподходящего кабеля, встречается часто, но сама эта причина больше в данной книге не упоминается. (Сведения о расположении контактов кабеля Ethernet приведены в главе 2 тома 1.)

Стандарты кабельной разводки на основе *неэкранированной витой пары* Ethernet (Unshielded Twisted-Pair — UTP) указывают, с каким контактом разъемов RJ-45 на обоих концах кабеля должен быть соединен каждый из проводов. Устройства передают данные по парам проводов, причем в сетях 10BASE-T и 100BASE-T используются две пары: одна из них служит для передачи данных, а другая — для приема. При соединении кабелем двух устройств, в которых используются одни и те же пары выводов для передачи и приема данных, должен применяться так называемый *перекрестный кабель* (crossover cable), в котором одна пара проводов перекрещена с другой, поскольку провода, относящиеся к контактам одного устройства, через которые осуществляется передача данных, на другом конце кабеля должны быть присоединены к контактам, через которые происходит прием данных. С другой стороны, есть и такие устройства, в которых контакты, предназначенные для передачи и приема данных, в разъеме переставлены местами по сравнению с тем устройством, с которым они соединены, поэтому для них требуется кабель с прямым соединением, характеризующимся тем, что в нем самом пары проводов не пересекаются. На рис. 3.4 показан пример схемы типичной коммутируемой локальной сети, на которой указаны типы кабелей.

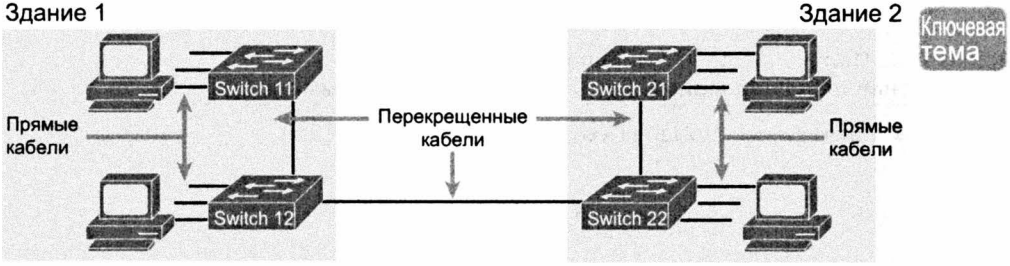


Рис. 3.4. Пример использования перекрестных кабелей и кабелей с прямыми соединениями

Чтобы успешно устранять нарушения в работе сети, необходимо знать, через какие пары выводов в каждом устройстве происходит передача и прием данных. В табл. 3.3 перечислены устройства, которые наиболее часто упоминаются в контексте экзаменов CCNA, и показано, какие пары выводов в них используются. Обратите внимание на то, что для соединения кабелем устройств двух типов, показанных в одном и том же

столбце, требуется перекрестный кабель, а для соединения двух устройств из разных столбцов таблицы требуется кабель с прямым соединением.

Ключевая тема **Таблица 3.3. Используемые пары выводов в сетях 10BASE-T и 100BASE-T**

Устройства, осуществляющие передачу через контакты 1 и 2 и прием — через контакты 3 и 6	Устройства, осуществляющие передачу через контакты 3 и 6, а прием — через контакты 1 и 2
Сетевые интерфейсные платы персонального компьютера	Концентраторы
Маршрутизаторы	Коммутаторы
Беспроводные точки доступа (интерфейс Ethernet)	—
Сетевые принтеры, подключенные к сети Ethernet	—

Определение скорости интерфейса коммутатора и режима дуплексности

Определение параметров скорости и режима дуплексной передачи в интерфейсах коммутатора может осуществляться несколькими способами. Зачастую в интерфейсах, в которых используется медная кабельная разводка и которые способны поддерживать несколько параметров скорости и дуплексной передачи, применяется процесс автоматического согласования, определяемый стандартом IEEE (а именно — IEEE 802.3x). Еще один вариант состоит в том, что для интерфейсов коммутаторов и маршрутизаторов, а также для большинства сетевых плат может применяться настройка конфигурации на использование конкретных параметров скорости или режима дуплексной передачи. Для коммутаторов и маршрутизаторов необходимые значения параметров задаются с помощью подкоманды интерфейса `speed {10 | 100 | 1000}`, применяемой в сочетании с подкомандой интерфейса `duplex {half | full}`.

Как показано в примере 3.2, параметры интерфейса, касающиеся определения скорости и дуплексной передачи коммутатора, можно определить с помощью команд `show interfaces` и `show interfaces status`.

Пример 3.2. Получение сведений о параметрах скорости и дуплексной передачи, применяемых в интерфейсах коммутатора

```
SW1# show interfaces f0/11 status

Port      Name          Status      Vlan   Duplex   Speed   Type
Fa0/11    link to PC1   connected   3      a-full     100   10/100BaseTX

SW1# show interfaces f0/12 status

Port      Name          Status      Vlan   Duplex   Speed   Type
Fa0/12    link to PC2   connected   3      a-full   a-100   10/100BaseTX

SW1# show interfaces fa0/12
FastEthernet0/12 is up, line protocol is up (connected)
  Hardware is Fast Ethernet, address is 1833.9d7b.0e8c (bia
1833.9d7b.0e8c)
  Description: link to PC2
```

```
MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
   reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Full-duplex, 100Mb/s, 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 never, 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: 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
   1453 packets input, 138334 bytes, 0 no buffer
   Received 1418 broadcasts (325 multicasts)
        0 runts, 0 giants, 0 throttles
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
        0 watchdog, 325 multicast, 0 pause input
        0 input packets with dribble condition detected
        33640 packets output, 2651335 bytes, 0 underruns
        0 output errors, 0 collisions, 1 interface resets
        0 unknown protocol drops
        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
```

Хотя обе команды могут быть полезными, только команда `show interfaces status` позволяет судить о том, как коммутатор определил параметры скорости и дуплекса. Вывод этой команды отображает параметры автопереговоров с префиксом `a-`. Например, наличие в выводе команды строки `a-full` означает, что автопереговоры договорились о применении дуплексной передачи, а строка `full` указывает, что настройка конфигурации выполнена вручную. Выделенные строки примера приводят следующее доказательство использования автопереговоров для интерфейсов F0/11 и F0/12.

`F0/11`. Скорость 100 Мбит/с по конфигурации (100, без `a-`) и дуплексная передача по автопереговорам (`a-full`).

`F0/12`. Оба значения получены в результате автопереговоров (`a-100` и `a-full`, оба с префиксом `a-`).

Обратите внимание на то, что команда `show interfaces Fa0/12` (без опционального параметра `status`) просто указывает значения параметров скорости и дуплексной передачи для интерфейса Fa0/12, но в ее выводе отсутствуют какие-либо сведения, по которым можно судить о том, что значения этих параметров были заданы в ходе автоматического согласования.

Проблемы, связанные со скоростью и дуплексом

При выяснении скорости и дуплекса в ходе поиска и устранения неисправностей имеет смысл изучить оба устройства на обоих концах канала связи. Устройства не обязаны использовать те же параметры скорости или дуплекса, но при различиях происходит следующее:

Ключевая тема

Определения рассогласования скорости и рассогласования дуплекса

- *Рассогласование скорости* (speed mismatch). Если конечные точки на канале связи Ethernet используют разные скорости, обе должны продемонстрировать состояние интерфейса `notconnect` или `down/down`.
- *Рассогласование дуплекса* (duplex mismatch). Если конечные точки используют ту же скорость, но разные параметры дуплекса, интерфейсы будут в состоянии `up`, но другие счетчики системного монитора покажут проблемы на полудуплексном конце канала связи.

Как ни странно, но распознать рассогласование скорости на коммутаторах Cisco довольно трудно. Безусловно, если оба устройства на канале связи используют автопереговоры, то они выберут одинаковую скорость. Но если на одном из устройств автопереговоры отключены, коммутатор Cisco, даже без автопереговоров, способен выяснить подходящую скорость и использовать ее, если командой `speed` не задана работа на предварительно установленной скорости. Будучи настроенным такой командой, как `speed 100`, интерфейс коммутатора должен пытаться использовать именно эту скорость.

ВНИМАНИЕ!

У коммутаторов Cisco нет единой команды для отключения автопереговоров IEEE; но задание командами `speed` и `duplex` конкретной скорости и дуплекса имеет побочный эффект отключения автопереговоров.

В качестве примера рассмотрим рис. 3.3 и предположим, что в конфигурацию интерфейса Gi0/2 коммутатора SW2 были введены команды `speed 100` и `duplex half` (между прочим, применение таких настроек для интерфейса, способного работать в гигабитовой сети, не рекомендуется). Коммутатор SW2 использует эти настройки и отменяет процесс автоматического согласования по стандарту IEEE, поскольку в его конфигурацию введены обе команды, `speed` и `duplex`. Если бы даже в конфигурацию интерфейса Gi0/1 коммутатора SW1 не была введена команда `speed`, коммутатор SW1 все равно распознал бы необходимую скорость (100 Мбит/с), несмотря на то, что в коммутаторе SW2 не используется согласование по стандарту IEEE, поэтому в коммутаторе SW1 также применялась бы скорость 100 Мбит/с. В примере 3.3 показаны результаты, полученные на коммутаторе SW1 в данном конкретном случае.

Пример 3.3. Получение сведений о параметрах скорости и дуплексной передачи, применяемых в интерфейсах коммутатора

```
SW1# show interfaces gi0/1 status

Port   Name          Status      Vlan   Duplex  Speed   Type
Gi0/1  Link to SW2   connected   trunk  a-half  a-100   10/100/1000BaseTX
```

В этом примере строки с информацией о скорости и дуплексной передаче все еще отображаются с префиксом "`a-`", а это означает, что по-прежнему применяется автоматическое согласование. Причина этого в том, что в данном случае скорость

была найдена автоматически, а параметр дуплексной передачи был выбран в связи с применением в процессе автоматического согласования по стандарту IEEE. В стандарте IEEE указано, что в случае неудачного завершения автоматического согласования в портах, работающих на скорости 100 Мбит/с, используется стандартная полудуплексная передача.

Рассогласование скорости может возникнуть просто при задании различных скоростей на устройствах обоих концов канала связи. Если канал связи не был подключен (команда `no shutdown`), интерфейс коммутатора перейдет в состояние `disabled` или `down/down`.

Задача обнаружения рассогласования дуплекса может оказаться много сложнее обнаружения рассогласования скорости, поскольку *даже при отсутствии согласования параметров дуплексной передачи на обоих концах сегмента Ethernet для интерфейса коммутатора отображается состояние* "`connected`" (*"*`up/up`*"*). В этом случае, безусловно, интерфейс работает, но характеристики его работы могут оказаться неудовлетворительными, поскольку имеет место низкая производительность и обнаруживаются признаки проблем, связанных с неустойчивостью функционирования сети.

Рассогласование дуплекса на канале связи приводит к проблемам, поскольку одно устройство (полудуплексный конец) использует логику множественного доступа с контролем несущей и обнаружением конфликтов (CSMA/CD), а другой нет. Полудуплексный конец ждет паузы для передачи и получения фреймов. Он полагает, что поступление другого фрейма во время его передачи приводит к коллизии и прекращает передачу фрейма. Дуплексный конец посылает фреймы в любое время, заставляя полудуплексный конец ошибочно полагать, что происходят коллизии. При достаточном трафике интерфейс может находиться в состоянии `connected`, но быть абсолютно бесполезным для передачи трафика и даже приводить к потере важных сообщений STP.

Для выявления проблем рассогласования режимов передачи рекомендуется выполнить описанные ниже действия.

Рекомендации по обнаружению проблем рассогласования режимов передачи Ключевая тема

- Воспользоваться такими командами, как `show interfaces`, на обоих концах канала, чтобы убедиться в правильности установки параметров дуплексной передачи на каждом конце.
- Проследить за увеличением значений определенных счетчиков, указывающих на то, что в интерфейсе применяется полудуплексная передача. Значения таких счетчиков, указывающих на появление *карликовых фреймов* (runt), коллизий и поздних коллизий, увеличивается, если в соседнем устройстве, в отличие от данного устройства, применяется дуплексная передача. (Но следует отметить, что значения этих счетчиков могут увеличиваться и в результате закономерного возникновения коллизий в обычных обстоятельствах.)

В примере 3.2 выделены значения указанных счетчиков в выводе команды `show interfaces`.

Основной причиной несоответствия режимов передачи может оказаться несовпадение значений, выбранных в процессе автоматического согласования по стандарту IEEE. Если одно устройство предпринимает попытки автоматического согласования, а другое на них не отвечает, то первое устройство выбирает стандартные параметры дуплексной передачи, установленные с учетом текущей скорости. Согласно стандарту IEEE, параметры дуплексной передачи выбираются, как описано ниже.

Ключевая тема

Стандартные варианты выбора режима дуплексной передачи на основе автоматического согласования по стандарту IEEE с учетом текущей скорости

- Если скорость равна 10 или 100 Мбит/с, то стандартно используется полудуплексная передача.
- Если скорость составляет 1000 Мбит/с, то стандартно используется дуплексная передача.

ВНИМАНИЕ!

В интерфейсах Ethernet, работающих на скорости свыше 1 Гбит/с, всегда применяется дуплексная передача.

Этап 3. Локализация проблем фильтрации и безопасности портов

В ходе любого анализа процесса перенаправления необходимо учитывать применение средств безопасности, в результате действия которых могут быть уничтожены некоторые фреймы или пакеты. Отметим, что настройка конфигурации маршрутизаторов и коммутаторов может выполняться с применением *списков управления доступом* (Access Control List — ACL), в результате чего проверяются пакеты и фреймы, переданные или полученные через интерфейс, а при определенных условиях маршрутизаторы или коммутаторы уничтожают некоторые из пакетов или фреймов.

На экзаменах CCNA списки управления доступом коммутатора не рассматриваются, но некоторые вопросы могут касаться аналогичного средства коммутатора, называемого защитой порта. Как описано в главе 8 тома 1, служба защиты порта может использоваться для уничтожения коммутатором некоторых фреймов, переданных и полученных через интерфейс. Служба защиты порта включает три основные функции, описанные ниже, с помощью которых определяется, какие фреймы должны быть отфильтрованы.

- Ограничение списка MAC-адресов, которые могут передавать и принимать фреймы через интерфейс коммутатора, а также уничтожение фреймов, в которых приведены другие MAC-адреса.
- Ограничение количества MAC-адресов, для которых разрешено использование интерфейса и уничтожение входящих и исходящих фреймов с MAC-адресами, обнаруженными по достижении максимально допустимого количества адресов.
- Сочетание двух указанных выше функций.

Этап 1 процедуры поиска причин нарушений в работе, связанных с применением защиты порта, должен предусматривать поиск интерфейсов, на которых включе-

на защита порта, с последующим определением того, не происходят ли где-либо в настоящее время определенные нарушения, связанные с этим. В данном процессе сложнее всего учесть различия в том, как операционная система IOS реагирует на нарушения в соответствии с параметрами, заданными подкомандой интерфейса `switchport port-security violation` *режим_нарушения*, которая сообщает коммутатору, какие действия следует выполнять при возникновении нарушений. Общий процесс поиска причин нарушения в работе описан ниже.

Этап 3 Проверить наличие проблем в работе средства защиты порта, как указано ниже.

A. Выявить все интерфейсы, в которых включена защита порта (с помощью команды `show running-config` или `show port-security`).

B. Определить, есть ли в настоящее время нарушение защиты, отчасти основываясь на том, какой режим нарушения работы интерфейса задан в конфигурации защит порта, как описано ниже.

`shutdown`. Интерфейс находится в состоянии "`err-disabled`" (отключен из-за ошибки).

`restrict`. Интерфейс находится в состоянии "`connected`", но команда интерфейса `show port-security` показывает увеличение значения счетчика нарушений.

`protect`. Интерфейс находится в состоянии "`connected`", но команда интерфейса `show port-security` не показывает увеличение значения счетчика нарушений.

C. Во всех случаях сравнить конфигурацию защиты порта со схемой сети, а также проверить значение поля "`last source address`" (адрес последнего отправителя) в выводе команды интерфейса `show port-security`

Одна из сложностей в процессе устранения нарушений в работе защиты порта обусловлена тем, что при использовании некоторых конфигураций защиты порта уничтожаются лишь фреймы, не соответствующие установленным требованиям, но в результате это приводит к запрещению работы интерфейса в полном соответствии с заданным в конфигурации режимом устранения нарушений. Все три режима устранения нарушений предусматривают уничтожение трафика, не соответствующего требованиям, согласно тому, что задано в конфигурации.

Например, если допустимым является только один заранее заданный MAC-адрес, 0200.1111.1111, то коммутатор уничтожает весь трафик в соответствующем интерфейсе, отличный от входящего и исходящего трафика с адресом 0200.1111.1111. Но применение режима `shutdown` вынуждает отбрасывать весь трафик, даже допустимые входящий и исходящий трафики с адресом 0200.1111.1111, после возникновения хотя бы одного нарушения. В табл. 3.4 приведены некоторые итоги, чтобы упростить процесс подготовки к сертификационному экзамену.

На этапе 3B процедуры поиска неисправностей упоминается состояние интерфейса "`err-disabled`" (сокращение от "error disabled" — "отключен из за ошибки"). В этом состоянии проверяется, что интерфейс настроен на использование средства безопасности порта, что произошло нарушение и в настоящее время не допускается прохождение через интерфейс какого-либо трафика. Следствием применения такого состояния интерфейса становится ввод в действие режима устранения нарушений `shutdown`, поскольку это единственный из трех режимов безопасности порта, отключающий интерфейс.

Ключевая тема

Таблица 3.4. Действия, предпринимаемые средствами защиты порта, в зависимости от установленного режима устранения нарушений

Параметр команды нарушения защиты `switchport port-security`	`protect`	`restrict`	`shutdown*`
Отбрасывает не соответствующий требованиям трафик	Да	Да	Да
Отключает интерфейс, отбрасывает весь трафик	Нет	Нет	Да
Увеличивает значение счетчика нарушений для каждого недопустимого фрейма	Нет	Да	Да

* Стандартное значение — `shutdown`.

Для исправления такого нарушения в работе интерфейс необходимо отключить командой `shutdown`, а затем снова включить командой `no shutdown`. В примере 3.4 показано, как происходит перевод интерфейса в состояние "`err-disabled`".

Пример 3.4. Использование средств защиты порта при определении допустимых MAC-адресов для конкретных интерфейсов

```
! В выводе первой команды перечислены все интерфейсы, для которых
! разрешено применение средств защиты порта, а также указан режим
! устранения нарушений под заголовком "Security Action" (действие по
! обеспечению безопасности).
SW1# show port-security
Secure Port  MaxSecureAddr  CurrentAddr SecurityViolation Security Action
               (Count)        (Count)     (Count)
---------------------------------------------------------------------------
  Fa0/13              1              1           1            Shutdown
---------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 8192
!
! В выводе следующей команды показано состояние "err-disabled", из чего
! следует, что произошло нарушение защиты.
SW1# show interfaces Fa0/13 status

Port    Name   Status        VLAN   Duplex   Speed  Type
Fa0/13         err-disabled  1      auto     auto   10/100BaseTX
!
! Кроме того, в выводе следующей команды выделены некоторые наиболее
! важные сведения.
SW1# show port-security interface Fa0/13
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   : 0200.3333.3333:2
Security Violation Count   : 1
```

В частности, в выводе команды интерфейса `show port-security` приведен определенный объем информации, способствующей упрощению процесса поиска неисправностей. Наличие обозначения состояния порта "`secure-shutdown`" указывает на то, что интерфейс запрещен для всего трафика в результате нарушения и что состоянием интерфейса должно быть "`err-disabled`". В конце вывода команды приведено значение счетчика нарушений, увеличивающееся на 1 после каждого нового нарушения. Любопытно отметить, что при использовании режима устранения нарушений `shutdown` после увеличения значения счетчика на 1 интерфейс переводится в состояние "`err-disabled`" и значение счетчика больше не может увеличиваться до тех пор, пока инженер последовательно не выполнит применительно к этому интерфейсу команды `shutdown` и `no shutdown`. Наконец, следует отметить, что в предпоследней строке приведен MAC-адрес отправителя последнего фрейма, полученного через интерфейс. Это значение может применяться при обнаружении MAC-адреса устройства, которое вызвало нарушение.

Перейдем к другому примеру. Режимы устранения нарушений `restrict` и `protect` по-прежнему вызывают уничтожение фреймов, но сами осуществляемые при этом действия во многом отличаются. При использовании этих режимов интерфейс остается в состоянии "`connected`" (`up/up`), но вместе с тем уничтожает фреймы, не соответствующие требованиям, согласно заданным параметрам конфигурации средств безопасности порта. Поэтому не следует руководствоваться предположением, что если интерфейс находится в состоянии "`connected`" или "`up/up`", то нет иных причин, по которым устанавливался бы запрет на прохождение трафика.

В примере 3.5 показаны типичная конфигурация и вывод команды `show` при использовании режима `protect`. В этом случае персональный компьютер с MAC-адресом 0200.3333.3333 передает фреймы в порт Fa0/13, а конфигурация порта имеет такую настройку, что интерфейс Fa0/13 может получать только фреймы с адресом отправителя 0200.1111.1111.

Пример 3.5. Применение средства безопасности на основе режима "`protect`"

```
SW1# show running-config
! Часть строк вывода опущена
interface FastEthernet0/13
  switchport mode access
  switchport port-security
  switchport port-security mac-address 0200.1111.1111
  switchport port-security violation protect
! Часть строк вывода опущена

SW1# show port-security interface Fa0/13
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Protect
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    : 0200.3333.3333:1
Security Violation Count    : 0
```

Показанный в примере 3.5 вывод команды `show` был получен после передачи персональным компьютером с MAC-адресом 0200.3333.3333 большого количества фреймов, притом что все эти фреймы были уничтожены коммутатором согласно режиму безопасности порта. В выводе этой команды MAC-адрес персонального компьютера с уничтожаемыми фреймами, 0200.3333.3333, показан как последний MAC-адрес отправителя в полученном фрейме. Но заслуживает внимания то, что состояние порта обозначено как "`secure-up`", а счетчик нарушений имеет нулевое значение. Иными словами, наблюдаемые показатели являются такими, что напрашивается вывод, будто все обстоит благополучно. Тем не менее в режиме "`protect`" команда интерфейса `show port-security` не показывает никаких сведений, подтверждающих факт происходящих в действительности нарушений. Единственным свидетельством нарушения становится то, что трафик конечного пользователя не достигает того места, в которое он направлен.

Если бы в этом примере использовался режим устранения нарушений "`restrict`", то состояние порта по-прежнему оставалось бы таким, что в выводе команды присутствовала бы информация о состоянии "`secure-up`", но счетчик нарушений безопасности продолжал бы увеличиваться на 1 после обнаружения каждого фрейма, не соответствующего требованиям.

Что касается экзаменов, то сама проблематика нарушения защиты порта вряд ли будет рассматриваться; скорее всего, речь может идти о том, какая именно функция защиты применяется в тех или иных условиях. А в тексте экзаменационного вопроса вполне может быть явно указано, какие действия должны выполняться применяемым средством защиты порта. В этих случаях может оказаться более целесообразным такой способ поиска решения, который предусматривает немедленную проверку конфигурации защиты порта. После этого следует сравнить MAC-адреса, заданные в конфигурации, с MAC-адресами устройств, подключенных к интерфейсу. С наибольшей вероятностью на экзаменах будут рассматриваться такие задачи, по условиям которых в конфигурацию неправильно введены MAC-адреса или задано слишком малое значение максимального количества MAC-адресов.

Ниже для справки кратко приведены этапы настройки защиты порта, подробно рассматриваемые в главе 8 первого тома книги.



Этапы настройки защиты порта

Этап 1 Сделать интерфейс коммутатора либо интерфейсом статического доступа, либо магистральным интерфейсом, используя подкоманды интерфейса `switchport mode access` или `switchport mode trunk` соответственно

Этап 2 Включить защиту порта, используя подкоманду интерфейса `switchport port-security`

Этап 3 Переопределить стандартное максимальное количество связанных с интерфейсом допустимых MAC-адресов (1), используя подкоманду интерфейса `switchport port-security maximum` *число* (Необязательно)

Этап 4 Переопределить стандартное действие при нарушении защиты (завершение работы системы), используя подкоманду интерфейса `switchport port-security violation {protect | restrict | shutdown}` (Необязательно)

Этап 5 Предопределить все допустимые MAC-адреса отправителей для этого интерфейса, используя команду `switchport port-security mac-address` *mac-адрес*. Для определения нескольких MAC-адресов используйте команду многократно (Необязательно)

Этап 6 Указать коммутатору автоматически динамически изучать MAC-адреса, используя подкоманду интерфейса `switchport port-security mac-address sticky` (Необязательно)

Этап 4. Локализация проблем сетей VLAN и магистральных каналов

Успешная пересылка трафика коммутатором зависит и от правильности конфигурации сетей доступа VLAN в интерфейсах доступа, и от надлежащего функционирования магистралей VLAN, способных передавать трафик во многие сети VLAN. Следует помнить, что коммутатор получает возможность перенаправлять фреймы в конкретную сеть VLAN только после получения информации об этой сети VLAN либо с помощью настройки конфигурации, либо с применением протокола VTP, а сама сеть VLAN должна быть активной. В следующих разделах рассматриваются некоторые инструментальные средства, позволяющие диагностировать все проблемы сетей VLAN, связанные с указанной темой. Рассматриваемый этап поиска и устранения неисправностей состоит из указанных ниже действий.

Этап 4 Проверить сети VLAN и магистрали VLAN, как показано ниже.

A. Идентифицировать все интерфейсы доступа и назначенные им сети доступа VLAN, после чего задать в случае необходимости правильные назначения сетей VLAN.

B. Определить, выполняются ли оба требования, согласно которым сети VLAN должны существовать (будучи сформированными в результате настройки конфигурации или ввода в действие с помощью протокола VTP) и быть активными на каждом коммутаторе. В противном случае настроить конфигурацию и активизировать сети VLAN, чтобы устранить нарушения в работе, если это потребуется.

C. Определить работоспособность магистральных интерфейсов каждого коммутатора и определить сети VLAN, в которые может перенаправляться трафик с помощью каждой магистрали

В следующих трех разделах последовательно рассматриваются три проверки, описанные выше.

Проверка правильности привязки интерфейсов к сетям VLAN

Чтобы убедиться в правильности назначения каждому интерфейсу доступа сети VLAN, инженеру достаточно определить, какие интерфейсы коммутатора являются интерфейсами доступа, а не магистральными интерфейсами, узнать, для какой сети VLAN назначен каждый интерфейс доступа, и сравнить полученную информацию с информацией в документации. В этом процессе могут оказаться особенно полезными команды `show`, перечисленные в табл. 3.5.

Ключевая тема

Таблица 3.5. Команды, позволяющие находить порты доступа и сети VLAN

Команда EXEC	Описание
`show vlan`	Выводит все сети VLAN и все интерфейсы, назначенные для каждой сети VLAN, исключая магистральные интерфейсы
`show vlan brief`	Выводит краткую версию той же информации, что и команда `show vlan`
`show vlan id` *номер*	Перечисляет порты доступа и магистральных каналов VLAN
`show interfaces` *тип номер* `switchport`	Идентифицирует сеть доступа VLAN интерфейса, голосовую сеть VLAN, а также административный режим (заданный в конфигурации) и рабочий режим (доступа или магистральный)
`show mac address-table dynamic`	Формирует список записей таблицы MAC-адресов, в который входят MAC-адреса с соответствующими им интерфейсами и сетями VLAN

По возможности осуществление данного этапа следует начинать с выполнения команд `show vlan` и `show vlan brief`, поскольку с их помощью можно получить список всех известных сетей VLAN и интерфейсов доступа, назначенных для каждой сети VLAN. Но следует учитывать, что вывод этих команд включает много интерфейсов, но не все; конкретно эти команды выводят следующее.

- Интерфейсы, не работающие в настоящее время как магистрали.
- Интерфейсы в любом текущем состоянии, включая состояния `notconnect` и `err-disabled`.

Например, может оказаться так, что в выводе этих команд в список интерфейсов сети VLAN 1 будет включен интерфейс Gi0/2, но после перехода в рабочее состояния интерфейса Gi0/1 произойдет согласование и создание магистрального соединения, а это означает, что указанный интерфейс с какого-то момента перестанет относиться к категории интерфейсов доступа и больше не появится в выводе команды `show vlan brief`.

Если в каком-то контрольном вопросе на экзамене не предусмотрено применение команд `show vlan` и `show interface switchport`, то для выявления сетей доступа VLAN можно также применить команду `show mac address-table`. Она выводит таблицу MAC-адресов в виде отдельных записей, в которых указан MAC-адрес, интерфейс и идентификатор сети VLAN. Если контрольный вопрос содержит сведения о том, что интерфейс коммутатора подключен к одному устройству, такому как персональный компьютер, то в выводе команды должна обнаруживаться только одна запись таблицы MAC-адресов, в которой указан данный конкретный интерфейс доступа, а идентификатор сети VLAN, указанный в той же записи, обозначает сеть доступа VLAN. (Такие предположения не могут относиться к магистральным интерфейсам.)

После определения интерфейсов доступа и связанных с ними сетей VLAN и обнаружения того, что интерфейс назначен для сети VLAN неправильно, можно воспользоваться командой режима конфигурирования интерфейса `switchport access vlan` *номер* для правильного присваивания идентификатора сети VLAN.

Обнаружение заданных или не активных сетей доступа VLAN

Коммутатор не будет перенаправлять фрейм в сеть VLAN *X* если он:

- не имеет определения сети VLAN *X* (например, командой `vlan x`);
- сеть VLAN X на коммутаторе есть, но она блокирована (командой `shutdown`).

Следующий этап поиска и устранения неисправностей, этап 4B, требует удостовериться в том, что у каждого коммутатора есть определение сети VLAN и что она не блокирована.

Коммутаторы обычно знают о существовании сети VLAN, или узнают о ней, используя протокол VTP, или она непосредственно задается на локальном коммутаторе. В этой книге подразумевается, что протокол VTP был отключен или переведен в прозрачный режим, поэтому для поддержки сети VLAN номер *x* все коммутаторы следует непосредственно настроить командой `vlan x`.

Обе проблемы могут быть легко обнаружены в выводе команды `show vlan` или `show vlan brief`. Если сеть VLAN на коммутаторе отсутствует, эти команды просто не выводят сеть VLAN; в этом случае добавьте ее в конфигурацию, используя команду конфигурации `vlan идентификатор_vlan`. В выводе состояние будет обозначено как `active` или `act/lshut`. Второе из этих состояний означает, что сеть VLAN блокирована. Для решения этой проблемы используйте глобальную команду конфигурации `no shutdown vlan идентификатор_vlan`.

Идентификация магистральных интерфейсов и принадлежащих им сетей VLAN

На этапе 4C наблюдаемые проблемы можно разделить на две общие категории, чтобы приступить к раздельному рассмотрению проблем, относящихся к разным категориям: проблем, обусловленных некорректной работой магистральных интерфейсов, и проблем, вызванных тем, что интерфейс, который должен присоединиться к магистрали, не становится магистральным.

Этап отладки, на котором рассматриваются проблемы первой категории, может быть легко выполнен с помощью команды `show interfaces trunk`, позволяющей получить только сведения о том, какие магистрали в настоящее время являются действующими. Изучение вывода этой команды лучше всего начать с последнего раздела, в котором перечисляются сети VLAN, трафик которых должен быть перенаправлен по магистрали. Любые сети VLAN, упоминаемые в этом последнем списке сетей VLAN в выводе команды, соответствуют указанным ниже критериям.

Четыре причины, по которым коммутатор не передает трафик сети VLAN через конкретную магистраль



- Сеть VLAN существует и является активной в данном коммутаторе (что было описано в предыдущем разделе, согласно которому соответствующую информацию можно получить с помощью команды `show vlan`).
- Сеть VLAN не удалена из списка допустимых сетей VLAN в данной магистрали (в соответствии с тем, что может быть задано в конфигурации с помощью команды режима конфигурирования интерфейса `switchport trunk allowed vlan`).

- Сеть VLAN не была отсечена от магистрали с помощью протокола VTP. (Это функция VTP, которая в данном разделе пока игнорируется. Она упоминается здесь только потому, что ее выводит команда `show`.)
- Магистраль находится в состоянии пересылки STP в этой сети VLAN (что также можно определить с помощью вывода команды `show spanning-tree vlan` *номер*).

В примере 3.6 показан вывод команды `show interfaces trunk`, в котором последний раздел вывода выделен. В этом случае магистраль перенаправляет трафик только для сетей VLAN 1 и 4.

Пример 3.6. Список активных сетей VLAN

```
SW1# show interfaces trunk
Port        Mode         Encapsulation    Status         Native vlan
Gi0/1       desirable    802.1q           trunking       1

Port        Vlans allowed on trunk
Gi0/1       1-2,4-4094

Port        Vlans allowed and active in management domain
Gi0/1       1,4

Port        Vlans in spanning tree forwarding state and not pruned
Gi0/1       1,4
```

Если какая-то сеть VLAN не показана в последней части вывода рассматриваемой команды, это вовсе не означает, что возникла проблема. В действительности сеть VLAN могла быть исключена из магистрали на законных основаниях по любой из причин, указанных выше, непосредственно перед выполнением команды примера 3.6. Следует учитывать, что при подготовке к ответам на некоторые экзаменационные вопросы может оказаться полезным получение сведений о том, по каким причинам трафик, относящийся к некоторой сети VLAN, не перенаправляется по магистральному каналу, а подробности в выводе укажут конкретные причины.

Вывод команды `show interfaces trunk` создает три отдельных списка сетей VLAN, каждый под своим заголовком. Эти три списка демонстрируют набор причин, по которым сеть VLAN не перенаправляет пакеты по магистральному каналу. В табл. 3.6 резюмируются заголовки, предшествующие каждому списку и причинам, по которым коммутатор решает, включать или не включать сеть VLAN в каждый из списков.

Ключевая тема **Таблица 3.6. Сети VLAN, выводимые командой `show interfaces trunk`**

Позиция списка	Заголовок	Причины
Первый	Сети VLAN разрешены	Сети VLAN 1–4094 минус сети, удаленные командой `switchport trunk allowed`
Второй	Сети VLAN разрешены и активны...	Первый список минус сети, либо не определенные на локальном коммутаторе, либо находящиеся в отключенном состоянии
Третий	Сети VLAN в связующем дереве...	Второй список минус интерфейсы, блокированные протоколом STP и отсеченные протоколом VTP

Переходя к следующему разделу магистралей, следует также проверить конфигурацию собственной сети VLAN магистрального канала. Идентификатор собственной сети VLAN может быть вручную установлен для другой сети VLAN на любом конце магистрального канала командой `switchport trunk native vlan` *идентификатор-vlan*. Если собственные сети VLAN будут отличаться, то коммутаторы случайно заставят фреймы покидать одну сеть VLAN и входить в другую.

Например, передавая фрейм по магистрали 802.1Q с использованием собственной сети VLAN 1, коммутатор SW1 не добавляет к фрейму заголовок сети VLAN, что полностью соответствует условиям применения собственной сети VLAN. А после того как коммутатор SW2 получает фрейм и обнаруживает, что отсутствует заголовок 802.1Q, он предполагает, что этот фрейм относится к собственной сети VLAN коммутатора SW2, заданной в его конфигурации. Но если в конфигурации коммутатора SW2 задано, что собственной сетью VLAN в этой магистрали является сеть VLAN 2, то коммутатор SW2 предпринимает попытку перенаправить полученный фрейм в сеть VLAN 2.

Второй общий класс проблем при создании магистральных соединений заключается в том, что магистраль не создается в том интерфейсе, в котором это должно произойти. Наиболее вероятной причиной возникновения этой проблемы является то, что на противоположных концах канала настройка конфигурации магистрального соединения выполнена неправильно. Для указания на то, что должно быть создано магистральное соединение, и для определения правил согласования магистрального соединения служит подкоманда интерфейса `switchport mode {access | trunk | dynamic {desirable | auto}}`. Информацию о том, какой режим создания магистрального соединения задан в том или ином интерфейсе административно (в конфигурации) с помощью указанной команды настройки конфигурации, можно получить с использованием команды `show interface switchport`.

Удостоверьтесь, что знаете значение каждого из параметров команды конфигурации. Особенно плохо использовать на обоих концах комбинацию `dynamic auto`, что иногда является стандартной настройкой на некоторых коммутаторах Cisco. Эти параметры на обоих концах означают, что оба конца договорятся о магистральном соединении, если другой конец запустит процесс. В таком случае оба конца ожидают начала переговоров и никогда не сформируют магистральный канал. Параметры команды `switchport mode` и результирующий магистральный режим приведены в табл. 3.7.

Таблица 3.7. Ожидаемый рабочий режим магистрали на основании заданных административных режимов

Ключевая тема

Административный режим	access	dynamic auto	trunk	dynamic desirable
`access`	access	access	access	access
`dynamic auto`	access	access	trunk	trunk
`trunk`	access	trunk	trunk	trunk
`dynamic desirable`	access	trunk	trunk	trunk

В некоторых случаях попытка создания магистрального соединения на интерфейсе может окончиться неудачей из-за неправильной настройки в конфигурации типа магистрального соединения, иными словами, — из-за неправильного указания того, должен ли использоваться протокол ISL или 802.1Q. Например, если в двух коммутаторах на противоположных концах сегмента выполнена настройка конфигурации с помощью команд `switchport trunk encapsulation isl` и `switchport trunk encapsulation dot1Q` соответственно, то магистраль не формируется из-за несовпадения типов магистралей (инкапсуляции).

Примеры и упражнения на поиск и устранение неисправностей

Остальная часть этой главы посвящена в основном практическим занятиям. Решайте сами, хотите ли вы обучаться, больше читая, пытаясь найти ответы до чтения или, полагая, что материал главы абсолютно понятен, перейти к следующей главе.

Далее приведены два длинных примера применения концепций и процессов поиска и устранения неисправностей к локальным сетям. В первом примере приведена сеть LAN и множество команд `show`. Сеть LAN имеет проблемы конфигурации. Поэтому для локализации проблемы и нахождения первопричины проблем здесь используется четырехэтапный процесс, описанный в данной главе.

Второй пример, как и первый, начинается с той же сети LAN, но с устраненными проблемами. В данном примере задается вопрос: куда передаются фреймы в этой сети LAN? Далее пример рассматривает множество команд `show`, позволяющих выяснить это.

Для поиска и устранения неисправностей необходимы навыки, и эти примеры помогут их выработать. Одним из таких навыков является способность просмотреть текст вывода команды `show` и применить то, что он означает, к схеме сети. Эти два примера насчитывают 34 команды `show`, служащие в конечном счете единой цели. Данные примеры — последняя посвященная исключительно локальным сетям тема в подготовке к экзаменам CCNA, они помогут объединить множество концепций. Все части, вероятно, займут свои места, и вы поймете, что полностью овладели технологией LAN Ethernet.

Поиск и устранение неисправностей. Пример 1: поиск проблемы уровня данных существующих LAN

В первом примере приведена схема сети и набор примеров с выводом команд `show`. Пример занимает приблизительно 12 страниц. Его можно использовать одним из двух способов.

- **Обзор**. Прочитайте раздел, как обычно.
- **Упражнение**. Просмотрите рисунки и примеры, попытайтесь найти все проблемы и разработайте план их устранения. А именно: рассмотрите рис. 3.5 и примеры 3.7–3.14. Проигнорируйте текст и рис. 3.6 в конце данного примера. При чтении примеров, анализе вывода команд и их сравнении с рисунком найдите так много проблем, сколько сможете. Сравните свой список со списком в конце главы. Затем можно прочитать сам текст примеров, чтобы заполнить пробелы в знаниях.

В примере проводится исследование сети, представленной на рис. 3.5, с помощью вывода различных команд show. Здесь применяется тот же четырехэтапный процесс, обсуждаемый повсюду во втором разделе этой главы. В начале этого раздела для справки кратко повторены все этапы поиска и устранения неисправностей; подробней они описаны в разделе "Краткий обзор нормального процесса перенаправления на сетевом коммутаторе".

Тем, кто использует этот пример как упражнение, следует игнорировать текст и, рассматривая примеры вывода, искать проблемы. Остальные могут читать весь текст.

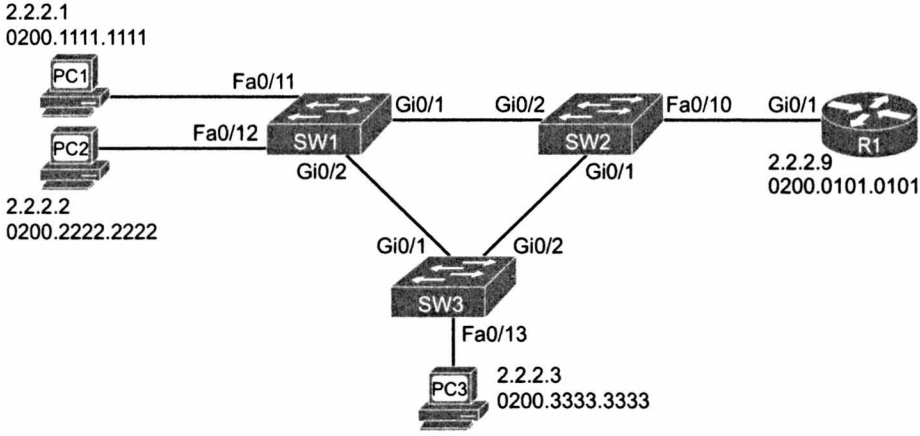


Рис. 3.5. Исходная схема сети первого примера поиска и устранения неисправностей

Этап 1. Проверка правильности схемы сети с помощью протокола CDP

В примере 3.7 приведен вывод нескольких вариантов команд show cdp neighbors и show cdp entry, полученный на трех коммутаторах, которые показаны на рис. 3.5. Достаточно провести простое сравнение, чтобы убедиться в правильности информации об именах и интерфейсах, приведенной на рис. 3.5, если не считать того, что, согласно этому выводу, к маршрутизатору R1 подключен интерфейс Fa0/9 коммутатора SW2, а не интерфейс Fa0/10 коммутатора SW2, как показано на рис. 3.5.

Пример 3.7. Проверка сведений, приведенных на рис. 3.5, с использованием протокола CDP

```
SW1# show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID    Local Intrfce  Holdtme  Capability    Platform      Port ID
SW2          Gig 0/1        170      S I           WS-C2960-     Gig 0/2
SW3          Gig 0/2        167      S I           WS-C2960-     Gig 0/1
! ------------------------------------------------------------------------
! Далее следуют команды для коммутатора SW2
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,
```

```
                D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID    Local Intrfce  Holdtme  Capability    Platform      Port ID
SW1          Gig 0/2        146      S I           WS-C2960-     Gig 0/1
SW3          Gig 0/1        162      S I           WS-C2960-     Gig 0/2
R1           Fas 0/9        139      R S I         CISCO2901     Gig 0/1

SW2# show cdp entry R1
-------------------------
Device ID: R1
Entry address(es):
    IP address: 2.2.2.9
Platform: Cisco CISCO2901/K9, Capabilities: Router Switch IGMP
Interface: FastEthernet0/9, Port ID (outgoing port): GigabitEthernet0/1
Holdtime : 148 sec

Version :
Cisco IOS Software, C2900 Software (C2900-UNIVERSALK9-M), Version
15.2(4)M1, RELEASE
SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Thu 26-Jul-12 20:54 by prod_rel_team

advertisement version: 2
VTP Management Domain: ''
Duplex: full
Management address(es):
! --------------------------------------------------------------------
! Далее следуют команды для коммутатора SW3
SW3# show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID    Local Intrfce  Holdtme  Capability    Platform      Port ID
SW1          Gig 0/1        167      S I           WS-C2960- Gig 0/2
SW2          Gig 0/2        176      S I           WS-C2960- Gig 0/1
```

Ошибка в документации, которая отражена на рис. 3.5 (в связи с чем указан интерфейс Fa0/10 коммутатора SW2 вместо Fa0/9), в настоящее время не влияет на функционирование сети. Но если бы потребовалось создать магистральное соединение между коммутатором SW2 и маршрутизатором R1, то нужно было бы явно задать в конфигурации интерфейс Fa0/9 коммутатора SW2, а не интерфейс Fa0/10, чтобы обеспечить создание магистрального соединения, поскольку маршрутизаторы не способны выполнять автоматическое согласование для использования магистрального соединения. В главе 4 подробно рассмотрена конфигурация магистрального соединения маршрутизатора.

Следует отметить, что протокол CDP не позволяет выявлять неточности в документации, касающиеся интерфейсов, которые предназначены для подключения персональных компьютеров конечных пользователей. Для дальнейшего выполнения настоящего примера предположим, что остальные интерфейсы обозначены на рис. 3.5 правильно.

Этап 2. Поиск проблем, связанных с интерфейсами

Следующий этап предусматривает проверку состояния интерфейса, который должен использоваться в сети. В примере 3.8 приведено несколько команд `show interface status`, выполненных в коммутаторах SW1 и SW3. (Для данной главы предположим, что все интерфейсы коммутатора SW2 функционируют правильно.) После введения команд необходимо исследовать полученный вывод, выявить все проблемы, о которых свидетельствуют рассматриваемые результаты, а также составить список прочих проблем, относящихся к интерфейсам, которые может потребоваться изучить дополнительно согласно этому выводу.

Пример 3.8. Проблемы, связанные с интерфейсами коммутаторов SW1 и SW3

```
SW1# show interfaces fa0/11 status

Port    Name      Status        Vlan   Duplex   Speed  Type
Fa0/11            connected     3      a-full   a-100  10/100BaseTX
SW1#show interfaces fa0/12 status

Port    Name      Status        Vlan   Duplex   Speed  Type
Fa0/12            notconnect    3      auto     auto   10/100BaseTX
SW1#show interfaces Gi0/1 status

Port    Name      Status        Vlan   Duplex   Speed  Type
Gi0/1             connected     trunk  a-full   a-1000 10/100/1000BaseTX
SW1# show interfaces Gi0/2 status

Port    Name      Status        Vlan   Duplex   Speed  Type
Gi0/2             connected     trunk  a-full   a-1000 10/100/1000BaseTX
! ------------------------------------------------------------------------
! Переключаемся на коммутатор SW3
SW3# show interfaces fa0/13 status

Port    Name      Status        Vlan   Duplex   Speed  Type
Fa0/13            connected     3      a-half   a-100  10/100BaseTX
SW3#show interfaces Gi0/1 status

Port    Name      Status        Vlan   Duplex   Speed  Type
Gi0/1             connected     trunk  a-full   a-1000 1000BaseTX
SW3# show interfaces Gi0/2 status

Port    Name      Status        Vlan   Duplex   Speed  Type
Gi0/2             connected     trunk  a-full   a-1000 1000BaseTX
```

Очевидно, что в коммутаторе SW1 обнаруживается определенная проблема, связанная с тем, что интерфейс Fa0/12 находится в состоянии "`notconnect`". Это состояние может возникнуть по многим причинам, но почти все они касаются тех или иных проблем с кабельной системой, начиная с того, что кабель не полностью вставлен в разъем коммутатора, и заканчивая трудно диагностируемыми проблемами, связанными с помехами в кабеле. (Перечень возможных причин приведен в табл. 3.2.)

На первый взгляд создается впечатление, будто в интерфейсах коммутатора SW3 не обнаруживаются какие-либо проблемы. Но во всех трех интерфейсах задано зна-

чение параметра дуплексной передачи, совпадающее с используемым на коммутаторе в случае неудачного завершения процесса автоматического согласования, причем особенно бросается в глаза то, что на интерфейсе Fa0/13 применяется полудуплексная передача. Это наводит на мысль о возможности возникновения одной из двух проблем с интерфейсами, указанных ранее в этой главе, которые могут обнаруживаться, даже если интерфейс находится в состоянии "connected", а именно — несоответствие режимов передачи.

Можно определить, что между интерфейсами Gigabit 0/1 и 0/2 коммутатора SW3 нет несоответствия, просто выполнив команду show interfaces status в коммутаторах SW1 и SW2 на других концах этих каналов соответственно. Но когда речь заходит о портах, подключенных к персональным компьютерам, то в процессе устранения нарушений в работе могут возникнуть сложности, связанные с удаленным расположением персональных компьютеров, в связи с чем потребуется поручить конечному пользователю компьютера выполнение некоторых этапов для проверки параметров скорости и дуплексной передачи. Но и без этого имеет смысл ознакомиться с такими наглядными признаками несогласованности параметров конфигурации, как возрастание количества карликовых фреймов, коллизий и запоздалых коллизий в счетчиках, показанных в выводе команды show interfaces, согласно примеру 3.9.

Пример 3.9. Признаки несоответствия режимов передачи

```
SW3# show interfaces fa0/13
FastEthernet0/13 is up, line protocol is up (connected)
    Hardware is Fast Ethernet, address is f47f.35cb.d78d (bia
f47f.35cb.d78d)
    MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
        reliability 255/255, txload 1/255, rxload 1/255
    Encapsulation ARPA, loopback not set
    Keepalive set (10 sec)
    Half-duplex, 100Mb/s, 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 never, 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: 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
        14507 packets input, 1003344 bytes, 0 no buffer
        Received 14488 broadcasts (466 multicasts)
        54 runts, 0 giants, 0 throttles
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
        0 watchdog, 466 multicast, 0 pause input
        0 input packets with dribble condition detected
        43824 packets output, 3440304 bytes, 0 underruns
        0 output errors, 114 collisions, 2 interface resets
        0 unknown protocol drops
        0 babbles, 78 late collision, 0 deferred
        0 lost carrier, 0 no carrier, 0 pause output
        0 output buffer failures, 0 output buffers swapped out
```

В данном случае имеет место рассогласование дуплекса с портом коммутатора, использующим полудуплексную передачу. Но следует учитывать, что значения этих счетчиков возрастают и при нормальной работе в условиях полудуплексной передачи, поэтому указанные счетчики не могут рассматриваться как безусловное свидетельство наличия проблем, связанных с несоответствием режимов передачи.

В этом случае конфигурация коммутатора SW3 должна быть изменена для использования полудуплексной передачи в интерфейсе Fa0/13, что привело к установлению соответствия с параметрами, заданными вручную на компьютере PC3.

Этап 3. Проверка наличия проблем режима безопасности порта

На следующем этапе проверяется конфигурация безопасности порта и состояние каждого коммутатора. Чрезвычайно удобно начинать процесс с выполнения команды `show port-security`, поскольку с ее помощью можно получить список интерфейсов, в которых включен режим (т.е. служба) безопасности порта. В примере 3.10 показано применение указанной команды наряду с некоторыми другими командами в коммутаторах SW1 и SW2. Обратите внимание на то, что в коммутаторах SW2 и SW3 не включена служба безопасности порта.

Изучите вывод команд в примере 3.10 и, прежде чем переходить к чтению пояснений к этому примеру, отметьте для себя, какие следующие этапы должны быть выполнены для устранения потенциальных проблем, связанных с защитой порта, и какую команду следует использовать для более точной локализации источника проблемы.

Пример 3.10. Применение защиты порта на коммутаторах SW1 и SW2

```
SW1# show port-security
Secure Port  MaxSecureAddr  CurrentAddr SecurityViolation Security Action
               (Count)        (Count)       (Count)
-------------------------------------------------------------------------
Fa0/11              1              1             97              Restrict
-------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 4096
!-----------------------------------------------------------------------
! Приведенные ниже данные о коммутаторе SW2 показывают, что ни в одном
! интерфейсе не включен режим безопасности порта.
SW2# show port-security
Secure Port  MaxSecureAddr  CurrentAddr SecurityViolation Security Action
               (Count)        (Count)       (Count)
-------------------------------------------------------------------------
-------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 8192
```

В этом примере команды `show port-security` применяются для получения сведений об интерфейсах, на которых задействована защита порта, а именно: в рассматриваемом случае служба запущена на интерфейсе Fa0/11 коммутатора SW1 и полностью выключена на коммутаторе SW2. При изучении полученных сведений о коммутаторе SW1 для поиска причин нарушений в работе следует обратить особое внимание на заголовок с определением действия по защите, который соответствует установленному параметру режима нарушения защиты и показывает, что выбрано

действие "restrict". В связи с тем, что задан этот параметр, интерфейс Fa0/11 коммутатора SW1 может находиться в состоянии "connected" (как показано в примере 3.8), при том, что служба защиты порта уничтожает трафик, не соответствующий конфигурации защиты порта. Таким образом, следует более подробно изучить конфигурацию защиты порта, как показано в примере 3.11.

Пример 3.11. Применение защиты порта на коммутаторах SW1 и SW2

```
SW1# show port-security interface fa0/11
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Restrict
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   : 0200.1111.1111:3
Security Violation Count   : 97
!
! Приведенные ниже данные конфигурации показывают, что заданный в
! конфигурации MAC-адрес не соответствует MAC-адресу компьютера PC1.
SW1# show running-config interface fa0/11

interface FastEthernet0/11
  switchport access VLAN 3
  switchport mode access
  switchport port-security
  switchport port-security violation restrict
  switchport port-security mac-address 0200.3333.3333
!
! Следующее журнальное сообщение также указывает на наличие проблемы,
связанной с защитой порта.
01:46:58: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation oc-
curred, caused by MAC
address 0200.1111.1111 on port FastEthernet0/11.
```

Этот пример начинается с проверки режима защиты и счетчика нарушений, а также с определения последнего MAC-адреса (0200.1111.1111), который применялся для отправки фрейма на интерфейс Fa0/11. Как показано во второй части примера, MAC-адрес компьютера PC1 (0200.1111.1111) не соответствует конфигурации защиты порта, а в конфигурации используется стандартное максимальное количество MAC-адресов, равное 1, и явно указан MAC-адрес 0200.3333.3333.

В качестве простого решения можно предложить корректировку конфигурации службы защиты порта, чтобы в конфигурации вместо этого был указан MAC-адрес компьютера PC1. Следует отметить, что инженеру не нужно выполнять команду shutdown, а затем — no shutdown применительно к этому интерфейсу для ввода интерфейса в действие после корректировки конфигурации, поскольку в конфигурации используется режим устранения нарушений "restrict", не требующий смены состояния "up" интерфейса и вместе с тем обеспечивающий удаление недопустимого входящего и исходящего трафиков компьютера PC1.

В конце этого примера показано сообщение системного журнала из числа сообщений, которые формируются коммутатором при каждом нарушении, если используется режим устранения нарушений "restrict". Эти журнальные сообщения отображаются на консоли или на устройстве, подключенном с помощью протокола Telnet или Secure Shell (SSH), с коммутатором, если удаленный пользователь ввел команду terminal monitor в сеансе удаленного соединения. Они могут также сохраняться на сервере системного журнала, как описано в главе 19.

Этап 4. Поиск проблем в сетях VLAN и магистралях

Этап 4А начинается с исследования интерфейсов доступа, что позволяет проверить, правильно ли назначены эти интерфейсы в сети VLAN. В данном случае, как показано на рис. 3.5, все интерфейсы, подключенные к персональным компьютерам и маршрутизаторам, должны быть назначены в сеть VLAN 3. В примере 3.12 показан вывод некоторых удобных команд show. Найдите время, чтобы внимательно ознакомиться с этим примером и определить наличие проблем, связанных с назначением в сеть VLAN.

Пример 3.12. Проверка назначений интерфейсов доступа в сеть VLAN

```
SW1# show interfaces fa0/11 status

Port    Name      Status        Vlan    Duplex   Speed  Type
Fa0/11            connected     3       a-full   a-100  10/100BaseTX

SW1#show interfaces fa0/12 status

Port    Name      Status        Vlan    Duplex   Speed  Type
Fa0/12            notconnect    3       auto     auto   10/100BaseTX
!--------------------------------------------------------------------------
! Далее рассматривается коммутатор SW2
SW2# show interfaces status
! Часть строк вывода опущена
Fa0/9             connected     1       a-full   a-100  10/100BaseTX
Fa0/10            notconnect    3       auto     auto   10/100BaseTX
!--------------------------------------------------------------------------
! Далее рассматривается коммутатор SW3
SW3# show interfaces fa0/13 status

Port    Name      Status        Vlan    Duplex   Speed  Type
Fa0/13            connected     3       full     a-100 10/100BaseTX
```

Единственной проблемой в этом случае является то, что, несмотря на назначение интерфейса Fa0/10 коммутатора SW2 в сеть VLAN 3 (см. рис. 3.5), коммутатор SW2 подключается к маршрутизатору R1 с использованием интерфейса Fa0/9 (как показывают данные, полученные с помощью протокола CDP, которые приведены в примере 3.7). Конфигурация интерфейса Fa0/9 определена так, что стандартно он должен находиться в сети VLAN 1. Таким образом, чтобы решить данную конкретную проблему, следует выполнить применительно к коммутатору SW2 подкоманду switchport access vlan 3 для интерфейса Fa0/9, чтобы внести изменение в конфигурацию.

На этапе 4Б предусмотрено проведение проверок сетей VLAN для определения, являются ли эти сети VLAN активными на каждом коммутаторе. Данный пример

фактически представляет собой продолжение предыдущего, и в нем используется только сеть VLAN 3, поэтому в примере 3.13 показано, что сеть VLAN 3 действительно известна на каждом коммутаторе. При изучении этого примера следует определить, имеют ли место какие-либо проблемы, связанные с сетью VLAN 3.

Пример 3.13. Проверка активных сетей VLAN

```
SW1# show vlan id 3

VLAN Name             Status    Ports
---- ---------------- --------- -------------------------------
3    book-vlan3       active    Fa0/11, Fa0/12, Gi0/1, Gi0/2
! Часть строк вывода опущена
!-------------------------------------------------------------------------
! Далее рассматривается SW2
SW2# 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
                                Fa0/11, 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
3    VLAN0003         active    Fa0/9, Fa0/10
! Часть строк вывода опущена
!-------------------------------------------------------------------------
! Далее рассматривается SW3
SW3# 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
                                 Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                 Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                 Fa0/22, Fa0/23, Fa0/24
9    book-vlan3       active    Fa0/13
! Часть строк вывода опущена
```

В данном случае сеть VLAN 3 существует и является активной во всех трех коммутаторах. Но коммутатор SW2 показывает имя, не совпадающее с именем, которое находится в выводе других двух коммутаторов. Однако определение имени не имеет значения с точки зрения функционирования сети VLAN, поэтому отмеченное различие несущественно.

Наконец, на этапе 4C предусмотрена проверка состояния магистральных соединений во всех интерфейсах, которые предназначены для использования в качестве магистральных. Кроме того, целесообразно определить, по каким магистралям должен перенаправляться трафик сетей VLAN. В примере 3.14 приведен вывод команд, который позволяет найти искомые ответы. Ознакомьтесь с данными, приведенными в этом примере, и, прежде чем приступить к чтению пояснений к примеру, составьте список магистралей, которые в настоящее время не перенаправляют

трафик сети VLAN 3, а также определите возможные причины, по которым сеть VLAN 3 исключена из магистрали.

Пример 3.14. Проверка магистральных соединений и сети VLAN 3

```
SW1# show interfaces trunk

Port        Mode         Encapsulation    Status    Native vlan
Gi0/1       desirable    802.1q           trunking  1
Gi0/2       desirable    802.1q           trunking  1

Port        Vlans allowed on trunk
Gi0/1       1-4094
Gi0/2       1-4094

Port        Vlans allowed and active in management domain
Gi0/1       1,3
Gi0/2       1,3

Port        Vlans in spanning tree forwarding state and not pruned
Gi0/1       3
Gi0/2       1,3
!--------------------------------------------------------------------------
! Ниже рассматривается коммутатор SW2
SW2# show interfaces trunk

Port      Mode    Encapsulation    Status      Native vlan
Gi0/1     auto    802.1q           trunking    1
Gi0/2     auto    802.1q           trunking    1

Port      Vlans allowed on trunk
Gi0/1     1-4094
Gi0/2     1-4094

Port      Vlans allowed and active in management domain
Gi0/1     1,3
Gi0/2     1,3

Port      Vlans in spanning tree forwarding state and not pruned
Gi0/1     1,3
Gi0/2     1
!--------------------------------------------------------------------------
! Ниже рассматривается коммутатор SW3
SW3# show interfaces trunk

Port    Mode         Encapsulation    Status      Native vlan
Gi0/1   auto         n-802.1q         trunking    1
Gi0/2   desirable    n-802.1q         trunking    1

Port    Vlans allowed on trunk
Gi0/1   1-4094
Gi0/2   1-4094

Port    Vlans allowed and active in management domain
Gi0/1   1,3
Gi0/2   1,3
```

```
Port      Vlans in spanning tree forwarding state and not pruned
Gi0/1     1,3
Gi0/2     1,3
```

Сначала посмотрите в конец вывода всех трех команд примера и сосредоточьтесь на сети VLAN 3. Все порты магистрального канала на этих коммутаторах указали сеть VLAN 3 в последнем списке VLAN, за одним исключением: порт G0/2 коммутатора SW2. Почему? Протокол STP решил блокировать сеть VLAN 3 на этом порту.

Несколько разных команд `show spanning-tree` могут подтвердить, что порт G0/2 коммутатора SW2 блокирован для сети VLAN 3, но в выводе примера можно также установить, что порт G0/2 коммутатора SW2 следует блокировать. Для этого достаточно исключить другие причины того, почему сеть VLAN 3 не была включена в списки вывода команд `show interfaces trunk` следующим образом.

- Сеть VLAN 3 выводится в первом списке VLAN вывода команды `show interfaces trunk` для коммутатора SW2, означая, что сеть VLAN 3 должна быть в списке дозволенных для этого магистрального канала.
- Сеть VLAN 3 выводится во втором списке VLAN вывода команды `show interfaces trunk` для коммутатора SW2, означая, что сеть VLAN 3 активна на коммутаторе SW2.

После выявления всех проблем в этом примере и их устранения обнаруживается, что в компьютерах PC1 и PC3 и в маршрутизаторе R1 может успешно выполняться эхо-тестирование всех устройств сети. С другой стороны, на компьютере PC2 обнаруживается неопределенное нарушение в работе, связанное с кабельной системой, поэтому работа по-прежнему невозможна.

Поиск и устранение неисправностей. Пример 2: прогноз поведения уровня данных

Во втором примере применен несколько иной подход, чем в первом. Он начинается с полностью работоспособной локальной сети. Задача заключается в анализе локальной сети и прогнозе перенаправления фреймов уровнем данных.

Фактически в данном примере используется та же сеть LAN, что и в предыдущем, но на сей раз все ошибки исправлены. В данном случае локальная сеть работоспособна, а пример сосредоточен на использовании команд для прогнозирования путей передачи фреймов. В частности, этот пример сосредоточен на двух сообщениях.

- Компьютер PC1 посылает запрос ARP на маршрутизатор R1 как широковещательный фрейм.
- Маршрутизатор R1 посылает ответ ARP на компьютер PC1 как одноадресатный фрейм.

В конце этого раздела представлены пути передачи запросов и ответов ARP для схем сетей, приведенных на рис. 3.6–3.8.

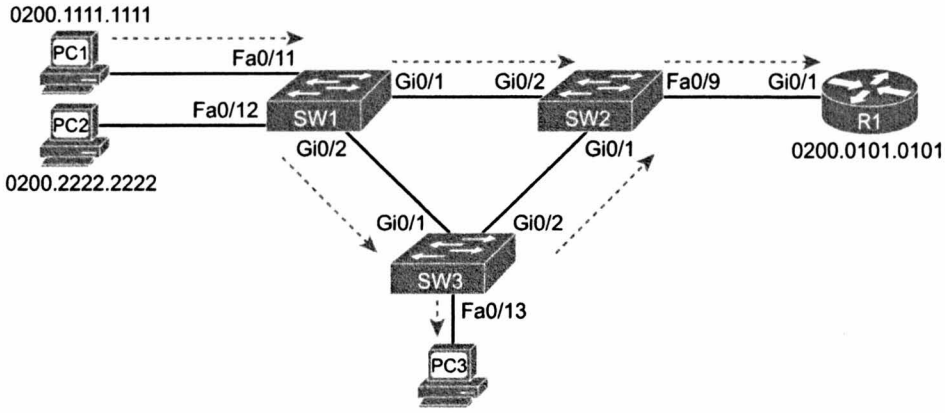


Рис. 3.6. Сеть для второго примера поиска и устранения неисправностей

ВНИМАНИЕ!

Сеть для этого примера использует тот же проект, что и предыдущий, но с исправленными ошибками. Все порты доступа находятся в сети VLAN 3.

Тем, кто желает использовать этот пример как практическое упражнение, следует использовать только рис. 3.6, игнорируя текст. Сделайте заметки о прогнозе путей передачи широковещательного сообщения ARP с компьютера PC1 и ответа ARP компьютеру R1. Если вы предпочитаете просто читать, то продолжайте чтение.

Широковещательное сообщение, переданное компьютером PC1

Когда компьютер PC1 должен будет послать пакет IP в другую подсеть, он передаст его на свой стандартный маршрутизатор. Его стандартным маршрутизатором в данном случае является маршрутизатор R1. Если компьютер PC1 не выводит MAC-адрес маршрутизатора R1 в кеше ARP, то он посылает широковещательное сообщение ARP на адрес Ethernet FFFF.FFFF.FFFF.

Чтобы изучить маршрут рассматриваемого широковещательного сообщения, вначале рассмотрим, как в целом осуществляется процесс перенаправления, в соответствии с информацией, приведенной выше в этой главе. Рассмотренные ранее примеры показали, что порт Fa0/11 коммутатора SW1 включен в сеть VLAN 3, а интерфейс Fa0/11 коммутатора SW1 является интерфейсом доступа. Фрейм, о котором идет речь, представляет собой широковещательное сообщение, поэтому коммутатор SW1 передает этот фрейм по принципу лавинной рассылки. С учетом этого факта в примере 3.15 приведен достаточный объем информации для того, чтобы можно было прогнозировать, через какие интерфейсы коммутатор SW1 перенаправит фрейм широковещательного сообщения, отправленный компьютером PC1, изучая вывод команды `show spanning-tree vlan 3 active`.

Пример 3.15. Список перенаправляющих интерфейсов коммутатора SW1 в сети VLAN 3

```
SW1# show spanning-tree vlan 3 active

VLAN0003
```

```
    Spanning tree enabled protocol ieee
    Root ID     Priority    20483
                Address     f47f.35cb.d780
                Cost        1
                Port        26 (GigabitEthernet0/2)
                Hello Time  2 sec Max Age 20 sec Forward Delay 15 sec

    Bridge ID   Priority    32771 (priority 32768 sys-id-ext 3)
                Address     1833.9d7b.0e80
                Hello Time  2 sec Max Age 20 sec Forward Delay 15 sec
                Aging Time  300
Interface        Role Sts Cost  Prio.Nbr   Type
---------------- ---- --- ----- ---------- --------------------------
Fa0/11           Desg FWD 19    128.11     P2p Edge
Fa0/12           Desg FWD 19    128.12     P2p
Gi0/1            Desg FWD 4     128.25     P2p
Gi0/2            Root FWD 1     128.26     P2p
```

Обратите внимание на то, что коммутатор SW1 не перенаправляет фрейм обратно через интерфейс Fa0/11, поскольку сам этот фрейм поступил в коммутатор через интерфейс Fa0/11. Кроме того, коммутатор SW1 перенаправляет фрейм через оба магистральных интерфейса (Gi0/1 и Gi0/2), а также Fa0/12. Более того, в примере 3.14 обнаруживаются свидетельства того, что в обеих магистралях коммутатора SW1 используется протокол 802.1Q, согласно которому в качестве *собственной* сети (native) применяется VLAN 1, поэтому коммутатор SW1 добавляет заголовок 802.1Q с указанием идентификатора сети VLAN 3 к каждой копии фрейма широковещательного сообщения, передаваемого по этим двум магистралям.

Изучив действия, выполняемые коммутатором SW1, можно сделать вывод, что копию фрейма широковещательного сообщения, отправленного компьютером PC1, должны получить и коммутатор SW2, и коммутатор SW3. Что касается коммутатора SW2, то он уничтожает относящуюся к нему копию фрейма широковещательного сообщения компьютера PC1, полученную через интерфейс Gi0/2 коммутатора SW2. Коммутатор SW2 уничтожает этот фрейм на этапе 3 общего процесса перенаправления, описанного ранее в главе, так как входящий интерфейс коммутатора SW2 (интерфейс Gi0/2) находится в состоянии блокирования в сети VLAN 3, как свидетельствует пример 3.16.

Пример 3.16. Коммутатор SW2: блокировка интерфейса Gi0/2 приводит к игнорированию входящих широковещательных фреймов

```
SW2# show spanning-tree vlan 3

VLAN0003
  Spanning tree enabled protocol ieee
  Root ID     Priority    20483
              Address     f47f.35cb.d780
              Cost        4
              Port        25 (GigabitEthernet0/1)
              Hello Time  2 sec Max Age 20 sec Forward Delay 15 sec

  Bridge ID   Priority    32771 (priority 32768 sys-id-ext 3)
              Address     1833.9d7b.1380
              Hello Time  2 sec Max Age 20 sec Forward Delay 15 sec
```

```
            Aging Time  300 sec

Interface        Role Sts Cost  Prio.Nbr   Type
---------------- ---- --- ----- ---------- ----------------------------
Fa0/9            Desg FWD 19    128.9      P2p
Gi0/1            Root FWD 4     128.25     P2p
Gi0/2            Altn BLK 4     128.26     P2p
```

Важно заметить, что применение состояния блокирования в коммутаторе SW2 не становится препятствием для отправки коммутатором SW1 фрейма коммутатору SW2; коммутатор SW2 получает отправленный ему фрейм, а затем уничтожает его без предупреждения.

Что же касается копии фрейма широковещательного сообщения, отправленного компьютером PC1, то коммутатор SW3 получает ее через свой интерфейс Gi0/1, после чего передает полученный фрейм по принципу лавинной рассылки. Коммутатор SW3 определяет, к какой сети VLAN относится фрейм, на основе заголовка 802.1Q входящего фрейма и обнаруживает, что входящий интерфейс находится в состоянии пересылки STP. С учетом этих фактов коммутатор SW3 перенаправляет фрейм в сеть VLAN 3. В примере 3.17 приведена информация, необходимая для определения, через какие интерфейсы коммутатор SW3 перенаправляет широковещательное сообщение сети VLAN 3.

Пример 3.17. Коммутатор SW3: перенаправление широковещательного сообщения сети VLAN 3

```
SW3# show mac address-table dynamic vlan 3
               Mac Address Table
-------------------------------------------
VLAN    Mac Address       Type        Ports
----    -----------       --------    -----
3       0200.0101.0101    DYNAMIC     Gi0/2
3       0200.1111.1111    DYNAMIC     Gi0/1
3       0200.2222.2222    DYNAMIC     Gi0/1
3       0200.3333.3333    DYNAMIC     Fa0/13
Total Mac Addresses for this criterion: 3

SW3# show spanning-tree vlan 3 active
VLAN0003
    Spanning tree enabled protocol ieee
    Root ID   Priority   20483
              Address    f47f.35cb.d780
              This bridge is the root
              Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

    Bridge ID Priority   20483 (priority 20483 sys-id-ext 3)
              Address    f47f.35cb.d780
              Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
              Aging Time 300

Interface        Role Sts Cost Prio.Nbr    Type
---------------- ---- --- ---- ---------- ------------------------------
Fa0/13           Desg FWD  19  128.13     P2p
Gi0/1            Desg FWD   4  128.25     P2p
Gi0/2            Desg FWD   4  128.26     P2p
```

Как и в случае коммутатора SW1, коммутатор SW3 не перенаправляет широковещательное сообщение через тот же интерфейс, в который поступил содержащий его фрейм (в данном случае через интерфейс Gi0/1), а передает этот фрейм по принципу лавинной рассылки через все прочие интерфейсы, относящиеся к той же сети VLAN и находящиеся в состоянии пересылки STP, а именно через интерфейсы Fa0/13 и Gi0/2. Кроме того, интерфейс Gi0/2 коммутатора SW3 в настоящее время используется в магистральном соединении 802.1Q, для которого собственной сетью является VLAN 1, поэтому коммутатор SW3 добавляет заголовок 802.1Q с указанием идентификатора сети VLAN 3.

Наконец, после получения коммутатором SW2 копии широковещательного сообщения, отправленного коммутатором SW3 через интерфейс Gi0/1 коммутатора SW2, коммутатор SW2 осуществляет тот же общий процесс перенаправления, что и другие коммутаторы. Коммутатор SW2 идентифицирует сеть VLAN на основании заголовка 802.1Q входящего фрейма, проверяет, находится ли входящий интерфейс в состоянии пересылки, и передает широковещательное сообщение через все остальные свои интерфейсы, которые находятся в состоянии пересылки и относятся к сети VLAN 3, по принципу лавинной рассылки. В данном случае коммутатор SW2 направляет фрейм только через интерфейс Fa0/9, подключенный к маршрутизатору R1. В примере 3.18 показан вывод вспомогательной команды.

Пример 3.18. Коммутатор SW2: перенаправление широковещательного сообщения, полученного от коммутатора SW3, в сети VLAN 3

```
! Прежде всего, следует отметить, что широковещательный
! адрес FFFF.FFFF.FFFF не находится в таблице MAC-адресов сети VLAN 3.
SW2# show mac address-table dynamic vlan 3
                    Mac Address Table
------------------------------------------
VLAN    Mac Address       Type        Ports
----    -----------       --------    -----
   3    000a.b7dc.b79a    DYNAMIC     Gi0/9
   3    0200.0101.0101    DYNAMIC     Fa0/1
   3    0200.2222.2222    DYNAMIC     Fa0/1
   3    0200.1111.1111    DYNAMIC     Gi0/1
   3    0200.3333.3333    DYNAMIC     Gi0/1
Total Mac Addresses for this criterion: 4

! Далее, заслуживает внимания то, что интерфейсы Fa0/9 и Gi0/1 находятся
! в состоянии перенаправления STP,а широковещательное сообщение поступило
! через интерфейс Gi0/1, поэтому коммутатор SW2 передает фрейм по
! принципу лавинной рассылки только через интерфейс Fa0/9.

SW2# show spanning-tree vlan 3 active
! Часть строк вывода команды опущена

Interface           Role    Sts    Cost        Prio.Nbr    Type
----------------    ----    ---    ---------   --------    -------------
Fa0/9               Desg    FWD    19          128.9       P2p
Gi0/1               Root    FWD    4           128.25      P2p
Gi0/2               Altn    BLK    4           128.26      P2p
```

Коммутатор SW2 не перенаправляет фрейм через интерфейс Gi0/1, поскольку сам фрейм был принят интерфейсом Gi0/1 коммутатора SW2.

Одноадресатный ответ ARP маршрутизатора R1

Ответ ARP от маршрутизатора R1 передается как одноадресатный фрейм. MAC-адресом получателя ответа ARP маршрутизатора R1 является MAC-адрес компьютера PC1. Путь приведен в конце раздела на рис. 3.8, это сделано специально, чтобы не подсказывать ответ тем, кто использует данный пример как упражнение.

Ответ ARP поступает во фрейме Ethernet, переданным на одноадресатный адрес Ethernet компьютера PC1: 0200.1111.1111. Получив фрейм от маршрутизатора R1, коммутатор SW2 обнаруживает, что фрейм поступил через интерфейс Fa0/9, представляющий собой интерфейс доступа в сети VLAN 3. В конце приведенного выше примера 3.18 показано, что интерфейс Fa0/9 находится в сети VLAN 3 в состоянии пересылки данных для протокола STP, поэтому коммутатор SW2 пытается перенаправить фрейм и не предпринимает попытки его уничтожить. Как будет показано в примере 3.19, в таблице MAC-адресов коммутатора SW2 указан MAC-адрес компьютера PC1 (0200.1111.1111), который доступен через интерфейс Gi0/1 и находится в сети VLAN 3, поэтому коммутатор SW2 перенаправляет фрейм через интерфейс Gi0/1 в коммутатор SW3.

Пример 3.19. Действия, выполняемые коммутатором SW2 при перенаправлении одноадресатного фрейма с известным адресатом компьютеру PC1

```
SW2# show mac address-table dynamic vlan 3
                Mac Address Table
------------------------------------------
VLAN    Mac Address       Type        Ports
----    -----------       --------    -----
3       0200.0101.0101    DYNAMIC     Fa0/9
3       0200.1111.1111    DYNAMIC     Gi0/1
3       0200.2222.2222    DYNAMIC     Gi0/1
3       0200.3333.3333    DYNAMIC     Gi0/1
3       f47f.35cb.d79a    DYNAMIC     Gi0/1
Total Mac Addresses for this criterion: 5
```

После получения коммутатором SW3 фрейма, отправленного коммутатором SW2, коммутатор SW3 обнаруживает, что фрейм поступил через интерфейс Gi0/2, т.е. через магистральный канал, а в его заголовке магистрального соединения указан идентификатор сети VLAN 3. В конце примера 3.17 уже было показано, что интерфейс Gi0/2 находится в состоянии пересылки STP в сети VLAN 3 (этап 3), поэтому коммутатор SW3 не уничтожает полученный фрейм в связи с тем, что этого не требует протокол STP. Как показано в примере 3.20, в таблице MAC-адресов коммутатора SW3 приведен MAC-адрес компьютера PC1 (0200.1111.1111), который доступен через интерфейс Gi0/1 и находится в сети VLAN 3, поэтому коммутатор SW3 перенаправляет фрейм через интерфейс Gi0/1 коммутатору SW1.

Пример 3.20. Действия коммутатора SW3 по перенаправлению одноадресатного фрейма с известным адресатом компьютеру PC1

```
SW3# show mac address-table dynamic vlan 3
                Mac Address Table
------------------------------------------
VLAN    Mac Address       Type        Ports
----    -----------       -------     -----
3       0200.0101.0101    DYNAMIC     Gi0/2
3       0200.1111.1111    DYNAMIC     Gi0/1
3       0200.2222.2222    DYNAMIC     Gi0/1
3       0200.3333.3333    DYNAMIC     Fa0/13
Total Mac Addresses for this criterion: 3
```

После получения коммутатором SW1 фрейма от коммутатора SW3 коммутатор SW1 обнаруживает, что фрейм поступил через интерфейс Gi0/2, т.е. через магистральный канал, а в его заголовке магистрального соединения указан идентификатор сети VLAN 3. В конце примера 3.15 уже было показано, что интерфейс Gi0/2 коммутатора SW1 находится в состоянии пересылки STP в сети VLAN 3, поэтому коммутатор SW1 не уничтожает фрейм по той причине, что интерфейс не находится в состоянии пересылки STP. Как показано в примере 3.21, в таблице MAC-адресов коммутатора SW1 указан MAC-адрес компьютера PC1 (0200.1111.1111), как доступный через интерфейс Fa0/11 и находящийся в сети VLAN 3, поэтому коммутатор SW1 перенаправляет фрейм через интерфейс Fa0/11 компьютеру PC1. В данном случае коммутатор SW1 удаляет заголовок сети VLAN, соответствующий протоколу 802.1Q, поскольку интерфейс Fa0/11 представляет собой интерфейс доступа.

Пример 3.21. Действия коммутатора SW1 по перенаправлению одноадресатного фрейма с известным адресатом компьютеру PC1

```
SW1# show mac address-table dynamic vlan 3
                Mac Address Table
------------------------------------------
VLAN    Mac Address       Type        Ports
----    -----------       --------    -----
3       0200.2222.2222    DYNAMIC     Fa0/12
3       0200.3333.3333    DYNAMIC     Gi0/2
3       f47f.35cb.d799    DYNAMIC     Gi0/2
Total Mac Addresses for this criterion: 3

SW1# show mac address-table vlan 3
Mac Address Table
------------------------------------------
VLAN    Mac Address       Type        Ports
----    -----------       -------     -----
All     0100.0ccc.cccc    STATIC      CPU
All     0100.0ccc.cccd    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
3        0200.1111.1111    STATIC    Fa0/11
3        0200.2222.2222    DYNAMIC   Fa0/12
3        0200.3333.3333    DYNAMIC   Gi0/2
3        f47f.35cb.d799    DYNAMIC   Gi0/2
Total Mac Addresses for this criterion: 24
```

При изучении этого последнего этапа необходимо отметить важный факт, касающийся таблицы MAC-адресов и защиты порта. Обратите внимание на то, что в выводе команды `show mac address-table dynamic`, выполненной применительно к коммутатору SW1, не указан MAC-адрес компьютера PC1 (0200.1111.1111), а это могло бы навести на мысль, что коммутатор SW1 передает фрейм по принципу лавинной рассылки, поскольку фрейм является одноадресатным фреймом с неизвестным адресатом. Тем не менее в конфигурации коммутатора SW1 выполнена настройка режима безопасности порта применительно к интерфейсу Fa0/11, в том числе выполнена подкоманда интерфейса `switchport port-security mac-address 0200.1111.1111`, поэтому в IOS коммутатора этот MAC-адрес рассматривается как статический. Поэтому после удаления ключевого слова "`dynamic`" в выводе команды `show mac address-table vlan 3` обнаруживаются все известные MAC-адреса в этой сети VLAN, в том числе 0200.1111.1111. Вывод этой команды подтверждает, что коммутатор SW1 перенаправляет одноадресатный фрейм с адресом 0200.1111.1111 только через интерфейс Fa0/11.

На рис. 3.7 показан путь передачи запроса ARP (широковещание) через этот LAN, а на рис. 3.8 — путь одноадресатного ответа ARP.

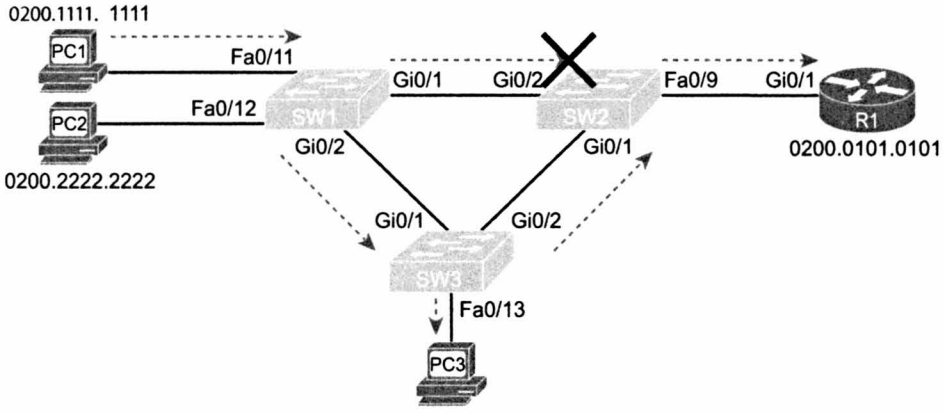


Рис. 3.7. Путь передачи запроса ARP (широковещание) с компьютера PC1 на маршрутизатор R1

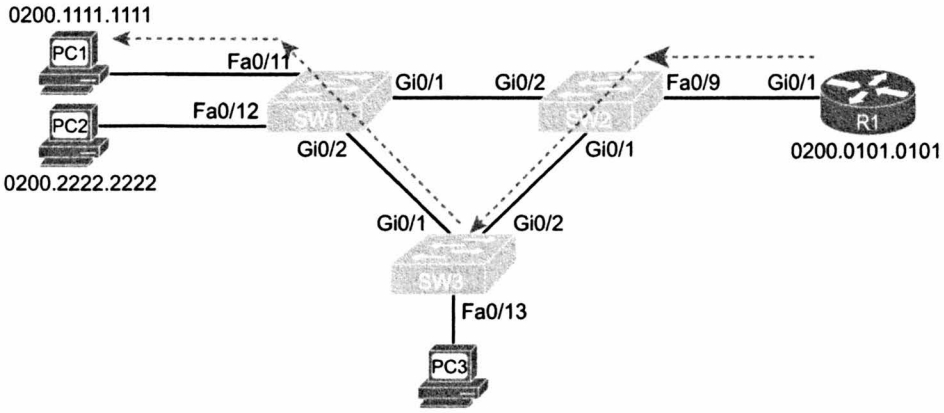


Рис. 3.8. Путь передачи ответа ARP (широковещание) с маршрутизатора R1 на компьютер PC1

Обзор

Резюме

- Каждый, кто сталкивается с необходимостью устранить ту или иную сетевую проблему, вынужден использовать определенную методологию поиска неисправностей.
- Методология поиска неисправностей включает анализ и прогнозирование нормальной работы, локализацию проблемы и анализ первопричин.
- При поиске неисправностей на уровне данных последовательно рассматривается каждое устройство в предполагаемом пути перенаправления данных.
- Многие процессы уровня управления непосредственно затрагивают тот или иной процесс уровня данных.
- Процессы уровня управления слишком разнообразны, поэтому возможность предложить для них подобный обобщенный процесс поиска неисправностей отсутствует.
- Процесс поиска и устранения неисправностей подразумевает нахождение первопричины проблемы и ее устранение.
- При анализе первопричины стремятся выявить конкретное устройство и функцию, подлежащую внесению исправлений.
- При поиске и устранении неисправностей уровня данных коммутируемой сети LAN можно рассмотреть процессы уровня данных на уровнях 1 и 2.

Ключевые темы

Повторите все ключевые темы данной главы, отмеченные пиктограммой "Ключевая тема". Ключевые темы и соответствующие им страницы приведены в табл. 3.8.

Таблица 3.8. Ключевые темы главы 3

Элемент	Описание	Страница
Табл. 3.2	Коды состояния интерфейса сетевого коммутатора	134
Рис. 3.4	Пример использования перекрестных кабелей и кабелей с прямыми соединениями	135
Табл. 3.3	Используемые пары выводов в сетях 10BASE-T и 100BASE-T	136
Список	Определения рассогласования скорости и рассогласования дуплекса	138
Список	Рекомендации по обнаружению проблем рассогласования режимов передачи	139
Список	Стандартные варианты выбора режима дуплексной передачи на основе автоматического согласования по стандарту IEEE с учетом текущей скорости	140
Табл. 3.4	Действия, предпринимаемые средствами защиты порта, в зависимости от установленного режима устранения нарушений	142

Окончание табл. 3.8

Элемент	Описание	Страница
Список	Этапы настройки защиты порта	144
Табл. 3.5	Команды, позволяющие находить порты доступа и сети VLAN	146
Табл. 3.6	Сети VLAN, выводимые командой show interfaces trunk	148
Табл. 3.7	Ожидаемый рабочий режим магистрали на основании заданных административных режимов	149

Заполните таблицы и списки по памяти

Распечатайте приложение Г с веб-сайта или его раздел, относящийся к этой главе, и заполните таблицы и списки по памяти. В приложении Д приведены заполненные таблицы и списки для самоконтроля.

Ответы на задачи примера 1 по поиску и устранению неисправностей

Для тех, кто использовал пример 1 по поиску и устранению неисправностей как упражнение, ниже приведен список проблем, возможно раскрытых в этом упражнении.

- На рис. 3.5 представлен порт Fa0/10 коммутатора SW2, соединенный с маршрутизатором R1, в то время как протокол CDP показал, что в действительности используется порт F0/9 коммутатора SW2. Проблема устранена заменой порта на схеме сети на Fa0/9.
- Согласно рис. 3.5, порт F0/12 коммутатора SW1 соединен с компьютером PC2 и, по-видимому, находится в состоянии `notconnect`. Примеры не могли указать конкретную причину состояния `notconnect`. (В действительности был отключен кабель; он был подключен при подготовке ко второму примеру.)
- Порт Fa0/13 коммутатора SW3, вероятно, находится в состоянии рассогласования дуплекса. В выводе указан параметр скорости/дуплекса `a-100/a-half`, что может случиться при отключении автопереговоров на другом устройстве (PC13) и установке для него параметров `100/full`. Проблема была устранена установкой вручную дуплексного режима на коммутаторе.
- Защита порта F0/11 на коммутаторе SW1 отфильтровывает трафик от единственного соединенного с ним устройства (компьютера PC1, 0200.1111.1111) из-за неправильной настройки MAC-адреса 0200.3333.3333. Настройка защиты порта была изменена на правильный MAC-адрес 0200.1111.1111.
- Порт F0/9 коммутатора SW2, фактически соединенный с маршрутизатором R1, присваивается сети VLAN 1, в то время как порт F0/10, представленный на рис. 3.5 как подключенный к маршрутизатору R1, назначен (правильно) сети VLAN 3. Следует либо переключить кабель, либо порт F0/9 должен быть перемещен в сеть VLAN 3. В данном случае изменена конфигурация порта F0/9 коммутатора SW2 командой `switchport access vlan 3`.

Обзор части I

Проследите свой прогресс изучения материала части по контрольному списку в следующей таблице. Подробно задачи описаны ниже.

Контрольный список обзора части I

Задача	Первая дата завершения	Вторая дата завершения
Повторите вопросы из обзоров глав		
Ответьте на вопросы обзора части		
Повторите ключевые темы		
Создайте диаграмму связей концепций STP		

Повторите вопросы из обзоров глав

Ответьте снова на вопросы обзоров глав этой части книги, используя программное обеспечение PCPT. Инструкция по запуску программного обеспечения PCPT с вопросами обзоров глав только этой части приведена в разделе "Как просмотреть вопросы только обзоров глав конкретной части" введения к книге.

Ответьте на вопросы обзора части

Ответьте на вопросы обзора этой части книги, используя программное обеспечение PCPT. Инструкция по запуску программного обеспечения PCPT с вопросами обзоров только этой части приведена в разделе "Как просмотреть вопросы только обзоров частей" введения к книге.

Повторите ключевые темы

Снова просмотрите темы прочитанных глав, отмеченные пиктограммой "Ключевая тема". Если понятны не все их подробности, уделите время повторному изучению.

Создайте диаграмму связей концепций протокола STP

Протокол распределенного связующего дерева (STP) определяет много концепций, которые имеет смысл организовать в памяти. В этом может помочь создание диаграммы связей, организующей концепции протокола STP в три категории, следующим образом.

Правила. Сюда относятся все правила, используемые коммутатором при выборе (например, правила выбора корневого коммутатора).

Роли. Протокол STP определяет и роли, и состояния; пример роли — роль корневого порта.

Состояния. Пример состояния — перенаправление.

Создайте диаграмму связей с тремя ветвями (правила, роли и состояния) и заполните их таким количеством соответствующих концепций, сколько сможете вспомнить.

ВНИМАНИЕ!

Подробную информацию по этой теме см. в разделе "О диаграммах связей" введения к данной книге.

Создайте диаграммы связей из таблицы ниже на бумаге или с помощью любого графического программного обеспечения. Если используется программное обеспечение, имеет смысл сохранить результат в файле для последующего анализа. Ответы приведены в приложении E на веб-сайте, но ваши диаграммы связей могут выглядеть иначе.

Диаграммы связей обзора части I

Диаграмма	Описание	Где сохранен результат
1	Диаграмма связей концепций STP	

И наконец, помните о следующих важных моментах при работе над этим проектом.

- Самообучение в этом упражнении осуществляется, по большей части, при его выполнении; конечно, заманчиво перейти к примеру диаграмм в приложении E, но это не поможет в обучении.
- Используйте по возможности меньше слов, достаточно лишь напомнить мысль. Не пытайтесь писать полные фразы или предложения.
- Не заглядывайте сразу в книгу или в свои заметки. Постарайтесь составить диаграмму связей по памяти и только затем обратитесь к своим записям.
- Позже повторите это упражнение, с начала без заметок, а впоследствии еще раз для улучшения памяти и умственных способностей.

Часть II несколько отступает от тем по сетям LAN и сосредоточивается на темах маршрутизации IPv4. Книга по экзамену ICND1 ознакомила со многими подробностями маршрутизации IPv4 (общими концепциями, математическим механизмом и подробностями реализации подсетей на маршрутизаторах), а настоящая часть этой книги продолжает рассмотрение данных тем. В этой части содержится обзор тем по перенаправлению IPv4 из книги по ICND1, но теперь основное внимание уделяется поиску и устранению неисправностей в объединенных сетях IPv4, а главы 4 и 5 полностью посвящены теме поиска и устранения неисправностей маршрутизации IPv4.

Последние две главы части знакомят с новыми темами, не рассматриваемыми в первом, посвященном экзамену ICND1, томе этой книги, а также с двумя темами, несвязанными с маршрутизацией IPv4. В главе 6 представлена идея избыточных стандартных маршрутизаторов, а в главе 7 обсуждается создание частного сетевого соединения с использованием IPv4 поверх Интернета.

Часть II. Маршрутизация IP версии 4

Глава 4. “Поиск и устранение неисправностей маршрутизации IPv4. Часть I”

Глава 5. “Поиск и устранение неисправностей маршрутизации IPv4. Часть II”

Глава 6. “Создание резервного маршрутизатора первого транзитного участка”

Глава 7. “Виртуальные частные сети”

Обзор части II

Глава 4

Поиск и устранение неисправностей маршрутизации IPv4. Часть I

Маршрутизация IPv4 требует взаимодействия хостов и маршрутизаторов. Сначала хосты создают пакеты IPv4 и посылают их на некий соседний маршрутизатор (стандартный маршрутизатор хоста, или стандартный шлюз). Затем маршрутизатор принимает решение о маршрутизации, т.е. куда перенаправить пакет IPv4 далее, и посылает пакет по соответствующему физическому каналу связи. Каждый маршрутизатор, получающий пакет IPv4, повторяет процесс до тех пор, пока пакет наконец не достигнет хоста получателя.

Эта глава посвящена поиску и устранению неисправностей маршрутизации IPv4. В частности, она детально рассматривает перенаправление пакета (т.е. на уровне данных IPv4). По большей части, данная глава не рассматривает проблемы канала связи и физического уровня, оставляя их части I (локальные сети) и части IV (глобальные сети), и сосредоточивается на функциях сетевого уровня маршрутизации IP. В главе не рассматриваются также проблемы уровня управления IPv4, в частности, проблемы протоколов маршрутизации IP рассматриваются в части III (протоколы маршрутизации IP версии 4) этой книги.

Чтобы помочь вам в поиске и устранении неисправностей маршрутизации IPv4, в этой главе приведен обзор концепций маршрутизации IPv4. Компания Cisco отнесла большинство концепций маршрутизации IPv4, а также темы по настройке и проверке к экзамену ICND1, а не CCNA, но поиск и устранение неисправностей по тем же темам относится к ICND2. В результате эта книга содержит главы по поиску и устранению неисправностей IPv4, а также периодические обзоры темы IPv4.

Настоящая глава разделена на три основных раздела, представляющих информацию о сети с точки зрения поиска и устранения неисправностей. В первом разделе содержится обзор маршрутизации IPv4 на хостах и маршрутизаторах (это поможет предсказать нормальное поведение сети при поиске и устранении неисправностей). Во втором разделе обсуждается команда `ping`, а именно: как она позволяет локализовать проблему все в меньших и меньших областях сети, пока не будет найдена первопричина проблемы. Заключительный раздел посвящен команде `traceroute`, имеющей ту же цель, что и команда `ping`: поиск способов локализации проблемы.

В этой главе рассматриваются следующие экзаменационные темы

Поиск и устранение неисправностей

Поиск и устранение наиболее распространенных проблем сети

Поиск и устранение проблем маршрутизации

- Разрешение маршрутизации
- Правильность таблицы маршрутизации
- Выбор правильного пути

Основные темы

Предсказание нормального поведения при направлении IPv4

Люди решают сетевые проблемы разными способами. И ни один из способов не может претендовать на роль лучшего во всех случаях. Но, как упоминалось в главе 3, при поиске и устранении неисправностей имеет смысл выработать некий системный подход. Таким образом, эта глава (равно как и другие разделы этой книги по поиску и устранению неисправностей) подходит к проблемам согласно той же общей стратегии.

1. Предсказать нормальную работу.
2. Постараться локализовать проблему до как можно более специфической причины, а если возможно, то и до конкретного устройства.
3. Обнаружить и устранить первопричину проблемы.

Первый основной раздел этой главы посвящен обзору маршрутизации IPv4, согласно первому этапу процесса поиска неисправности: предсказание нормальной цепи событий при передаче пакета IPv4 с одного хоста на другой.

Так как же работает маршрутизация IPv4? Если сосредоточиться на логике сетевого уровня, то любая объединенная сеть может быть представлена как набор этапов маршрутизации. Первый этап начинается с создания и передачи хостом пакета своему стандартному маршрутизатору. По достижении маршрутизатора пакет передается через один или несколько маршрутизаторов, пока не прибудет к месту назначения (первые три этапа на рис. 4.1).

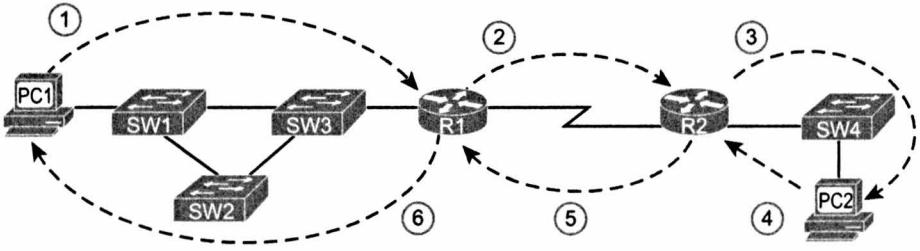


Рис. 4.1. Основные этапы маршрутизации IP

На первых трех этапах в примере на рис. 4.1 осуществляется перенаправление пакета по объединенной сети. Но большинство приложений требует передачи пакетов в обоих направлениях. Таким образом, анализ нормальной работы при поиске и устранении неисправностей также должен учитывать передачу пакетов назад, к первому хосту (в данном случае PC1), как демонстрируют этапы 4–6 на рисунке.

Чтобы доставить пакет IPv4 с одного хоста на другой и назад, хосты и маршрутизаторы должны взаимодействовать. Данный раздел разделяет логику маршрутизации на логику хоста и логику маршрутизатора.

Логика перенаправления IPv4, используемая на хостах

Процесс маршрутизации IPv4 начинается с хоста, создающего пакет IP. После того как хост создаст пакет IP, он задает себе вопрос: находится ли IP-адрес получателя нового пакета в моей же локальной подсети? Чтобы определить диапазон адресов в локальной подсети, хост использует собственный IP-адрес и маску, сравнивает этот диапазон с IP-адресом получателя, а потом действует следующим образом.

Логика перенаправления хоста

Ключевая тема

Этап 1 Если получатель находится в локальной сети, передает пакет непосредственно.

A. Находит MAC-адрес хоста получателя, используя записи таблицы ARP, если адрес уже известен, или сообщения ARP в противном случае.

B. Инкапсулирует пакет IP во фрейм канала связи с адресом канала связи *хоста получателя*

Этап 2 Если получатель находится не в локальной сети, передать пакет на стандартный маршрутизатор (стандартный шлюз).

A. Находит MAC-адрес стандартного маршрутизатора, используя записи таблицы ARP, если адрес уже известен, или сообщения ARP в противном случае.

B. Инкапсулирует пакет IP во фрейме канала связи с адресом канала связи *стандартного маршрутизатора*

Подробности логики перенаправления IPv4 хоста представлены на рис. 4.2. Как принимается решение, показано на рис. 4.2, *слева*? На рисунке представлен хост A, непосредственно передающий пакет локальному хосту D. Но пакет к хосту B, находящемуся с другой стороны маршрутизатора, а следовательно, в подсети, отличной от подсети хоста A, он посылает своему стандартному маршрутизатору (R1).

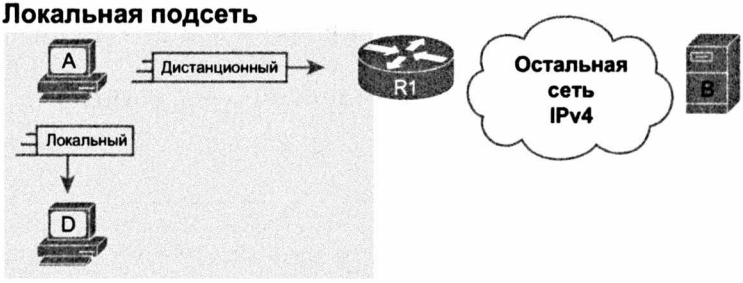


Рис. 4.2 Логика перенаправления хоста

Логика перенаправления IPv4, используемая на маршрутизаторах

Поскольку маршрутизаторы работают независимо, процесс маршрутизации одиночного пакета требует, чтобы маршрутизатор прошел собственную логическую последовательность без помощи любого другого маршрутизатора.

В то же время маршрутизаторы взаимодействуют друг с другом. Маршрутизаторы один за другим перенаправляет пакет так, чтобы он в конечном счете достиг нужного хоста получателя. Перенаправляя пакет по одному транзитному участку всего маршрута к хосту получателя, каждый маршрутизатор действует независимо.

В следующем разделе обсуждается работа маршрутизаторов по перенаправлению пакетов. Сначала как независимый процесс на одном маршрутизаторе, а затем в общем.

Логика перенаправления IP на одном маршрутизаторе

По сравнению с хостами, у маршрутизаторов немного больше работы с маршрутизируемыми пакетами IPv4. В то время как логика хоста начинается с находящегося в памяти пакета IP, маршрутизатору придется проделать некоторую работу, прежде чем перейти в состояние, с которого можно начинать самую важную часть: поиск соответствия в таблице маршрутизации IP. Собственно этапы маршрутизации таковы.

Ключевая тема **Логика перенаправления маршрутизатора**

Этап 1 Принять решение по каждому полученному фрейму канала связи, стоит ли его обрабатывать. Фрейм следует обработать, если:

A. У фрейма нет никаких ошибок (определяется по контрольной сумме фрейма в концевике канала связи или по полю FCS).

B. Адрес получателя фрейма канала связи — это адрес самого маршрутизатора (многоадресатный либо широковещательный адрес)

Этап 2 Если на этапе 1 решено обработать фрейм, то извлекает пакет из фрейма канала связи

Этап 3 Принимается решение о маршрутизации. Для этого IP-адрес получателя пакета сравнивается с записями в таблице маршрутизации и находится маршрут, соответствующий адресу получателя. Маршрут указывает исходящий интерфейс маршрутизатора, а возможно, и следующий транзитный маршрутизатор

Этап 4 Пакет инкапсулируется во фрейм канала связи, соответствующий исходящему интерфейсу. При перенаправлении через интерфейсы Ethernet LAN может потребоваться применение протокола ARP, если MAC-адреса следующего устройства нет в кеше ARP маршрутизатора

Этап 5 Передать фрейм через исходящий интерфейс, указанный в соответствующем маршруте IP

ВНИМАНИЕ!

Номера этапов этого списка не имеют значения, важны концепции, применяемые на каждом этапе. Запомните их! На экзамене важны только концепции, а не номера этапов.

Это описание изложено подробно и точно, однако упрощенно процесс маршрутизации можно описать одним предложением:

Маршрутизатор получает фрейм, извлекает пакет из фрейма, выбирает интерфейс для перенаправления пакета, помещает пакет в другой фрейм и передает фрейм (с пакетом) через соответствующий интерфейс маршрутизатора.

Хотя читать о процессе маршрутизации тоже полезно, рисунок позволит сделать его нагляднее. На рис. 4.3 процесс маршрутизации разделен на те же пять этапов, причем пакет поступает на маршрутизатор слева, а покидает справа. Пакет поступает на интерфейс Ethernet, IP-адрес которого указан хостом B как адрес получателя. Как показано на рисунке, маршрутизатор R1 обрабатывает фрейм и пакет согласно

описанному ранее процессу маршрутизации из пяти этапов, причем номера на рисунке соответствуют номерам этапов. В конечном счете маршрутизатор перенаправляет пакет в новом фрейме HDLC через последовательный канал справа.

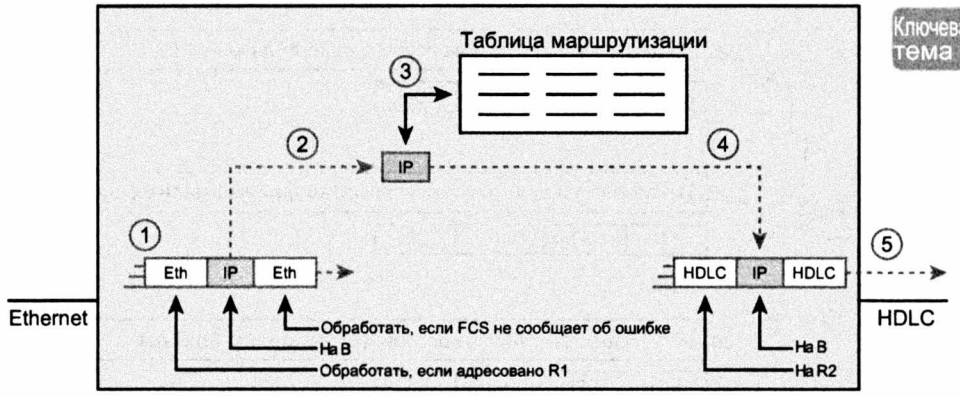


Рис. 4.3. Логика перенаправления маршрутизатора

Маршрутизация IP от хоста до хоста

До сих пор речь шла о логике маршрутизации на одиночном маршрутизаторе с тремя разными представлениями процесса: подробное и краткое текстовые описания процесса и схема. Но логика на одном маршрутизаторе не обеспечит доставки пакета через всю объединенную сеть IP. Сквозная передача требует использования всеми маршрутизаторами одинаковой логики, обеспечивающей перенаправление каждым маршрутизатором пакета следующему и следующему маршрутизатору, пока пакет не достигнет получателя.

На рис. 4.4 представлена сквозная маршрутизация пакета, с его извлечением (этап 2) и инкапсуляцией (этап 4) каждым маршрутизатором. Каждый маршрутизатор отбрасывает заголовок и концевик канала связи входящего фрейма, поскольку каждый фрейм перемещается только от хоста до маршрутизатора или между маршрутизаторами. Перенаправляя пакет, каждый маршрутизатор добавляет новый заголовок и концевик канала связи, создавая каждый раз новый фрейм. Поле адреса в заголовке канала связи также имеет значение только на данном локальном канале связи.

На рисунке, где компьютер PC1 передает пакет на компьютер PC2, показаны разные представления фреймов. Сверху на рисунке компьютер PC1 передает фрейм Ethernet маршрутизатору R1. Маршрутизатор R1 извлекает (деинкапсулирует) пакет и снова помещает (инкапсулирует) его во фрейм HDLC. Маршрутизатор R2 повторяет тот же процесс, но на сей раз инкапсулируя пакет во фрейм Frame Relay. Маршрутизатор R3 также повторяет процесс, инкапсулируя пакет во фрейм Ethernet и передавая его на компьютер PC2.

Ключевая тема

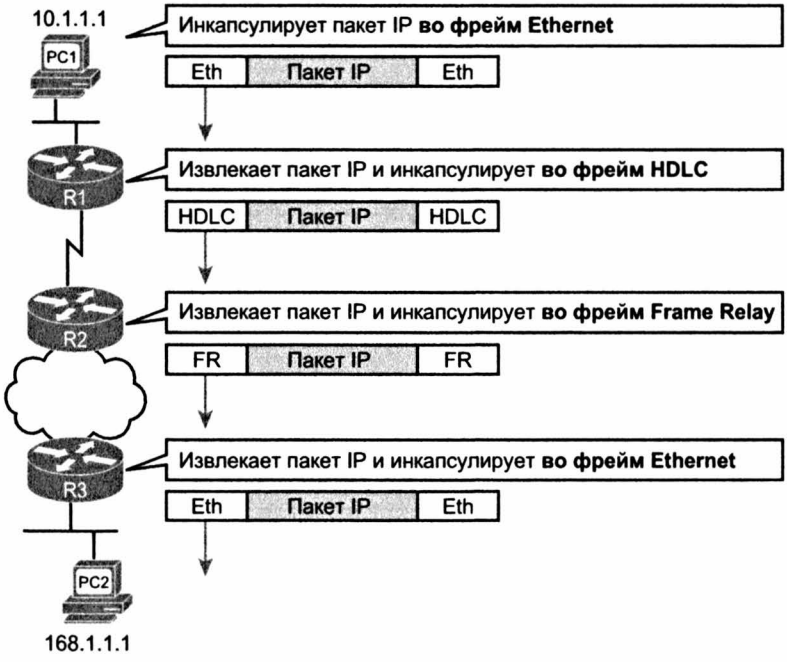


Рис. 4.4. Инкапсуляция и деинкапсуляция пакета при маршрутизации

Создание новых заголовков канала связи с использованием информации ARP

Другой важной частью процесса маршрутизации является выбор адреса канала связи, используемого в новом заголовке канала связи. Заголовки канала связи обычно содержат адрес, как MAC-адрес в заголовке канала связи Ethernet. Чтобы инкапсулировать пакет IP и передать его по некоторым типам каналов связи, маршрутизатор должен сначала узнать адрес устройства на другом конце канала связи. Например, маршрутизатор R3 (см. рис. 4.4, *снизу*) должен знать MAC-адрес компьютера PC2 прежде, чем он сможет создать и послать ему одноадресатный фрейм Ethernet.

Для обеспечения процесса изучения MAC-адресов других устройств в локальных сетях протокол IPv4 использует *протокол преобразования адресов* (ARP). Протокол ARP определяет два сообщения (запрос ARP и ответ ARP). Посылающий хост или маршрутизатор использует запрос ARP со следующим смыслом: "Если это ваш IP-адрес, сообщите мне ваш MAC-адрес". Второй хост отсылает ответ ARP, содержащий его IPv4-адрес и MAC-адрес Ethernet. Например, на рис. 4.5 представлен процесс ARP, происходящий в той же сети, что и на рис. 4.4, прежде, чем маршрутизатор R3 сможет перенаправить пакет (инкапсулируемый во фрейме) по MAC-адресу компьютера PC2.

Темы экзаменов CCENT и CCNA включают только один протокол канала связи LAN (Ethernet) и три протокола канала связи WAN (HDLC, PPP и Frame Relay). Протокол Ethernet использует протокол ARP, как показано на рис. 4.5. Протоколы HDLC и PPP, используемые в последовательных каналах двухточечной топологии, не нуждаются в функции протокола ARP. Протокол Frame Relay использует подобную функцию под названием Inverse ARP, рассматриваемую в главе 13.

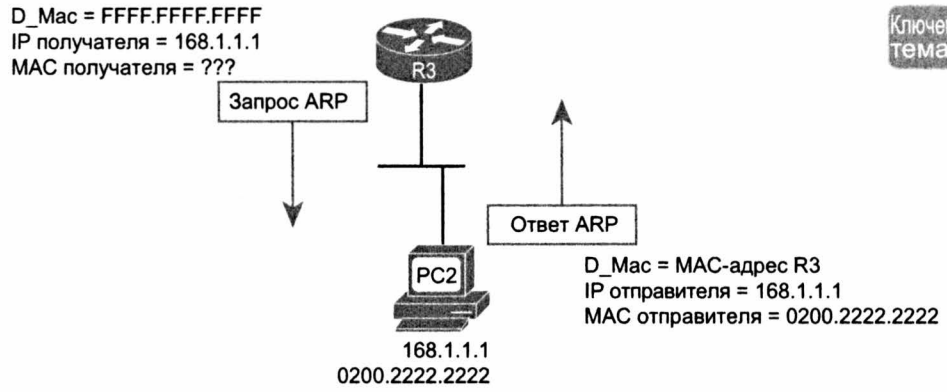


Рис. 4.5. Пример процесса ARP

Таким образом, когда адрес получателя пакета находится в другой подсети, хосты перенаправляют пакеты своим стандартным маршрутизаторам. Каждый маршрутизатор извлекает пакет, решает, куда его перенаправить, и инкапсулирует пакет в новый фрейм канала связи. От хоста отправителя к хосту получателя доходит только пакет IP, а все заголовки и концевики канала связи служат лишь средством передачи пакета от хоста к маршрутизатору, от маршрутизатора к маршрутизатору или от маршрутизатора к хосту.

Теперь, когда известно, как хосты и маршрутизаторы перенаправляют пакеты IPv4, перейдем к двум темам изоляции первопричины проблемы с использованием команд `ping` и `traceroute`. Эти команды позволяют исключать части процесса маршрутизации IPv4, подтверждая их работоспособность.

Локализация проблемы с использованием команды `ping`

Предположим, пользователь присылает вам сообщение электронной почты или звонит по телефону с просьбой разобраться с сетевой проблемой. Вы устанавливаете *защищенное удаленное соединение* (Secure Shell — SSH) с маршрутизатором и вводите команду `ping`, завершающуюся успешно. Поможет ли это исключить возможные причины проблемы или, наоборот, выявить первопричины?

Затем вы вводите другую команду `ping` по другому адресу, и на сей раз происходит отказ. О чем свидетельствует отказ команды `ping`? Какие элементы маршрутизации IPv4 все еще могут создавать проблемы, а какие, как уже известно, нет?

Команда `ping` — это один из наиболее распространенных инструментов поиска и устранения неисправностей сети. Когда команда `ping` завершается успешно, она подтверждает работоспособность некоторых индивидуальных элементов маршрутизации IP, исключая некоторые возможные причины текущей проблемы. Когда команда `ping` терпит неудачу, она зачастую помогает сузить список возможных первопричин проблем в объединенной сети, еще более локализуя проблему.

Этот раздел начинается с краткого обзора работы команды `ping`. Далее следуют рекомендации по использованию команды `ping` и анализу ее результатов в целях изоляции проблемы за счет удаления некоторых элементов из рассматриваемых.

Основы команды ping

Команда ping проверяет подключение, посылая пакеты на некий IP-адрес и ожидая от устройства с этим адресом ответных пакетов. Смысл посылаемых этой командой пакетов сводится к следующему: "Если вы получили этот пакет, отошлите ответ назад". Каждый раз, когда команда ping посылает один из этих пакетов и получает ответное сообщение, отосланное назад другим хостом, она знает, что пакет проделал путь от исходного хоста до хоста получателя и обратно.

Если быть более формальным, команда ping использует сообщения ICMP Echo Request и ICMP Echo Reply *протокола управляющих сообщений Интернета* (Internet Control Message Protocol — ICMP). Протокол ICMP определяет также и другие сообщения, но эти два специально предназначены для проверки подключения командой ping. Протокол ICMP не полагается в работе ни на протокол TCP, ни на протокол UDP, он не использует также протоколы уровня приложений. Этот протокол обычно считается вспомогательным для протокола IP, поскольку он выполняет функции обслуживания сети IP.

На рис. 4.6 представлены сообщения ICMP с заголовками IP. В данном случае пользователь на хосте A открывает приглашение к вводу команд и вводит команду ping 172.16.2.101, проверяя подключение к хосту B. Команда посылает эхо-запрос (этап 1) и переходит к ожиданию; хост B получает сообщения и отсылает назад эхо-ответ (этап 2).

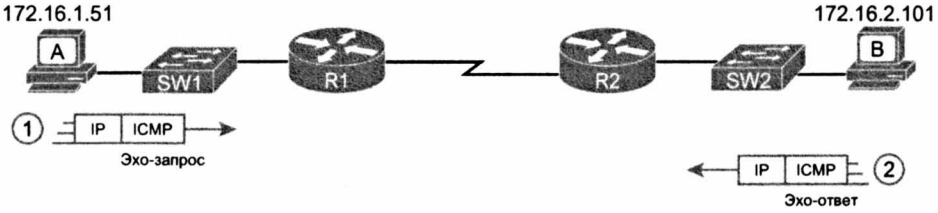


Рис. 4.6. Концепция, лежащая в основе команды ping 172.16.2.101 на хосте A

Команду ping поддерживает множество разных устройств и наиболее распространенных операционных систем. У команды есть много параметров: имя или IP-адрес получателя, количество передаваемых командой эхо-запросов, период ожидания эхо-ответов, размер пакетов и многие другие. Пример 4.1 демонстрирует вывод на хосте A с той же команды, что и на рис. 4.6: ping 172.16.2.101.

Пример 4.1. Пример вывода команды ping 172.16.2.101 на хосте A

```
Wendell-Odoms-iMac:~ wendellodom$ ping 172.16.2.101
PING 172.16.2.101 (172.16.2.101): 56 data bytes
64 bytes from 172.16.2.101: icmp_seq=0 ttl=64 time=1.112 ms
64 bytes from 172.16.2.101: icmp_seq=1 ttl=64 time=0.673 ms
64 bytes from 172.16.2.101: icmp_seq=2 ttl=64 time=0.631 ms
64 bytes from 172.16.2.101: icmp_seq=3 ttl=64 time=0.674 ms
64 bytes from 172.16.2.101: icmp_seq=4 ttl=64 time=0.642 ms
64 bytes from 172.16.2.101: icmp_seq=5 ttl=64 time=0.656 ms
^C
--- 172.16.2.101 ping statistics ---
6 packets transmitted, 6 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.631/0.731/1.112/0.171 ms
```

Стратегия проверки командой ping и ее результаты

Сотрудник, отвечающий на сообщения пользователей о проблемах (т.е. сотрудник клиентской службы или CSR), зачастую не может ввести команду ping на устройстве пользователя. Иногда проблему можно решить, продиктовав пользователю соответствующие команды, которые он введет на своей машине. Но пользователь может быть недоступен по голосовой связи. В качестве альтернативы можно использовать различные команды ping на разных маршрутизаторах, что может помочь локализовать проблему.

ВНИМАНИЕ!

На экзамене имеет смысл использовать команды ping на разных маршрутизаторах, как обсуждается далее.

Проблема с использованием команд ping на маршрутизаторах, вместо испытывающих проблемы хостов, заключается в том, что команда ping ни на каком отдельном маршрутизаторе не сможет точно воспроизвести команду ping на устройстве пользователя. Но каждая отдельная команда ping может помочь локализовать свою часть проблемы. В оставшейся части этого раздела обсуждаются поиск и устранение неисправностей маршрутизации IPv4 с использованием различных команд ping из *интерфейса командной строки* (Command-Line Interface — CLI) маршрутизатора.

Проверка длинных маршрутов ближе к источнику проблемы

Большинство проблем начинается с некого сообщения типа "хост X не может связаться с хостом Y". Вполне очевидным первым этапом поиска и устранения неисправностей является ввод команды ping на хосте X с IP-адресом хоста Y. Но у инженера может не быть доступа к хосту X, поэтому следующей возможностью является проверка командой ping IP-адреса хоста X с маршрутизатора, ближайшего к проблемному хосту.

Предположим, например, что пользователь хоста (см. рис. 4.6) обратился в службу поддержки с жалобой, связанной с передачей пакетов на хост B. Команда ping 172.16.2.101 на хосте A была бы великолепным первым этапом поиска и устранения неисправностей, но служба CSR не имеет доступа к хосту A и не может созвониться с его пользователем. Поэтому она устанавливает сеанс telnet с маршрутизатором R1 и вводит команду ping для хоста B, как показано в примере 4.2.

Пример 4.2. Маршрутизатор R2 проверяет хост B (две команды)

```
R1# ping 172.16.2.101
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.2.101, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/2/4 ms
R1# ping 172.16.2.101
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.2.101, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Уделим минуту обзору вывода первой команды `ping`. Стандартно команда Cisco IOS `ping` посылает пять эхо-запросов с периодом в 2 секунды. Если команда не получает эхо-ответ в течение 2 секунд, то полагает, что сообщение не прошло, и выводит период. Если ответ успешно получен в течение 2 секунд, команда выводит восклицательный знак. Таким образом, в первой команде период ожидания на первый эхо-ответ истек, а на четыре других был получен эхо-ответ в течение 2 секунд.

Кстати, пример демонстрирует обычное нормальное поведение команды `ping`: первый запрос завершается отказом, но остальные успешны. Обычно это происходит потому, что некое устройство на маршруте в целом не имеет соответствующей записи в таблице ARP.

Теперь вернемся к поиску и устранению неисправностей, а также к тому, что сообщает команда `ping` о текущем поведении объединенной сети. Сначала опишем общую картину.

- Маршрутизатор R1 может послать сообщение ICMP Echo Request на хост B (172.16.2.101).
- Стандартно маршрутизатор R1 посылает эти сообщения с IP-адреса своего исходящего интерфейса, в данном случае 172.16.4.1.
- Хост B может послать ответные сообщения ICMP Echo Reply на IP-адрес 172.16.4.1 маршрутизатора R1 (хосты посылают ответные сообщения на тот IP-адрес, с которого был получен эхо-запрос).

Последовательность передачи пакетов представлена на рис. 4.7.

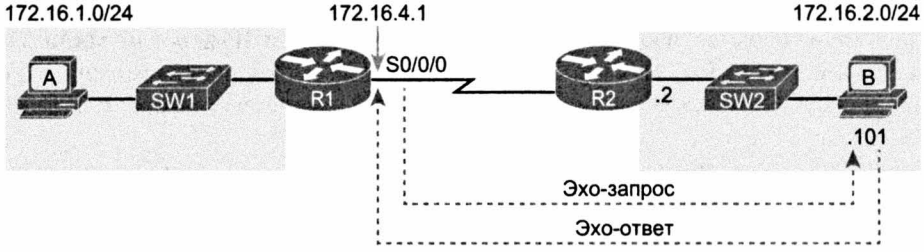


Рис. 4.7. Стандартно команда `ping 172.6.2.101` использует IP-адрес исходящего интерфейса

Теперь рассмотрим маршрутизацию IPv4. У маршрутизатора R1 должен быть маршрут передачи в прямом направлении к адресу хоста B (172.16.2.101); этот маршрут будет либо статическим, либо изученным по протоколу маршрутизации. Маршрутизатору R2 также нужен маршрут к адресу хоста B; в данном случае это подключенный маршрут к подсети хоста B (172.16.2.0/24), как показано верхней линией со стрелкой на рис. 4.8.



Рис. 4.8. Для успеха команды `ping 172.16.2.101` *на маршрутизаторе R1 необходимы маршруты уровня 3*

Линии со стрелками внизу на рис. 4.8 обозначают маршруты перенаправления ответных сообщений ICMP Echo Reply на маршрутизатор R1 по адресу 172.16.4.1. В первую очередь, хост B должен иметь правильный параметр стандартного маршрутизатора, поскольку адрес 172.16.4.1 находится в подсети, отличной от подсети хоста B. У маршрутизатора R2 должен также быть маршрут к адресу 172.16.4.1 (в данном случае это, вероятно, будет подключенный маршрут).

Для успеха команды `ping` в примере 4.2 также требуется рабочий канал связи на физическом уровне. Последовательный канал должен находиться в рабочем состоянии: интерфейс маршрутизатора должен быть в состоянии up/up, т.е. когда канал связи может передавать данные. Интерфейс маршрутизатора R2 на стороне локальной сети также должен быть в состоянии up/up. Кроме того, все изложенное ранее о локальных сетях Ethernet должно работать, поскольку команда `ping` подтвердила прохождение пакетов от маршрутизатора R1 до хоста B и назад. В частности:

- интерфейсы коммутатора в используемой области находятся в подключенном состоянии (up/up);
- защита порта не отфильтровывает фреймы, передаваемые маршрутизатором R2 или хостом B;
- протокол STP перевел используемые порты в состояние перенаправления.

ВНИМАНИЕ!

На этом рисунке показана небольшая сеть LAN с одним коммутатором, в большой сети LAN со многими коммутаторами успех команды `ping` подтверждает, что протокол STP завершил конвергенцию в рабочей топологии.

Команда `ping 172.16.2.101` в примере 4.2 также подтверждает, что списки управления доступом IP (ACL) не отфильтровывают сообщения ICMP. Напомню, что списки ACL на маршрутизаторе не фильтруют пакеты, созданные на том же маршрутизаторе, поэтому маршрутизатор R1 не фильтровал бы собственные сообщения ICMP Echo Request. Остальная часть сообщений ICMP, возможно, была бы отфильтрована на входе или выходе из интерфейсов маршрутизатора. На рис. 4.9 представлены области, где списки ACL могут отфильтровать сообщения, созданные командой `ping 172.16.2.101` на маршрутизаторе R1.

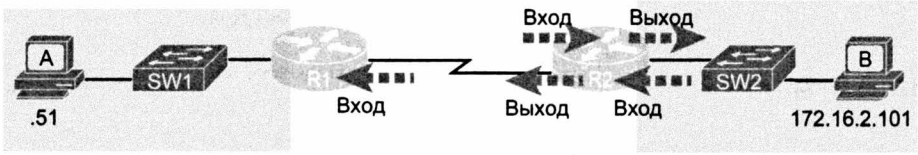


Рис. 4.9. Области, где списки ACL могут отфильтровать сообщения команды `ping`

И наконец, успех команды `ping 172.16.2.101` на маршрутизаторе R1 позволяет также установить, что на маршрутизаторе R2 и хосте B работает протокол ARP и что коммутатор SW2 получал MAC-адреса для своей таблицы MAC-адресов. Маршрутизатор R2 и хост B должны знать MAC-адреса друг друга, чтобы инкапсулировать пакет IP во фрейме Ethernet, а значит, у обоих должна быть соответствующая запись в таблице ARP. Коммутатор изучает MAC-адрес, используемый маршрутизатором R2 и хостом B, когда он посылает сообщения ARP или посылает фреймы, содержащие пакеты IP. На рис. 4.10 представлены типы информации, ожидаемой в этих таблицах.

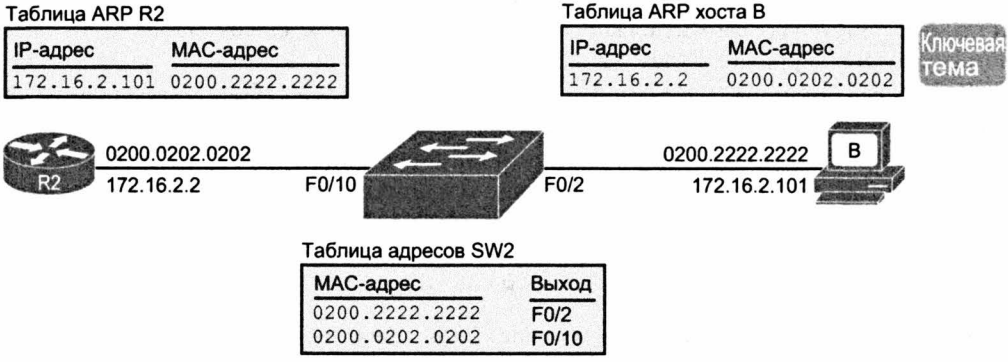


Рис. 4.10. Таблицы ARP и MAC-адресов

Как можно заметить, стратегия применения команды `ping` ближе к источнику проблемы позволяет исключить множество возможных первопричин любых проблем между двумя хостами, если команда `ping` успешна. Но в этом случае команда `ping` работает не совсем так, как на фактическом хосте. Следующие примеры демонстрируют несколько стратегий, позволяющих проверить другие части пути между двумя хостами, в которых может крыться проблема.

Использование расширенной команды `ping` для проверки обратного маршрута

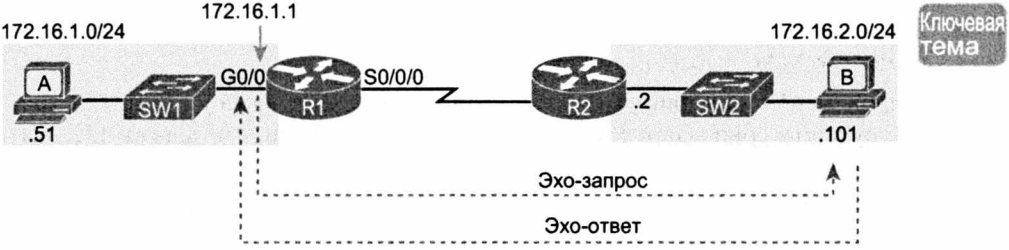
Обсуждавшаяся только что проверка командой `ping` со стандартного маршрутизатора не позволяет проверить маршруты IP полностью. В частности, она не проверяет обратный маршрут — назад к хосту отправителя.

Например, в объединенной сети (см. рис. 4.7) можно заметить, что обратные маршруты указывают не на адрес в подсети хоста A. Когда маршрутизатор R1 выполняет команду `ping 172.16.2.101`, он должен выбрать IP-адрес отправителя для эхо-запроса, и маршрутизаторы выбирают *IP-адрес исходящего интерфейса*. Эхо-запрос от маршрутизатора R1 до хоста B передается с IP-адресом отправителя

172.16.4.1 (IP-адрес интерфейса S0/0/0 маршрутизатора R1). Эхо-ответ возвращается по тому же адресу (172.16.4.1).

Стандартная команда `ping 172.16.2.101` на маршрутизаторе R1 не проверяет возможность маршрутизатора перенаправить пакеты назад в подсеть 172.16.1.0/24. Расширенная команда `ping` лучше, так как позволяет проверить обратный маршрут к подсети хоста A от маршрутизатора R1. Расширенная команда `ping` позволяет маршрутизатору R1 использовать IP-адрес из подсети 172.16.1.0/24. Поэтому эхо-ответы передавались бы в подсеть хоста A, как показано на рис. 4.11.

Кстати, обратите внимание, что маршрутизатор расширил возможности команды `ping` в интерфейсе командной строки (CLI). Она позволяет пользователю выбирать несколько дополнительных параметров по сравнению со стандартной командой `ping`. Расширенная команда `ping` позволяет не только ввести все параметры в потенциально длинной командной строке, но также просто ввести команду `ping` и нажать клавишу <Enter>, а операционная система IOS попросит ответить на вопросы, чтобы завершить команду, как показано в примере 4.3. Пример демонстрирует команду `ping` на маршрутизаторе R1 в соответствии с логикой на рис. 4.11.



Ключевая тема

Рис. 4.11. Расширенная команда `ping` проверяет маршрут к 172.16.1.51

Пример 4.3. Проверка обратного маршрута с использованием расширенной команды `ping`

```
R1# ping
Protocol [ip]:
Target IP address: 172.16.2.101
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 172.16.1.1
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 172.16.2.101, timeout is 2 seconds:
Packet sent with a source address of 172.16.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Данная конкретная расширенная команда `ping` проверяет те же маршруты, что и эхо-запрос, следующий вправо, но обеспечивает лучшую проверку маршрутов для эхо-ответов, следующих влево. Для этого направления маршрутизатор R2 нуждается в маршруте к адресу 172.16.1.1, который, вероятно, будет маршрутом к подсети 172.16.1.0/24. Это та же подсеть, в которой располагается хост A.

С точки зрения поиска и устранения неисправностей и стандартные, и расширенные команды `ping` могут быть очень полезны. Но ни одна не может точно подражать команде `ping`, отданной непосредственно на хосте, поскольку маршрутизаторы не могут послать пакеты с IP-адресом хоста. Например, расширенная команда `ping` в примере 4.3 использует IP-адрес отправителя 172.16.1.1, отнюдь не являющийся IP-адресом хоста A. В результате ни стандартные, ни расширенные команды `ping` в этих двух примерах не смогут проверить некоторые виды проблем, включая следующие.

Ключевая тема

Причины проблем подключения хоста, не обнаруживаемые командой `ping` на маршрутизаторе

- Список ACL отбрасывает пакеты с IP-адресом хоста A, но пропускает пакеты с IP-адресом маршрутизатора.
- Защита порта коммутатора LAN отфильтровывает пакеты хоста A (на основании его MAC-адреса).
- Маршруты IP на маршрутизаторах, соответствующие адресу 172.16.1.51 хоста A, случайно совпадают с маршрутами, соответствующими адресу 172.16.1.1 маршрутизатора R1.
- Неправильные параметры стандартного маршрутизатора на хосте A.

Проверка соседних LAN стандартной командой `ping`

Проверка командой `ping` другого устройства в сети LAN позволяет быстро подтвердить, способна ли сеть LAN передавать пакеты и фреймы. А именно, успех команды `ping` исключает много возможных первопричин проблемы, включая все средства Ethernet LAN, обсуждавшиеся в главе 3. Например, на рис. 4.12 представлены сообщения ICMP, передаваемые в случае, если маршрутизатор R1 пытается проверить командой `ping 172.16.1.51` хост A, находящийся в той же сети VLAN, что и маршрутизатор R1.

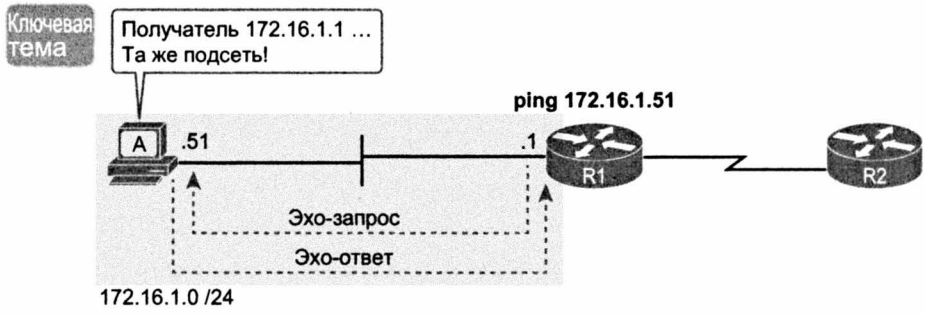


Рис. 4.12. Стандартная команда `ping` подтверждает работоспособность сети LAN

Успех команды `ping` подтверждает следующее, что исключает некоторые потенциальные проблемы.

- Хост с адресом 172.16.1.51 ответил.
- Локальная сеть может передавать одноадресатные фреймы с маршрутизатора R1 на хост 172.16.1.51, и наоборот.
- Вполне логично предположить, что коммутаторы изучили MAC-адреса маршрутизатора и хоста, добавив их в таблицы MAC-адресов.
- Хост A и маршрутизатор R1 завершили процесс ARP и записали друг друга в свои таблицы ARP.

Неудача команды `ping 172.16.1.51` на маршрутизаторе R1 указывает на ряд потенциальных первопричин, включая следующие.

Проблемы сетевого уровня, приводящие к неудаче команды `ping` между маршрутизатором и хостом в той же подсети LAN

Ключевая тема

- На хосте A может быть статически задан неправильный IP-адрес.
- Если используется протокол динамического конфигурирования хоста (DHCP), возможно множество проблем: хост A может использовать другой IP-адрес, отличный от 172.16.1.51, конфигурация DHCP могла быть неправильной, неправильной может быть конфигурация ретранслятора DHCP на маршрутизаторе, и, как следствие, хост A не получил IPv4-адреса и т.д.
- Маршрутизатор мог быть настроен на магистральное соединение 802.1Q, а коммутатор — нет (или наоборот).
- Любая проблема локальной сети, обсуждавшаяся в части I этой книги.

Таким образом, успех или отказ команды `ping` при проверке хоста LAN с маршрутизатора может помочь в последующей изоляции проблемы.

Проверка соседа LAN расширенной командой `ping`

Стандартная команда `ping` для хоста LAN с маршрутизатора не проверяет параметр стандартного маршрутизатора этого хоста. Но расширенная команда `ping` на это способна. Обе проверки могут быть полезны для локализации проблемы в случае, если:

Проверка параметра стандартного маршрутизатора на хосте с использованием расширенной команды `ping`

Ключевая тема

- стандартная команда `ping` для хоста локальной сети успешна...
- но расширенная команда `ping` для того же хоста закончилась неудачей...
- проблема так или иначе связана с параметром стандартного маршрутизатора хоста.

Сначала, чтобы понять, почему стандартные и расширенные команды `ping` имеют разные результаты, рассмотрим стандартную команду `ping 172.16.1.51` на маршрутизаторе R1, как было показано ранее на рис. 4.12. При стандартной ко-

манде ping маршрутизатор R1 использует IP-адрес своего интерфейса LAN (172.16.1.1) как адрес отправителя сообщений ICMP Echo. Таким образом, когда хост (A) возвращает ответ ICMP Echo Reply, хост A считает получателя 172.16.1.1 находящимся в той же подсети. Ответное сообщение ICMP Echo Reply хоста A, отосланное назад на адрес 172.16.1.1, будет получено, даже если у хоста A нет параметра стандартного маршрутизатора вообще!

Сравним это с использованием расширенной команды ping на маршрутизаторе R1, показанным на рис. 4.13. Расширенная команда ping от локального маршрутизатора R1 использует в качестве отправителя запроса ICMP Echo Request IP-адрес 172.16.4.1 своего интерфейса S0/0/0. Это означает, что ответ ICMP Echo Reply хоста A будет передан по адресу в другой подсети, что заставляет хост A использовать свой параметр стандартного маршрутизатора.

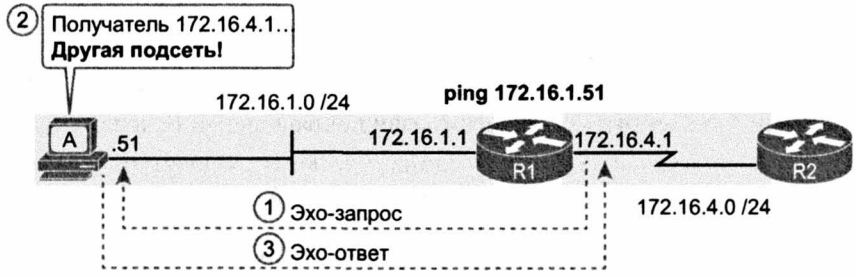


Рис. 4.13. Расширенная команда ping действительно проверяет параметр стандартного маршрутизатора хоста A

Различие между этим и предыдущим рисунками демонстрирует одну из самых классических ошибок при поиске и устранении неисправностей сетей. Иногда возникает искушение подключиться к маршрутизатору и проверить командой ping хост в подключенной сети LAN, и все работает. В результате инженер полагает, что проблем сетевого уровня между маршрутизатором и хостом нет, хотя это совсем не так — проблема в параметре стандартного маршрутизатора хоста.

Проверка соседа WAN стандартной командой ping

Подобно стандартной команде ping в локальной сети, стандартная команда ping позволяет проверить последовательные каналы связи WAN между маршрутизаторами на предмет передачи пакетов IPv4. При правильно составленном плане IPv4-адресации два маршрутизатора на том же последовательном канале должны иметь IP-адреса из той же подсети. Команда ping, отданная на одном маршрутизаторе с IP-адресом другого маршрутизатора на канале, подтверждает возможность передачи пакета IP по каналу связи вперед и назад, как показано в примере команды ping 172.16.4.2 на рис. 4.14.



Рис. 4.14. Проверка канала связи WAN

Успех команды `ping` подтверждает следующие конкретные факты.

Успешная проверка командой `ping` IP-адреса маршрутизатора подтверждает работоспособность следующих элементов на другом конце последовательного канала

Ключевая тема

- Последовательные интерфейсы обоих маршрутизаторов находятся в рабочем (up/up) состоянии.
- Средства уровня 1 и 2 канала связи находятся в рабочем состоянии.
- Маршрутизаторы полагают, что IP-адрес соседнего маршрутизатора находится в той же подсети.
- Входные списки ACL на обоих маршрутизаторах не отфильтровывают входящие пакеты друг друга.
- На дистанционном маршрутизаторе установлен ожидаемый IP-адрес (в данном случае 172.16.4.2).

При неудаче команды `ping` используйте тот же список для поиска первопричины. Например, подключившись к CLI маршрутизаторов, можно быстро проверить состояния интерфейсов маршрутизаторов и комбинации IP-адрес/маска. Проблемы уровней 1 и 2 обсуждаются в главе 12.

Проверка командой `ping` другого соседнего маршрутизатора позволяет выяснить многое, но не все. Например, проверка IP-адреса соседнего маршрутизатора позволяет подтвердить работоспособность только одного маршрута на каждом маршрутизаторе: подключенного маршрута к подсети на последовательном канале. Эта команда `ping` не проверяет маршруты к подсетям в локальных сетях. Кроме того, IP-адреса отправителя и получателя соответствуют адресам двух хостов с вероятной проблемой, поэтому не получится найти проблемы со списками ACL. Тем не менее, несмотря на ограниченность, такая проверка позволяет исключить проблемы каналы связи WAN уровня 1 или 2, а также некоторые простые проблемы адресации уровня 3.

Использование команды `ping` с именами и IP-адресами

До сих пор в этой главе во всех примерах команды `ping` использовались IP-адреса. Но команда `ping` может использовать и имена хостов, что позволяет проверить также работу системы доменных имен (DNS).

Большинство современных приложений TCP/IP используют для идентификации других устройств имена хостов, а не IP-адреса. Никто, открыв веб-браузер, не вводит **`http://72.163.4.161/`**, все вводят веб-адрес как **`http://www.cisco.com`**, вклю-

чающий имя хоста `www.cisco.com`. Далее, прежде чем хост сможет отправить данные по конкретному IP-адресу, хост должен сначала попросить сервер DNS преобразовать имя хоста в его IP-адрес.

Например, в небольшой объединенной сети, используемой для некоторых примеров в данной главе, команда `ping B` на хосте A проверяет параметры DNS, как показано на рис. 4.15. Когда хост A видит применение имени хоста (B), он сначала ищет его в его локальном кеше имен DNS, в надежде, что оно недавно использовалось. В противном случае хост A запрашивает сервер DNS, чтобы он преобразовал имя в соответствующий ему IP-адрес (этап 1 на рисунке). Только после этого хост A посылают пакет хосту B по IP-адресу 172.16.2.101 (этап 2).

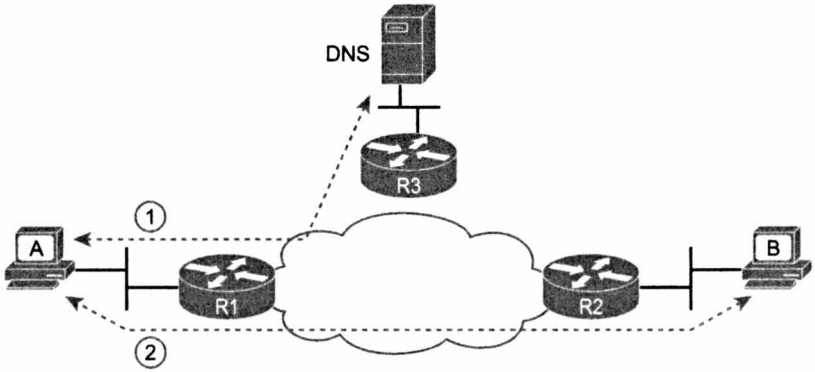


Рис. 4.15. Преобразование имен DNS для хоста A

Проверка с использованием имени хоста при поиске и устранении неисправностей может быть очень полезна, ведь команда проверяет параметры хоста как клиента DNS. Классический пример — сравнение результата команды `ping` с использованием имени хоста, требующего запроса DNS, с той же проверкой, но с использованием IP-адреса хоста получателя вместо его имени, что не требует запроса DNS. Если команда `ping` с IP-адресом успешна, а с именем хоста нет, то проблема обычно имеет некоторое отношение к службе DNS.

Локализация проблем с использованием команды `traceroute`

Как и команда `ping`, команда `traceroute` помогает сетевым инженерам локализовать проблемы. Ниже приведено их сравнение.

Ключевая тема

Сравнение команд `ping` и `traceroute`

- Обе посылают в сеть сообщения для проверки подключения.
- Для возвращения ответа обе полагаются на другие устройства.
- Обе поддерживаются многими операционными системами.
- Для идентификации получателя обе могут использовать имя хоста или IP-адрес.
- На маршрутизаторах у обеих есть стандартная и расширенная версии, позволяющие лучше проверить обратный маршрут.

Наибольшее различие кроется в более подробных результатах в выводе команды `traceroute` и более продолжительном времени построения этого вывода. В данном разделе рассматриваются работа команды `traceroute` и некоторые рекомендации по использованию более подробной информации, позволяющей быстрее локализовать проблемы маршрутизации IP.

Основы команды `traceroute`

Вообразите сетевого инженера или сотрудника CSR, начинающего поиск причины и устранение некой проблемы. Он вводит команду `ping` на хосте пользователя и на соседнем маршрутизаторе. После нескольких команд он убеждается, что хост способен передавать и получать пакеты IP. Проблема еще не решена, но уже понятно, что она не сетевая.

Теперь предположим, что рассматривается следующая проблема, и на сей раз команды `ping` неудачны. Это свидетельствует о том, что в сети IP действительно есть некая проблема. Но где ее причина? Где нужно искать внимательней? Хотя команда `ping` может оказаться полезной при локализации источника проблемы, команда `traceroute` обладает большими возможностями, так как помогает точно определить местоположение проблемы маршрутизации, демонстрируя, как далеко проходит пакет по сети IP прежде, чем произойдет отказ.

Команда `traceroute` идентифицирует маршрутизаторы по пути от исходного хоста до хоста назначения. А именно: выводит IP-адреса следующей транзитной точки перехода каждого маршрутизатора, оказавшегося на каждом конкретном маршруте. Например, команда `traceroute 172.16.2.101` на хосте A вывела бы IP-адрес маршрутизатора R1, далее маршрутизатора R2 и наконец хоста B, как показано на рис. 4.16. Вывод этой команды на хосте A представлен в примере 4.4.

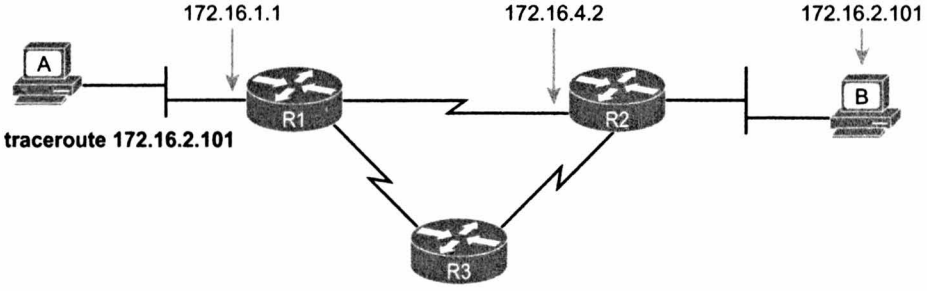


Рис. 4.16. IP-адреса, идентифицированные успехом команды `traceroute 172.16.2.101` на хосте A

Пример 4.4. Вывод команды `traceroute 172.16.2.101` на хосте A

```
Wendell-Odoms-iMac:~ wendellodom$ traceroute 172.16.2.101
traceroute to 172.16.2.101,    64 hops max, 52 byte packets
1 172.16.1.1    (172.16.1.1)    0.870 ms 0.520 ms 0.496 ms
2 172.16.4.2    (172.16.4.2)    8.263 ms 7.518 ms 9.319 ms
3 172.16.2.101 (172.16.2.101) 16.770 ms 9.819 ms 9.830 ms
```

Как работает команда `traceroute`

Команда `traceroute` собирает информацию, создавая пакеты, вызывающие на маршрутизаторах сообщения об ошибках; эти сообщения идентифицируют маршрутизаторы, позволяя команде `traceroute` создать в выводе команды список IP-адресов маршрутизаторов. Речь идет о сообщениях ICMP Time-to-Live Exceeded (TTL Exceeded), первоначально предназначенных для уведомления хостов о превышении времени существования зацикленных пакетов, курсирующих по сети.

Одним из способов устранения петлевых маршрутов маршрутизаторами IPv4 является отбрасывание зацикленных пакетов IP. Для этого заголовок IPv4 содержит поле времени жизни (Time To Live — TTL). Создающий пакет хост устанавливает начальное значение поля TTL. Затем каждый маршрутизатор, перенаправляющий пакет, уменьшает значение поля TTL на 1. Когда поле TTL достигает значения 0, маршрутизатор понимает, что пакет зациклен, и отбрасывает его. При этом маршрутизатор уведомляет хост, отправивший пакет, об отбрасывании сообщением ICMP TTL Exceeded.

Команда `traceroute` посылает сообщения с низкими значениями поля TTL, чтобы заставить маршрутизаторы возвращать сообщения TTL Exceeded. В частности, команда `traceroute` начинается с передачи нескольких пакетов (обычно трех) с полем TTL в заголовке, равным 1. Когда этот пакет достигает следующего (стандартного) маршрутизатора от хоста A (маршрутизатора R1 в примере на рис. 4.17), он уменьшает поле TTL до 0 и отбрасывает пакет. Затем маршрутизатор посылает хосту сообщение TTL Exceeded, идентифицирующее IP-адрес маршрутизатора для команды `traceroute`.



Рис. 4.17. Как команда `traceroute` идентифицирует первый маршрутизатор на маршруте

Команда `traceroute` посылает несколько пакетов с TTL=1, проверяя доступность для сообщений TTL Exceeded того же маршрутизатора на основании IP-адреса отправителя. Поскольку принятое сообщение исходит от того же маршрутизатора, команда `traceroute` отображает его IP-адрес в следующей строке вывода. Маршрутизаторы используют несколько IP-адресов, но, как уже можно догадаться, они используют IP-адрес исходящего интерфейса. В данном случае исходящий интерфейс маршрутизатора R1, отправляющего сообщение TTL Exceeded, имеет адрес 172.16.1.1.

Для составления списка всех маршрутизаторов на пути и подтверждения передачи пакетов от хоста отправителя к хосту получателя команда `traceroute` посылает пакеты с TTL=1, TTL=2, затем 3, 4 и т.д., до получения ответа от хоста назначения. На рис. 4.18 представлен пакет из второго набора с TTL=2. В данном случае один маршрутизатор (R1) перенаправляет пакет, а другой маршрутизатор (R2), после декремента TTL до 0, отбрасывает пакет и отсылает назад хосту A сообщение TTL Exceeded.

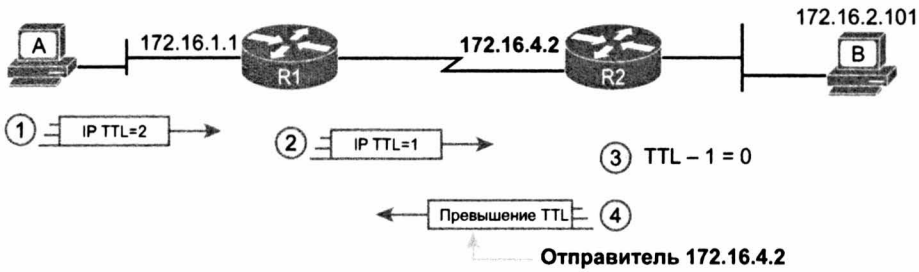


Рис. 4.18. TTL посланного командой `traceroute` *сообщения равно 2*

На рисунке представлены следующие четыре этапа.

1. Команда `traceroute` посылает пакет из второго набора с TTL=2.
2. Маршрутизатор R1, обрабатывая пакет, уменьшает значение TTL до 1 и перенаправляет его.
3. Маршрутизатор R2, обрабатывая пакет, уменьшает значение TTL до 0 и отбрасывает его.
4. Маршрутизатор R2 уведомляет хост, пославший отброшенный пакет сообщением ICMP TTL Exceeded. IP-адрес отправителя этого сообщения принадлежит исходящему интерфейсу маршрутизатора R2 (в данном случае 172.16.4.2).

Стандартная и расширенная команды `traceroute`

Стандартные и расширенные команды `traceroute` присваивают большинство тех же параметров, что и команда `ping`. Пример 4.5 демонстрирует вывод стандартной команды `traceroute` на маршрутизаторе R1. Как и стандартная команда `ping`, стандартная команда `traceroute` выбирает IP-адрес на основании исходящий интерфейса, передавшего пакет команды. В данном случае посланные маршрутизатором R1 пакеты поступают с IP-адреса отправителя 172.16.4.1, т.е. IP-адреса интерфейса S0/0/0 маршрутизатора R1.

Пример 4.5. Стандартная команда `traceroute` на маршрутизаторе R1

```
R1# traceroute 172.16.2.101
Type escape sequence to abort.
Tracing the route to 172.16.2.101
VRF info: (vrf in name/id, vrf out name/id)
  1 172.16.4.2 0 msec 0 msec 0 msec
  2 172.16.2.101 0 msec 0 msec *
```

Расширенная команда `traceroute`, показанная в примере 4.6, следует той же базовой структуре, что и расширенная команда `ping`. Пользователь может ввести все параметры в одной командной строке, но существенно проще ввести команду `traceroute` и нажать клавишу <Enter>. Это позволит приглашению IOS подобрать все параметры, включая IP-адрес отправителя пакетов (172.16.1.1 в данном случае).

Пример 4.6. Расширенная команда `traceroute` на маршрутизаторе R1

```
R1# traceroute
Protocol [ip]:
Target IP address: 172.16.2.101
Source address: 172.16.1.1
Numeric display [n]:
Timeout in seconds [3]:
Probe count [3]:
Minimum Time to Live [1]:
Maximum Time to Live [30]:
Port Number [33434]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Type escape sequence to abort.
Tracing the route to 172.16.2.101
VRF info: (vrf in name/id, vrf out name/id)
  1 172.16.4.2 0 msec 0 msec 0 msec
  2 172.16.2.101 0 msec 0 msec *
```

Команды `ping` и `traceroute` поддерживает большинство операционных систем, включая Cisco IOS. Однако некоторые операционные системы используют немного иной синтаксис команды `traceroute`. Например, большинство операционных систем Windows поддерживает команды `tracert` и `pathping`, а не `traceroute`. Linux и OS X поддерживают команду `traceroute`.

ВНИМАНИЕ!

Команды `traceroute` операционных систем хостов обычно создают сообщения ICMP Echo Request. Команда `traceroute` операционной системы Cisco IOS, напротив, создает пакеты IP с заголовком UDP. Сейчас эта информация может показаться тривиальной, но список ACL может фактически отфильтровать трафик сообщений команды `traceroute` хоста, но не маршрутизатора, и наоборот.

Использование команды `traceroute` для локализации проблемы на двух маршрутизаторах

Одной из отличительных возможностей команды `traceroute` по сравнению с командой `ping` является то, что при преждевременном завершении сразу понятно, где проверять далее. Когда команда `ping` терпит неудачу, следующим шагом обычно является использование следующих команд `ping`. Команда `traceroute` сразу указывает направление и маршрутизатор на маршруте, который следует проверить.

ВНИМАНИЕ!

Напомним, что термин *прямой маршрут* (forward route) описывает маршрут передачи пакетов, посланных командой `ping` или `traceroute`, а *обратный маршрут* (reverse route) — пакетов, передаваемых назад.

При наличии проблемы список маршрутизаторов в выводе команды `traceroute` оказывается незаконченным. Команда либо завершается с неполным списком, либо продолжает выполняется, пока пользователь не остановит ее. В любом случае в выводе перечисляются не все маршрутизаторы на маршруте.

ВНИМАНИЕ!

Кроме того, команда `traceroute` может не закончиться даже без проблем в сети. Дело в том, что сообщения, посланные командой `traceroute`, или ответные сообщения TTL Exceeded могут быть отфильтрованы маршрутизаторами и брандмауэрами, предотвратив отображение дальнейшей части сети.

Последний указанный в выводе маршрутизатор указывает, где и как искать далее следующим образом.

Где искать проблемы маршрутизации при незавершенной команде `traceroute`

Ключевая тема

- Подключитесь к CLI последнего указанного маршрутизатора и ищите проблемы прямого маршрута.
- Подключитесь к CLI следующего после указанного маршрутизатора, который должен был быть выведен, ищите проблемы обратного маршрута.

Рассмотрим пример объединенной сети на рис. 4.19. В данном случае маршрутизатор R1 использует расширенную команду `traceroute` к хосту 5.5.5.5, используя IP-адрес отправителя 1.1.1.1. Вывод этой команды укажет маршрутизаторы 2.2.2.2, 3.3.3.3, а затем отказ.

Сначала, согласно рис. 4.19, рассмотрим первую строку вывода, указывающую маршрутизатор первого транзитного участка 2.2.2.2.

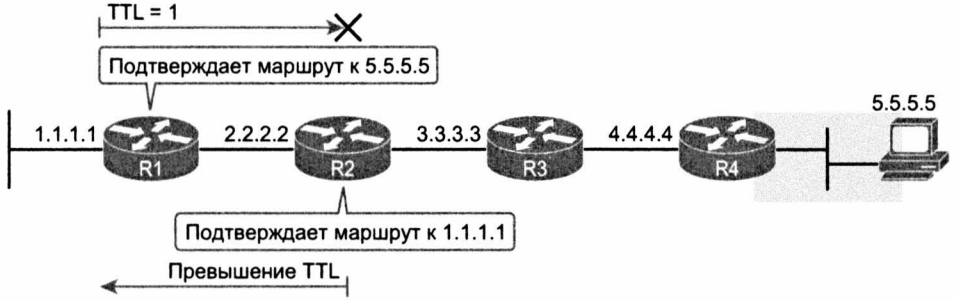


Рис. 4.19. Сообщения, позволяющие команде `traceroute` вывести адрес 2.2.2.2

Вверху представлено сообщение с TTL=1, внизу — обратное сообщение TTL Exceeded. Эта первая пара сообщений на рисунке, вероятно, сработала, поскольку без них команда `traceroute` на маршрутизаторе R1 не смогла бы вывести строку о маршрутизаторе с адресом 2.2.2.2. Первое (верхнее) сообщение требует, чтобы маршрутизатор R1 имел маршрут к хосту 5.5.5.5, по которому он послал пакеты далее на маршрутизатор R2. Сообщение превышения TTL требует наличия у маршрутизатора R2 маршрута к адресу 1.1.1.1, чтобы отослать пакеты назад, на IP-адрес интерфейса LAN маршрутизатора R1.

Рис. 4.20 демонстрирует сообщения, обеспечивающие вторую строку вывода команды `traceroute` на маршрутизаторе R1, указывающую адрес 3.3.3.3 как следующий маршрутизатор на маршруте.



Рис. 4.20. Сообщения, позволяющие команде `traceroute` *вывести адрес 3.3.3.3*

Согласно той же логике, команда `traceroute` выводит адрес 3.3.3.3, поскольку сообщения на рис. 4.20, очевидно, сработали. Для передачи этих сообщений должны существовать маршруты, указанные на рис. 4.19, а также новые маршруты, представленные на рис. 4.20. А именно: пакету с TTL=2 вверху требуется наличие на маршрутизаторе R2 маршрута к хосту 5.5.5.5, чтобы передать пакеты далее на маршрутизатор R3. Сообщению превышения TTL требуется наличие у маршрутизатора R3 маршрута к адресу 1.1.1.1, чтобы отослать пакеты назад, на IP-адрес интерфейса LAN маршрутизатора R1.

В этом примере команда `traceroute 5.5.5.5` не выводит маршрутизаторов далее адресов 2.2.2.2 и 3.3.3.3 Но, согласно рисункам, очевидно, что следующим выведенным IP-адресом должен быть 4.4.4.4. Поможет ли отказ передачи следующих сообщений (сообщения с TTL=3 и ответа на него) локализовать проблему еще больше?

На рис. 4.21 представлены проблемы маршрутизации, способные воспрепятствовать команде вывести в списке маршрутизатор 4.4.4.4 как следующий. В первую очередь, у маршрутизатора R3 должен быть прямой маршрут к получателю 5.5.5.5, чтобы перенаправить пакет на маршрутизатор R4. Для ответного сообщения требуется обратный маршрут к получателю 1.1.1.1, чтобы перенаправить пакет назад на маршрутизатор R3.



Рис. 4.21. Сообщения, позволяющие команде `traceroute` *вывести адрес 4.4.4.4*

Таким образом, если в этом примере проблема маршрутизации воспрепятствовала работе команды `traceroute`, то она кроется в одном из двух мест: прямой маршрут к адресу 5.5.5.5 на маршрутизаторе R3 или обратный маршрут к адресу 1.1.1.1 на маршрутизаторе R4.

Обзор

Резюме

- При передаче трафика нелокальному получателю хост создает и посылает пакет на свой стандартный маршрутизатор.
- Пакет передается от маршрутизатора к маршрутизатору (на основании содержимого индивидуальных таблиц маршрутизации маршрутизаторов), пока не будет достигнут получатель или пока не окажется маршрута к следующей транзитной точке перехода в направлении к получателю.
- Для обеспечения процесса изучения MAC-адресов других устройств в локальных сетях протокол IPv4 использует протокол преобразования адресов (ARP).
- Команда `ping` проверяет подключение, посылая пакеты на некий IP-адрес и ожидая от устройства с этим адресом ответных пакетов.
- Место ввода команды `ping` очень важно для определения или исключения возможных проблем между двумя хостами.
- Команда `ping` может использовать как имя хоста, так и его IP-адрес.
- Возможность задать IP-адрес позволяет расширенной команде `ping` проверить обратный маршрут.
- Используя поля TTL, команда `traceroute`, по существу, отправляет эхо-запросы по каждому транзитному участку вдоль пути к получателю.
- Расширенная команда `traceroute` позволяет инженеру изменять IP-адрес отправителя и намного лучше проверять обратные маршруты.

Ключевые темы

Повторите все ключевые темы данной главы, отмеченные пиктограммой "Ключевая тема". Ключевые темы и соответствующие им страницы перечислены в табл. 4.1.

Таблица 4.1. Ключевые темы главы 4

Элемент	Описание	Страница
Список	Логика перенаправления хоста	179
Список	Логика перенаправления маршрутизатора	180
Рис. 4.3	Логика перенаправления маршрутизатора	181
Рис. 4.4	Инкапсуляция и деинкапсуляция пакета при маршрутизации	182
Рис. 4.5	Пример процесса ARP	183
Рис. 4.10	Таблицы ARP и MAC-адресов	188
Рис. 4.11	Расширенная команда ping проверяет маршрут к 172.16.1.51	189
Список	Причины проблем подключения хоста, не обнаруживаемые командой ping на маршрутизаторе	190

Окончание табл. 4.1

Элемент	Описание	Страница
Рис. 4.12	Стандартная команда ping подтверждает работоспособность сети LAN	190
Список	Проблемы сетевого уровня, приводящие к неудаче команды ping между маршрутизатором и хостом в той же подсети LAN	191
Список	Проверка параметра стандартного маршрутизатора на хосте с использованием расширенной команды ping	191
Список	Успешная проверка командой ping IP-адреса маршрутизатора подтверждает работоспособность следующих элементов на другом конце последовательного канала	193
Список	Сравнение команд ping и traceroute	194
Список	Где искать проблемы маршрутизации при незавершенной команде traceroute	199

Ключевые термины

После первого прочтения главы попытайтесь дать определения следующим ключевым терминам. Но не расстраивайтесь, если не все получится сразу, в главе 22 описано, как использовать эти термины на завершающем этапе подготовки к экзамену.

инкапсуляция (encapsulation), деинкапсуляция (decapsulation), стандартный маршрутизатор (default router), протокол преобразования адресов (Address Resolution Protocol — ARP), команда `ping` (ping), команда `traceroute` (traceroute), эхо-запрос ICMP (ICMP echo request), эхо-ответ ICMP (ICMP echo reply), расширенная команда `ping` (extended ping), прямой маршрут (forward route), обратный маршрут (reverse route), система доменных имен (Domain Name System — DNS)

Глава 5

Поиск и устранение неисправностей маршрутизации IPv4. Часть II

В главе 4 обсуждение поиска и устранения неисправностей IPv4 начато с рассмотрения общепринятых первых этапов поиска и устранения неисправностей. Данная глава переходит к следующему этапу, когда проблема уже локализована в небольшой части сети и ограничена существенно меньшим набором возможных причин. Разделы этой главы посвящены поиску конкретных первопричин сетевых проблем со специфическими решениями.

Темы главы разделены на основании двух основных способов перенаправления пакетов в объединенной сети IPv4. Сначала речь пойдет о первопричинах проблем между хостом и его стандартным маршрутизатором. Затем будут рассмотрены маршрутизаторы, перенаправляющие пакет по остальной части маршрута от маршрутизатора, действующего как стандартный маршрутизатор, и до хоста получателя.

Кроме глав 4 и 5, теме поиска и устранения неисправностей объединенных сетей IPv4 посвящены и другие главы этой книги. В частности, в главе 11 обсуждаются поиск и устранение неисправностей, связанных с протоколами маршрутизации IPv4, а именно: открытым протоколом поиска первого кратчайшего маршрута (OSPF) и расширенным протоколом маршрутизации внутреннего шлюза (EIGRP). В главе 3 описаны поиск и устранение проблем LAN. В главах части IV затронуто несколько тем по поиску и устранению неисправностей каналов связи WAN. И наконец, в главе 16 обсуждается применение концепций поиска и устранения неисправностей IPv4 применительно к IPv6.

В этой главе рассматриваются следующие экзаменационные темы
Поиск и устранение неисправностей
Поиск и устранение наиболее распространенных проблем сети
Подключение
Инкапсуляция
Подсеть
Поиск и устранение проблем маршрутизации
Собственная сеть VLAN
Состояние режима порта магистрального канала
Поиск и устранение проблем маршрутизации
Разрешение маршрутизации
Правильность таблицы маршрутизации
Выбор правильного пути

Основные темы

Проблемы между хостом и стандартным маршрутизатором

Предположим, вы сотрудник службы CSR, отвечающий за заявления пользователей о проблемах. Пользователь оставил сообщение о невозможности подключиться к серверу. Вы перезвонили пользователю, но не застали его, поэтому ввели серию команд `ping` со стандартного маршрутизатора для этого хоста, используя одну из описанных в главе 4 стратегий локализации проблемы. По завершении вы приходите к выводу, что проблема кроется где-то между устройством пользователя и стандартным маршрутизатором, т.е. между маршрутизатором R1 и хостом A на рис. 5.1.

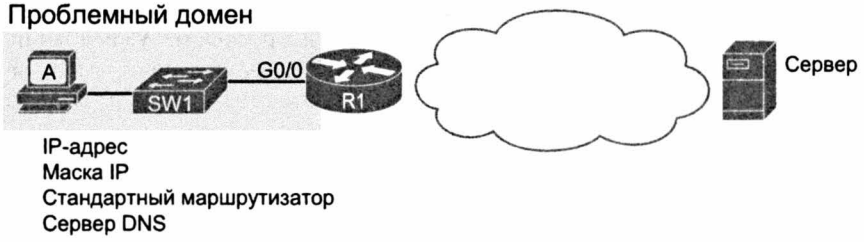


Рис. 5.1. Схема сети, обсуждаемой в этом разделе

В данном разделе будут рассмотрены проблемы, причина которых может крыться на хостах, их стандартных маршрутизаторах и между ними. Сначала рассматривается сам хост и его четыре параметра IPv4, представленные на рис. 5.1. Далее обсуждается стандартный маршрутизатор, его интерфейсы LAN и параметры, которые должны быть установлены на маршрутизаторе, чтобы он служил стандартным маршрутизатором хоста.

Первопричины в параметрах хоста IPv4

Типичный хост IPv4 получает свои четыре ключевых параметра IPv4 одним из двух способов: либо в ходе статической конфигурации, либо при помощи протокола DHCP. В обоих случаях параметры могут оказаться неправильными. Понятно, что при любой статической установке параметров человек может допустить ошибку при вводе значений. Куда удивительней факт, что протокол DHCP также может установить неправильные значения: процесс DHCP может работать, но при неправильных значениях на сервере DHCP хост может получить неправильные параметры IPv4.

Сначала рассмотрим параметры на хосте, а затем перейдем к обсуждению типичных проблем.

Гарантия правильности параметров IPv4

Если инженер подозревает, что проблема кроется где-то между хостом и его стандартным маршрутизатором, ему следует проверить параметры IPv4 хоста, сравнив их с правильными. Этот процесс начинается с запроса у пользователя ввода таких команд, как `ipconfig` и `ifconfig`, в зависимости от операционной системы хоста, при помощи GUI или командной строки. Этот процесс позволяет выяснить

наиболее очевидные проблемы, такие как полное отсутствие параметров, или, при использовании протокола DHCP, полный отказ протокола DHCP, не позволяющий получить никаких параметров IPv4.

Если параметры у хоста есть, то следующим шагом должна быть проверка соответствия их значений остальной части объединенной сети. IP-адрес сервера DNS (обычно это список как минимум из двух адресов) должен соответствовать адресу сервера DNS, фактически используемого в объединенной сети. В остальной части параметров должен быть указан правильный интерфейс LAN маршрутизатора, используемого как стандартный маршрутизатор этого хоста. На рис. 5.2 приведены все проверяемые элементы с объяснениями.

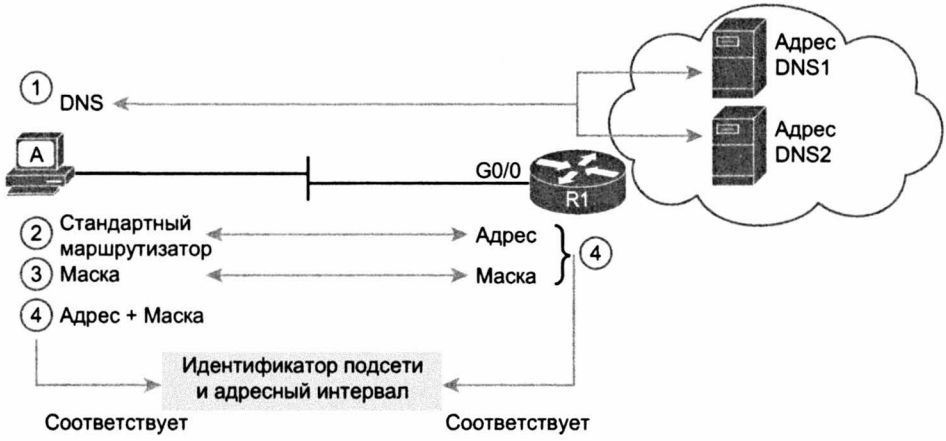


Рис. 5.2. Сравнение параметров IPv4 хоста с используемыми в сети

На рисунке пронумерованы следующие этапы проверки параметров хоста IPv4.

Этап 1 Проверьте правильность списка адресов серверов DNS на хосте

Этап 2 Используя команду `ip address`, сверьте параметр стандартного маршрутизатора на хосте с конфигурацией интерфейса LAN маршрутизатора

Этап 3 Сверьте маски подсети, используемые маршрутизатором и хостом; если они не совпадают, то и подсети не совпадают, что вызовет проблемы с некоторыми адресами хостов

Этап 4 Хост и маршрутизатор должны быть подключены к той же подсети — тот же идентификатор подсети и тот же диапазон IP-адресов. Поэтому, используя IP-адреса и маски маршрутизатора и хоста, вычислите идентификаторы подсети и диапазоны адресов. Убедитесь, что они принадлежат той же подсети, что и маршрутизатор (команда `ip address`)

Если параметр конфигурации IPv4 на хосте отсутствует или явно неправилен, его исправление может быстро устранить проблему. Например, если можно войти на маршрутизатору и ввести команду `show interfaces G0/0`, а затем попросить пользователя ввести команду `ipconfig /all` (или подобную) и прочитать вам вывод, то можно будет сравнить все параметры, как на рис. 5.2.

Несмотря на то что проверка параметров хоста действительно очень полезна, не все связанные с хостами проблемы так просто определить. В следующих разделах

рассматривается несколько примеров проблем, чтобы продемонстрировать признаки некоторых менее очевидных проблем.

Несовпадение масок влияет на маршрут доступа к подсети

Диапазоны адресов подсети на хосте и его стандартном маршрутизаторе должны быть согласованы. Иногда возникает желание пропустить эту проверку, игнорируя маску на хосте или на маршрутизаторе, считая, что на обоих устройствах используется одинаковая маска. Но если у хоста и маршрутизатора значения маски подсети отличаются, то каждый из них вычислит разный диапазон адресов в подсети, что создаст проблемы.

Рассмотрим пример такой сети, как на рис. 5.3. На хосте A заданы IP-адрес и маска 10.1.1.9/24, а также стандартный маршрутизатор 10.1.1.150. Быстро рассчитываем, принадлежит ли адрес 10.1.1.150 (адрес стандартного маршрутизатора) подсети хоста A? Да, принадлежит, как должно. Расчеты хоста A для этой подсети дают идентификатор подсети 10.1.1.0 с диапазоном адресов от 10.1.1.1 до 10.1.1.254 и широковещательный адрес подсети 10.1.1.255.

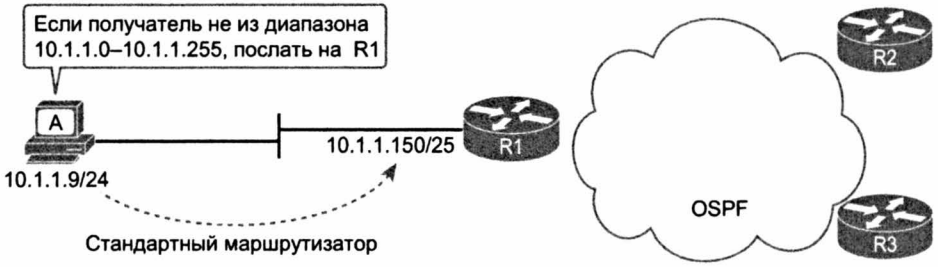


Рис. 5.3. Разные результаты вычисления подсети на хосте и в сети

В данном случае маршрутизация пакетов с хоста получателя вне подсети работает хорошо. Но в обратном направлении из остальной части сети назад на хост — нет. Быстрая проверка конфигурации маршрутизатора R1 показывает, что IP-адрес и маска, показанные на рис. 5.3, создают подключенный маршрут для подсети 10.1.1.128/25, как демонстрирует пример 5.1.

Пример 5.1. IP-адрес и маска на маршрутизаторе R1, а также подключенная подсеть, в которой отсутствует адрес хоста A

```
R1# show running-config interface g0/0
Building configuration...

Current configuration : 185 bytes
!
interface GigabitEthernet0/0
  description LAN at Site 1
  mac-address 0200.0101.0101
  ip address 10.1.1.150 255.255.255.128
  ip helper-address 10.1.2.130
  duplex auto
  speed auto
end
```

```
R1# show ip route connected
! Легенда опущена для краткости

     10.0.0.0/8 is variably subnetted, 9 subnets, 4 masks
C       10.1.1.128/25 is directly connected, GigabitEthernet0/0
L       10.1.1.150/32 is directly connected, GigabitEthernet0/0
! Другие маршруты опущены для краткости
```

Из-за данного конкретного несоответствия маршрутизатор R1 считает хост (10.1.1.9) не входящим в подсеть (10.1.1.128/25 дает диапазон от 10.1.1.129 до 10.1.1.254). Маршрутизатор R1 добавляет в таблицу маршрутизации подключенный маршрут к подсети 10.1.1.128/25 и даже анонсирует его (в данном случае по протоколу OSPF) другим маршрутизаторам в сети, как показано на рис. 5.4. Все маршрутизаторы знают, как перенаправить пакеты к подсети 10.1.1.128/25, но, к сожалению, этот маршрут не включает IP-адрес 10.1.1.9 хоста A.

Хосты должны использовать ту же маску подсети, что и стандартный маршрутизатор. Эти два устройства должны согласовать, какая подсеть существует в их общей LAN. В противном случае могут возникнуть проблемы, как в данном примере, или они могут возникнуть позже, если будут добавлены другие хосты.

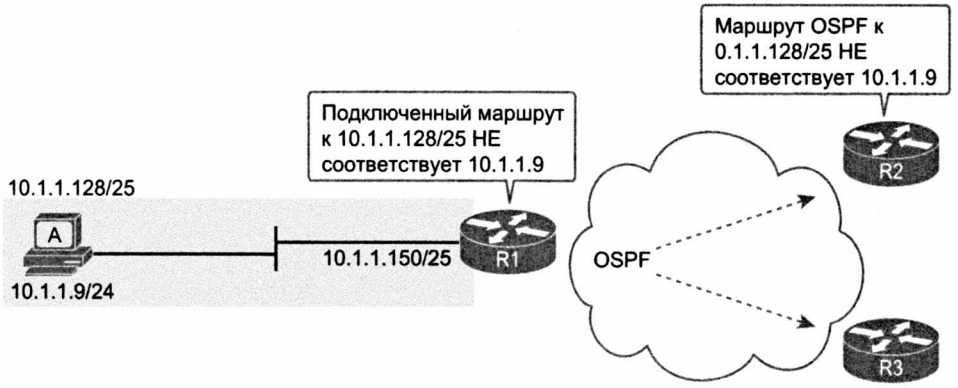


Рис. 5.4. У маршрутизаторов нет маршрута, соответствующего адресу 10.1.1.9 хоста A

Типичные причины проблем DNS

Когда на хосте задан неправильный список IP-адресов серверов DNS, симптомы вполне очевидны: неудачей заканчиваются любые действия пользователя, требующие преобразования имен. Если неправильный параметр DNS — это единственная проблема, то любая проверка сети при помощи команд `ping` и `traceroute` с использованием имен закончится отказом, но с IP-адресами вместо имен все работает исправно.

Если команда `ping` отказала с именем другого хоста, но сработала с IP-адресом того же хоста, то есть проблема с DNS. Предположим, например, что пользователь обратился в службу технической поддержки с жалобой на невозможность подключиться к серверу Server1. Сотрудник CSR вводит команду `ping server1` на своем компьютере. Команда срабатывает и демонстрирует IP-адрес 1.1.1.1 как адрес сервера Server1. Затем сотрудник CSR просит пользователя ввести на своем компьюте-

ре две команды: `ping Server1` (которая терпит неудачу) и `ping 1.1.1.1` (завершается успешно). Теперь понятно, что проблема в процессе преобразования имен DNS на компьютере пользователя.

В настоящей книге не рассматривается подробно внутренняя работа службы DNS, но следующие две первопричины проблем службы DNS встречаются на экзаменах CCENT и CCNA.

Ключевая тема

Две первопричины проблем DNS

- Неправильный параметр сервера DNS.
- Проблема соединения IP между хостом пользователя и сервером DNS.

Хотя первая проблема вполне очевидна, имейте в виду, что это может случиться и при статических параметрах, и при использовании протокола DHCP. Если на хосте задан неправильный IP-адрес сервера DNS, причем задан статически, достаточно изменить этот параметр. Если неправильный адрес сервера DNS получен по протоколу DHCP, необходимо исследовать конфигурацию сервера DHCP. (При использовании сервера DHCP для этого применяется команда `dns-server` *адрес-сервера* в режиме пула DHCP.)

Вторая проблема поднимает важный вопрос поиска и устранения любой реальной проблемы сети. Практически все реальные пользовательские приложения используют имена, а не адреса, и большинство хостов использует сервер DNS для преобразования имен. Таким образом, каждое соединение с новым приложением задействует два набора пакетов: пакеты, передаваемые между хостом и сервером DNS, и пакеты, передаваемые между хостом и реальным сервером (рис. 5.5).

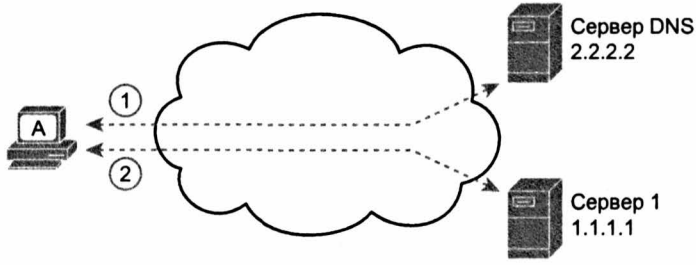


Рис. 5.5. Сначала передаются пакеты преобразования имен DNS, а затем пакеты реального сервера

И наконец, прежде чем завершить тему преобразования имен, обратим внимание на то, что на маршрутизаторе могут быть заданы IP-адреса серверов DNS, поэтому команды маршрутизатора могут преобразовывать имена. Например, пользователь интерфейса командной строки (CLI) маршрутизатора может ввести команду `ping server1` и рассчитывать на запрос DNS для преобразования имени server1 в его IP-адрес. Чтобы настроить маршрутизатор на использование службы DNS для преобразования имен, маршрутизатор нуждается в глобальной команде `ip name-server` *адрес-dns1 адрес-dns2...*. Он нуждается также в глобальной команде `ip domain-lookup`, используемой изначально.

Для поиска и устранения неисправностей имеет смысл задать на маршрутизаторе или коммутаторе параметры DNS, соответствующие таковым у локальных хостов. Но обратите внимание, что эти параметры никак не влияют на пользовательские запросы DNS.

ВНИМАНИЕ!

На практике команда `ip domain-lookup` стандартно задействована, но без IP-адреса сервера DNS. Большинство сетевых инженеров либо указывают в конфигурации адреса серверов DNS, либо отключают службу DNS командой `no ip domain-lookup`.

Неправильный параметр IP-адреса стандартного маршрутизатора

Понятно, что при указании на хосте неправильного IP-адреса стандартного маршрутизатора возникнут проблемы. При передаче пакетов в другие подсети хосты полагаются на стандартный маршрутизатор, и если на хосте задан неправильный параметр стандартного маршрутизатора, то хост не сможет посылать пакеты в другую подсеть. Такой пример представлен на рис. 5.6. В данном случае на хостах A и B неправильно указан адрес 10.1.3.4 как адрес стандартного маршрутизатора, вероятно, в связи с ошибкой в документации. Маршрутизатор R3 использует IP-адрес 10.1.3.3. (Будем считать, что никакой другой хост или маршрутизатор в этой подсети не использует адрес 10.1.3.4.)

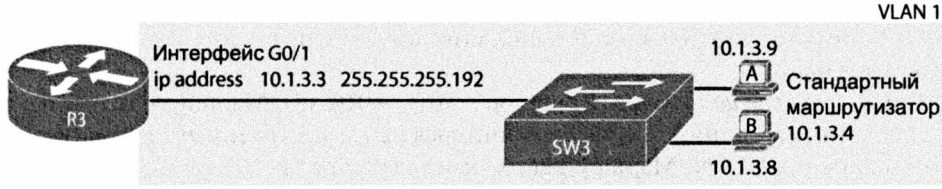


Рис. 5.6. Неправильный параметр стандартного маршрутизатора на хостах A и B

В данном случае некоторые функции действительно работают. Например, хосты A и B могут посылать пакеты другим хостам в той же сети LAN. Сотрудник CSR в CLI маршрутизатора может ввести команды `ping 10.1.3.9` и `ping 10.1.3.8`, причем обе сработают. В результате этих двух запросов маршрутизатор R3 указал бы MAC-адреса этих двух компьютеров в выводе команды `show arp`. Аналогично хосты содержали бы IP-адрес 10.1.3.3 маршрутизатора R3 (и соответствующий MAC-адрес) в своих кешах ARP (обычно они отображаются командой `arp -a`). Поскольку проблема в данном случае проявляется при попытке хостов посылать пакеты во внешние подсети, попытка послать пакеты на IP-адрес 10.1.3.4 потерпит неудачу.

Причины проблем в конфигурации стандартного маршрутизатора

Хотя для правильной работы на хостах должны быть заданы правильные параметры IPv4, это вовсе не гарантирует, что хост в локальной сети сможет успешно передать пакет на стандартный маршрутизатор. Сеть LAN между хостом и маршрутизатором должна работать. Кроме того, сам маршрутизатор должен работать правильно, согласно проекту объединенной сети.

Здесь рассматриваются проблемы между хостами и их стандартным маршрутизатором, когда причина проблем кроется на маршрутизаторе. В частности, рассматриваются три основных темы. Первая посвящена конфигурации магистрали на маршрутизаторе, необходимом для поддержки нескольких сетей VLAN (маршрутизатор на палочке, или ROAS). Далее рассматриваются типичные проблемы службы DHCP. Последняя обсуждаемая здесь первопричина относится к состоянию интерфейса маршрутизатора и к тому, что вызывает его отказ.

Несовпадение настройки магистрали VLAN и маршрутизатора на палочке

Примеры, объясняющие подробности конфигурации, зачастую сосредоточиваются на одной теме. Например, примеры по конфигурации IPv4 могут представить хост и параметр IP-адреса его стандартного маршрутизатора, заданный на интерфейсе LAN маршрутизатора, как было показано в примере 5.1.

И в реальной жизни, и на экзаменах требуется объединить все элементы поиска и устранения неисправностей. Следующий пример демонстрирует случай того, как страдает процесс поиска неисправности, если не рассмотреть одновременно как маршрутизатор, так и коммутатор. Пример демонстрирует вполне правильную конфигурацию маршрутизатора, которая, к сожалению, не соответствует конфигурации на соседнем коммутаторе LAN.

В следующем примере внимание уделено подключению маршрутизаторов к подсетям с несколькими сетями VLAN в той же территориальной сети LAN. Сегодня большинство площадок в корпоративных LAN используют по крайней мере две сети VLAN, поэтому для поддержки маршрутизации, как правило, применяют одну из двух возможностей.

Маршрутизатор на палочке (Router on a Stick — ROAS). Маршрутизатор подключается к сети LAN одним физическим интерфейсом, настроенным для магистрального соединения VLAN. Маршрутизатор имеет IP-адрес в каждой подсети, с одной подсетью на каждую VLAN. В конфигурацию маршрутизатора добавляется каждая соответствующая подсеть, а в конфигурацию субинтерфейса — каждая связанная сеть VLAN.

Коммутатор уровня 3 (Layer 3 switch), или *многоуровневый коммутатор* (multilayer switch), выполняет ту же задачу, что и маршрутизатор ROAS, но у него есть встроенные функции маршрутизации. В конфигурацию коммутатора добавляется каждая соответствующая подсеть, а в конфигурацию интерфейса VLAN — связанная сеть VLAN.

В данном примере используется ROAS, но большинство тех же видов представленных здесь ошибок может быть допущено в конфигурациях коммутатора уровня 3.

В первую очередь рассмотрим основные правила настройки ROAS с использованием стандарта 802.1Q как на маршрутизаторе, так и на соседнем коммутаторе.

Ключевая тема

Правила настройки ROAS

Этап 1 На маршрутизаторе. Для каждой сети VLAN, не являющейся собственной сетью VLAN, сделать следующее.

A. Создать индивидуальный субинтерфейс для каждой маршрутизируемой сети VLAN (`interface` *`тип номер.подсеть`*).

B. Разрешить протокол 802.1Q и ассоциировать в режиме конфигурации субинтерфейса каждую конкретную сеть VLAN с субинтерфейсом (`encapsulation dot1q` *`идентификатор_vlan`*).

C. В режиме конфигурации субинтерфейса задать параметры IP (адрес и маску) (`ip address` *`адрес маска`*)

Этап 2 На маршрутизаторе. Для каждой собственной сети VLAN, если они используются, применить одну из двух следующих возможностей.

A. Настроить как и для других VLAN, кроме добавления ключевого слова `native` в команду `encapsulation` (`encapsulation dot1q` *`идентификатор_vlan`* `native`). Или

B. Задать IP-адрес на физическом интерфейсе LAN, без субинтерфейса и без команды `encapsulation dot1q`

Этап 3 На коммутаторе. Разрешить магистральное соединение (поскольку маршрутизатор не будет вести переговоры о разрешении магистрального соединения 802.1Q).

A. Разрешить магистральное соединение подкомандой интерфейса `switchport mode trunk`.

B. Установить собственную сеть VLAN, как ту же ожидаемую на маршрутизаторе сеть VLAN, используя подкоманду интерфейса `switchport trunk native vlan` *`идентификатор_vlan`*

Этот довольно длинный список удобен для справки, но давайте теперь рассмотрим краткий пример конфигурации маршрутизатора. Предположим, что ранее площадка использовала одну сеть VLAN, поэтому конфигурация маршрутизатора проигнорировала магистральное соединение VLAN с IP-адресом, заданным на физическом интерфейсе LAN маршрутизатора. Все хосты находились в стандартной сети VLAN 1. Маршрутизатор мог игнорировать детали VLAN, не использовать магистральное соединение и действовать как стандартный маршрутизатор для всех хостов в сети VLAN 1, как показано на рис. 5.7.

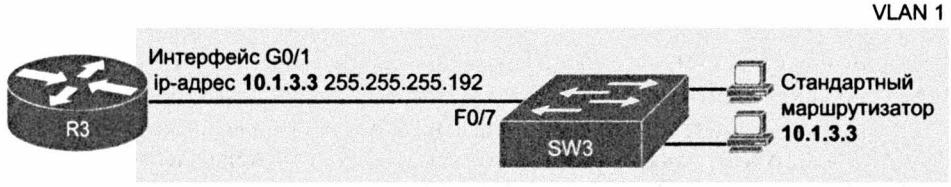


Рис. 5.7. Конфигурация IP-адреса маршрутизатора без магистрального соединения

Теперь руководство запланировало расширение, при котором будет использоваться вторая сеть VLAN. В данной конкретной компании один сетевой инженер отвечает за маршрутизаторы, а другой за коммутаторы. При планировании изменений инженер по коммутаторам был не очень внимателен, а затем инженер по маршрутизаторам ушел планировать изменения на маршрутизаторе. Инженер по маршрутизаторам запланировал сделать следующие изменения, чтобы использовать ROAS.

- Применить ROAS на интерфейсе G0/1 для поддержки обоих пользователей прежней подсети 10.1.3.0/26 в сети VLAN 1, а пользователи новой подсети 10.1.3.64/26 будут расположены в сети VLAN 2.

- Для поддержки пользователей сети VLAN 1 оставить на физическом интерфейсе подсеть 10.1.3.3/26 как есть. Здесь используется возможность настроить на физическом интерфейсе IP-адрес собственной сети VLAN, поскольку сеть VLAN 1 является стандартной собственной сетью VLAN.
- Добавить субинтерфейс ROAS в конфигурацию маршрутизатора. Для поддержки сети VLAN 2 использовать адрес 10.1.3.65/26 как IP-адрес/маску маршрутизатора в этой подсети.

Концепции и конфигурация представлены на рис. 5.8.

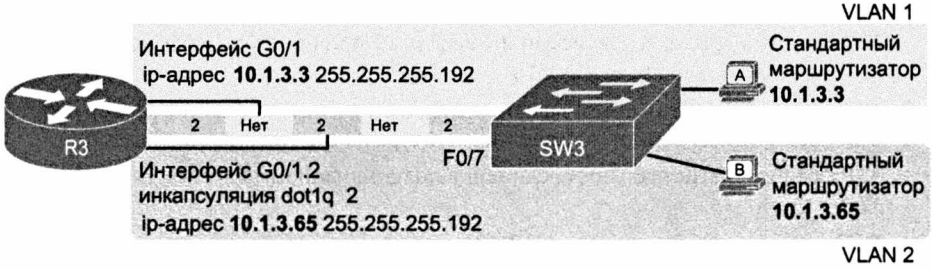


Рис. 5.8. Конфигурация IP-адреса маршрутизатора с ROAS и собственная сеть VLAN 1

Эта конфигурация будет отлично работать, если у коммутатора будет правильная конфигурация, соответствующая магистрали VLAN. Конфигурация маршрутизатора подразумевает следующие факты о магистральном соединении VLAN.

- При указанном на физическом интерфейсе G0/1 IP-адресе конфигурация подразумевает, что маршрутизатор намеревается использовать собственную сеть VLAN, посылая и получая не отмеченные фреймы.
- Маршрутизатор намеревается использовать сеть VLAN 2 как нормальную сеть VLAN, посылая и получая фреймы, помеченные как предназначенные для сети VLAN 2.

На коммутаторе (SW3) должно быть настроено магистральное соединение VLAN, чтобы соответствовать этой логике. В данном случае это означает необходимость разрешить магистральное соединение на этом канале связи, поддерживать сети VLAN 1 и VLAN 2, а также удостовериться, что сеть VLAN 1 является собственной. Вместо этого инженер коммутатора добавил конфигурацию магистрального канала не на тот порт, а порт F0/7, подключенный к маршрутизатору R3, имеет следующие параметры:

`switchport mode access` — Порт не создает магистральный канал.

`switchport access vlan 7` — Порт ассоциирован с сетью VLAN 7.

Первая команда, без сомнения, подтверждает, что канал связи между маршрутизатором R3 и коммутатором SW3 не является магистральным. Коммутатор SW3 не будет передавать по этому каналу связи никакого трафика сети VLAN 2 вообще. Стандартная команда `ping` с IP-адресом хоста B на маршрутизаторе R3 откажет; команда `ping 10.1.3.65` с хоста B также окончится неудачей.

Вторая команда свидетельствует, что VLAN доступна на интерфейсе F0/7 — это VLAN 7, а значит, коммутатор SW3 не будет перенаправлять трафик сети VLAN 1 по

каналу связи к маршрутизатору R3. Эхо-запросы между маршрутизатором R3 и хостами в сети VLAN 1 также теперь не будут проходить.

Таким образом, при настройке ROAS уделите время проверке конфигурации и на соседнем коммутаторе. В частности:

Элементы конфигурации магистрального соединения коммутатора, проверяемые на соответствие конфигурации ROAS маршрутизатора

Ключевая тема

- Удостоверьтесь, что на коммутаторе разрешено магистральное соединение (`switchport mode trunk`).
- Удостоверьтесь, что на коммутаторе в качестве собственной сети VLAN этого магистрального канала установлена правильная сеть VLAN (`switchport trunk native vlan` *`идентификатор_vlan`*).
- Удостоверьтесь, что коммутатору известно обо всех сетях VLAN, настроенных на маршрутизаторе (`vlan` *`идентификатор_vlan`*).

Проблемы ретранслятора DHCP

Хосты, использующие протокол DHCP для динамического резервирования IP-адреса (и изучения других параметров), вынуждены полагаться на работоспособность сети для передачи сообщений DHCP. В частности, если объединенная сеть применяет централизованный сервер DHCP, используемый многими дистанционными подсетями LAN, на маршрутизаторах должно быть разрешено такое средство, как *ретранслятор DHCP* (DHCP Relay), обеспечивающее работу протокола DHCP. Без ретранслятора DHCP запросы DHCP от хостов никогда не покинут локальную подсеть LAN.

Общие концепции работы ретранслятора DHCP представлены на рис. 5.9. В данном примере клиент DHCP (хост A) находится слева, а сервер DHCP (172.16.2.11) — справа. Клиент начинает процесс резервирования DHCP, передавая сообщение DHCP Discover. Без настройки ретранслятора DHCP на маршрутизаторе R1 они передавались бы только в локальный сети. Чтобы перенаправить сообщение DHCP Discover, маршрутизатор R1 разрешает ретрансляцию DHCP при помощи команды `ip helper-address 172.16.2.11` на его интерфейсе G0/0.

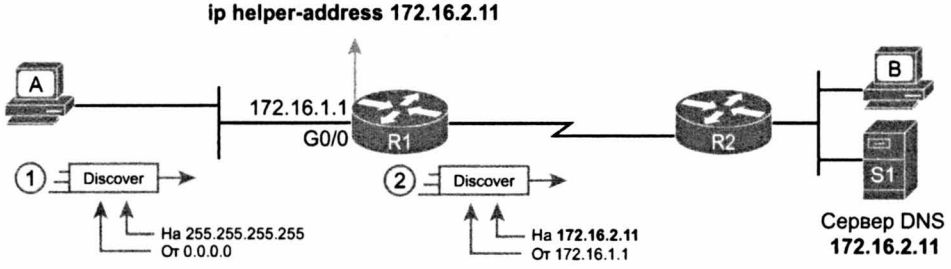


Рис. 5.9. Действие команды `ip helper-address`

Этапы на рисунке демонстрируют необходимость в ретрансляции DHCP. На этапе 1 хост A посылает сообщение на широковещательные IP и L2 адреса 255.255.255.255 и ff:ff:ff:ff:ff:ff соответственно. Посланные на этот широковещатель-

ный IP-адрес локальной подсети пакеты никогда не перенаправляются маршрутизатором вовне. Все устройства в подсети получат и обработают такой фрейм. Кроме того, поскольку на маршрутизаторе R1 введена команда `ip helper-address`, он извлечет пакет из фрейма, убедится, что это запрос DHCP, и примет меры. Этап 2 демонстрирует результаты применения ретранслятора DHCP, когда маршрутизатор R1 изменяет IP-адреса отправителя и получателя, а затем перенаправляет пакет по адресу 172.16.2.11, указанному в команде.

Теперь вернемся к поиску и устранению неисправностей. Посланные клиентом DHCP сообщения могут достичь сервера DHCP, если выполняются следующие условия.

Ключевая тема

Условия передачи сообщений с клиента DHCP на сервер DHCP

- Сервер находится в той же подсети, что и клиент при работоспособном соединении между ними.
- Сервер находится в другой подсети, а маршрутизатор в той же подсети, что и клиент. На маршрутизаторе настроен ретранслятор DHCP, и у него есть подключение IP к серверу DHCP.

При использовании ретранслятора DHCP обычно допускают две довольно очевидные ошибки. Если на интерфейсе LAN маршрутизатора (или субинтерфейсе при использовании ROAS, или интерфейсе VLAN при конфигурации с многоуровневой коммутацией (MLS)) отсутствует команда `ip helper-address`, служба DHCP будет недоступна клиентам. Если конфигурация включает команду `ip helper-address`, но содержит неправильный IP-адрес сервера DHCP, служба DHCP тоже будет недоступна.

Симптомы в обоих случаях одинаковы — клиент ничего не получает по протоколу DHCP.

Пример 5.2 демонстрирует измененную конфигурацию ROAS на маршрутизаторе R3, согласно тому же сценарию, что и на рис. 5.8. Конфигурация маршрутизатора работает прекрасно, поддерживая протокол IPv4 и обеспечивая его доступность. Но команда `ip helper-address` введена только на одном субинтерфейсе.

Пример 5.2. Отсутствие поддержки ретрансляции DHCP на субинтерфейсе ROAS

```
interface GigabitEthernet0/1
  ip address 10.1.3.3 255.255.255.192
  ip helper-address 10.1.2.130
!
interface GigabitEthernet0/1.2
 encapsulation dot1q 2
 ip address 10.1.3.65 255.255.255.192
```

В данном случае хосты в сети VLAN 1, которые собираются использовать протокол DHCP, вполне могут это сделать, подразумевая, что хост по адресу 10.1.2.130 действительно является сервером DHCP. Однако хосты в сети VLAN 2 не смогут изучать параметры по протоколу DHCP из-за отсутствия команды `ip helper-address`.

Интерфейс LAN маршрутизатора и проблемы LAN

В процессе локализации проблемы может оказаться, что команде `ping` с хоста недоступен его стандартный маршрутизатор, и наоборот. Таким образом, никакое устройство не может послать пакет IP на другое устройство в той же подсети. Эта простая проверка укажет инженеру, что маршрутизатор, хост и локальная сеть между ними по неизвестным причинам не могут передавать пакеты, инкапсулируемые во фрейме Ethernet.

Первопричины основных проблемы подключения LAN относятся к двум категориям:

- проблемы, вызвавшие отказ интерфейса LAN маршрутизатора;
- проблемы самой локальной сети.

Интерфейс LAN маршрутизатора должен находиться в рабочем состоянии, когда маршрутизатор попытается передавать или получать через него пакеты. Конкретно интерфейс LAN маршрутизатора должен находиться в состоянии up/up; если интерфейс находится в любом другом состоянии, маршрутизатор не будет использовать его для перенаправления пакетов. Таким образом, при отказе команды `ping` с маршрутизатора на хост LAN (или наоборот) проверьте состояние интерфейса, и если он не в рабочем состоянии, то ищите причину неработоспособности интерфейса маршрутизатора.

Но интерфейс маршрутизатора может находиться и в состоянии up/up, а проблема кроется в самой сети LAN. В данном случае это может быть любая проблема, связанная с локальными сетями Ethernet. В частности, первопричиной проблем LAN может быть все, что описано в главе 3, включая схемы расположения выводов кабелей Ethernet, защиту портов и даже протокол распределенного связующего дерева.

Например, на рис. 5.10 маршрутизатор R3 подключен к сети LAN с четырьмя коммутаторами. Интерфейс LAN маршрутизатора R3 (G0/1) может находиться в состоянии up/up, если канал связи между маршрутизатором R3 и коммутатором SW1 работает. Тем не менее предотвратить успешную передачу пакета IP, инкапсулируемого во фрейме Ethernet, с маршрутизатора R3 на хосты, подключенные к коммутаторам SW3 и SW4, могут еще многие другие причины.

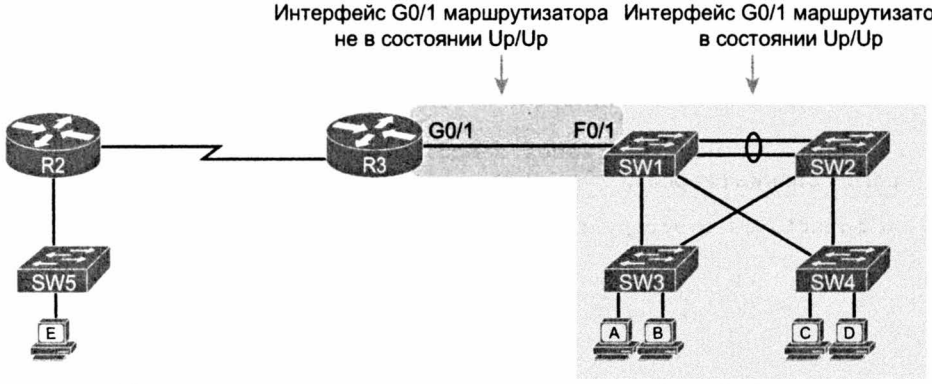


Рис. 5.10. Где искать проблемы на основании состояния интерфейса LAN маршрутизатора

ВНИМАНИЕ!

Проблемы LAN здесь не рассматриваются, обо всем, что изображено на рис. 5.10, *справа*, читайте в части I книги.

Интерфейсы LAN маршрутизатора могут находиться в нерабочем состоянии по нескольким причинам. Наиболее распространенные причины, обсуждаемые в рамках экзамена CCNA, приведены в табл. 5.1.

Ключевая тема

Таблица 5.1. Наиболее распространенные причины нерабочего состояния интерфейсов LAN

Причина	Описание	Состояние интерфейса маршрутизатора
Рассогласование скорости	И маршрутизатор, и коммутатор могут использовать подкоманды интерфейса для установки скорости, но скорости могут не совпадать	down/down
Отключение	На интерфейс маршрутизатора введена подкоманда интерфейса `shutdown`	admin down/down
Отключение из-за ошибки	Порт соседнего коммутатора использует защиту порта, переведшую порт в состояние отключения из за ошибки	down/down
Отсутствие (повреждение) кабеля	К маршрутизатору не подключен кабель или подключен кабель с неправильным расположением выводов *	down/down

*Коммутаторы Cisco используют такое средство, как auto-mdix, автоматически обнаруживающее некоторые неправильные схемы расположения выводов кабельных разъемов и внутренне изменяющие логику расположения контактов так, чтобы позволить использовать кабель. В результате неправильное расположение контактов не всегда приводит к отказу интерфейса.

На рис. 5.10, например, причиной рассогласования скоростей могли бы быть команды `speed 1000` на интерфейсе G0/1 маршрутизатора R3 и команды `speed 100` на интерфейсе F0/1 коммутатора SW1. Канал связи просто не сможет работать с таким различием в скоростях, поэтому интерфейсы маршрутизатора и коммутатора переходят в состояние down/down. В примере 5.3 показано результирующее состояние, на сей раз при помощи команды `show interfaces description`, выводящей по одной строке о каждом интерфейсе.

Пример 5.3. Команда `show interfaces description` при рассогласовании скорости

```
R3# show interfaces description
Interface          Status         Protocol     Description
Gi0/0              up             up
Gi0/1              down           down         link to campus LAN
Se0/0/0            admin down     down
Se0/0/1            up             up
Se0/1/0            up             up
Se0/1/1            admin down     down
```

Проблемы перенаправления пакетов между маршрутизаторами

Первая часть этой главы сосредоточена на первом транзитном участке, преодолеваемом пакетом IPv4 при передаче по сети. Вторая часть посвящена проблемам, связанным с перенаправлением маршрутизаторами пакетов от стандартного маршрутизатора до конечного хоста.

В частности, этот раздел начинается с рассмотрения логики направления IP на одиночном маршрутизаторе. Это позволит понять, что в настоящее время делает маршрутизатор. Последующее обсуждение затрагивает наиболее распространенные причины проблем маршрутизации, вызванные неправильной IP-адресацией, особенно когда в проекте адресации используются маски подсети переменной длины (VLSM).

В конце раздела рассматриваются проблемы, не связанные с базовой логикой маршрутизации IP, но все же влияющие на перенаправление пакетов, включая проблемы состояния интерфейса маршрутизатора (который должен быть в состоянии up/up) и случай, когда списки управления доступом IPv4 (ACL) отфильтровывают трафик IPv4.

Перенаправление IP при соответствии наиболее специфическому маршруту

Процесс маршрутизации IP любого маршрутизатора требует, чтобы маршрутизатор сравнил IP-адрес получателя каждого пакета с текущим содержимым таблицы маршрутизации IP данного маршрутизатора. Зачастую конкретному адресу получателя соответствует только один маршрут, но в некоторых случаях ему соответствует несколько маршрутов.

Перекрывающиеся подсети могут создать следующие факторы.

- Автоматическое суммирование (см. главу 10).
- Суммирование маршрутов вручную.
- Статические маршруты.
- Неправильный план подсетей, вызывающий наложение адресных интервалов подсетей.

В некоторых случаях наложение маршрутов создает проблемы, а в других случаях — это только нормальный результат применения некоторых средств. В данном разделе речь пойдет о том, как маршрутизатор выбирает, какой из накладывающихся маршрутов использовать. Возможные проблемы с накладывающимися маршрутами пока проигнорируем, некоторые из них обсуждаются далее, в разделе "Проблемы маршрутизации, вызванные неправильным планом адресации".

Сначала рассмотрим, как маршрутизатор находит соответствие в таблице маршрутизации даже при наличии в ней накладывающихся маршрутов. Если пакету соответствует только один маршрут, его маршрутизатор и использует. Но когда адресу получателя пакета соответствует несколько маршрутов, маршрутизатор использует лучший маршрут, определяемый следующим образом.

Ключевая тема *Когда адресу получателя пакета соответствует несколько маршрутов, используется наиболее специфический маршрут.*

Когда некоему IP-адресу получателя соответствует несколько маршрутов в таблице маршрутизации, маршрутизатор IPv4 использует самый специфический маршрут, иными словами, маршрут с самым длинным префиксом (маской).

Использование команды show ip route и вычисление подсети для поиска лучшего маршрута

Есть несколько способов выяснить, какой из маршрутов выберет маршрутизатор как самый лучший. Один из способов — использовать команду `show ip route` и математический механизм создания подсетей. Чтобы продемонстрировать эту возможность, в примере 5.4 представлен набор накладывающихся маршрутов.

Пример 5.4. Команда show ip route при накладывающихся маршрутах

```
R1# show ip route ospf
Codes: L - local, 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, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 172.16.25.129 to network 0.0.0.0

      172.16.0.0/16 is variably subnetted, 9 subnets, 5 masks
O        172.16.1.1/32 [110/50] via 172.16.25.2, 00:00:04, Serial0/1/1
O        172.16.1.0/24 [110/100] via 172.16.25.129, 00:00:09, Serial0/1/0
O        172.16.0.0/22 [110/65] via 172.16.25.2, 00:00:04, Serial0/1/1
O        172.16.0.0/16 [110/65] via 172.16.25.129, 00:00:09, Serial0/1/0
O        0.0.0.0/0 [110/129] via 172.16.25.129, 00:00:09, Serial0/1/0
!
```

ВНИМАНИЕ!

Команда `show ip route ospf` выводит маршруты, полученные только по протоколу OSPF, но статистика для номеров подсетей и масок (в данном примере 9 и 5 соответственно) указывается для всех маршрутов, а не только полученных по протоколу OSPF.

Чтобы предсказать, какой из маршрутов будет выбран маршрутизатором, необходимы две части информации: IP-адрес получателя пакета и содержимое таблицы маршрутизации маршрутизатора. Идентификатор подсети и маска, выведенные для маршрута, определяют диапазон адресов, соответствующий этому маршруту. Применив математический механизм создания подсетей, сетевой инженер может выяснить диапазон адресов, соответствующий каждому маршруту. Например, в табл. 5.2 представлены пять подсетей, указанных в примере 5.4, и их диапазоны адресов.

Таблица 5.2. Анализ диапазона адресов для подсетей в примере 5.4

Подсеть / префикс	Диапазон адресов
172.16.1.1/32	172.16.1.1 (только этот адрес)
172.16.1.0/24	172.16.1.0–172.16.1.255
172.16.0.0/22	172.16.0.0–172.16.3.255
172.16.0.0/16	172.16.0.0–172.16.255.255
0.0.0.0/0	0.0.0.0–255.255.255.255 (все адреса)

ВНИМАНИЕ!

Маршрут, выведенный как 0.0.0.0/0, является стандартным.

Судя по этим диапазонам, некоторые из диапазонов адресов маршрутов перекрываются. При соответствии нескольким маршрутам выбирается маршрут с наибольшей длиной префикса. Таким образом, маршрут с префиксом /16 лучше, чем маршрут с префиксом /10; маршрут с префиксом /25 лучше, чем с префиксом /20; и так далее.

Например, посланному на адрес 172.16.1.1 пакету фактически соответствуют все пять маршрутов, указанных в таблице маршрутизации примера 5.4. Длины префиксов варьируются от /0 до /32. Самый длинный префикс (наибольшее значение /P, означающее наилучший и самый специфический маршрут) — /32. Таким образом, посланный на адрес 172.16.1.1 пакет использует маршрут к подсети 172.16.1.1/32, а не другие маршруты.

Ниже приведено несколько примеров IP-адресов получателя. Для каждого адреса список указывает маршруты из табл. 5.2, выбираемые маршрутизатором в каждом случае.

- `172.16.1.1`. Подходят все пять маршрутов; самый длинный префикс — /32, используется маршрут к подсети 172.16.1.1/32.
- `172.16.1.2`. Подходят четыре маршрута; самый длинный префикс — /24, используется маршрут к подсети 172.16.1.0/24.
- `172.16.2.3`. Подходят три маршрута; самый длинный префикс — /22, используется маршрут к подсети 172.16.0.0/22.
- `172.16.4.3`. Подходят последние два маршрута; самый длинный префикс — /16, используется маршрут к подсети 172.16.0.0/16.

Использование команды `show ip route address` для поиска лучшего маршрута

Второй способ выявления используемого маршрутизатором маршрута не требует никаких вычислений подсетей — это команда `show ip route` *адрес*. Последний параметр этой команды — IP-адрес рассматриваемого пакета IP. Маршрутизатор укажет в выводе маршрут, который он использовал бы для перенаправления пакета, посланного на этот адрес.

В примере 5.5 показан вывод команды `show ip route 172.16.4.3` на том же маршрутизаторе, что и в примере 5.4. Первая (выделенная) строка вывода отобра-

жает соответствующий маршрут: маршрут к подсети 172.16.0.0/16. Остальная часть вывода отображает подробности данного конкретного маршрута, включая исходящий интерфейс S0/1/0 и следующий транзитный маршрутизатор 172.16.25.129.

Пример 5.5. Команда `show ip route` при накладывающихся маршрутах

```
R1# show ip route 172.16.4.3
Routing entry for 172.16.0.0/16
  Known via "ospf 1", distance 110, metric 65, type intra area
  Last update from 10.2.2.5 on Serial0/1/0, 14:22:06 ago
  Routing Descriptor Blocks:
  * 172.16.25.129, from 172.16.25.129, 14:22:05 ago, via Serial0/1/0
    Route metric is 65, traffic share count is 1
```

Конечно, если есть возможность, используйте именно эту команду для выяснения выбираемого маршрутизатором маршрута, — она намного быстрее и позволяет избежать математических вычислений.

Справка по команде `show ip route`

Команда `show ip route` играет главную роль в поиске и устранении неисправностей маршрутизации IP и проблем протокола маршрутизации IP. Эта команда нередко упоминается и здесь, и в книге по ICND1. Данный раздел объединяет все концепции для справки и простоты изучения.

На рис. 5.11 приведен типичный пример вывода команды `show ip route`. Номера на рисунке обозначают элементы вывода команды, а их описание приведено в табл. 5.3.

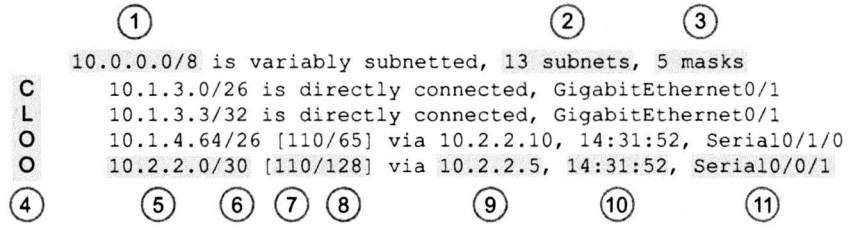


Рис. 5.11. Справка по выводу команды `show ip route`

Таблица 5.3. Описание вывода команды `show ip route`

Элемент	Идея	Значение на рисунке	Описание
1	Классовая сеть	10.0.0.0/8	Таблица маршрутизации организована по классовым сетям. Эта строка является заголовком для классовой сети 10.0.0.0; здесь указана стандартная маска для сетей класса A (/8)
2	Количество подсетей	13 subnets	Количество маршрутов к подсетям классовой сети, известных данному маршрутизатору, от всех отправителей, включая локальные маршруты, соответствующие каждому IP-адресу интерфейса маршрутизатора

Окончание табл. 5.3

Элемент	Идея	Значение на рисунке	Описание
3	Количество масок	5 masks	Количество разных масок, используемых на всех маршрутах, известных данному маршрутизатору в этой классовой сети
4	Коды легенды	C, L, O	Краткий код, идентифицирующий источник информации о маршрутизации. *O* — протокол OSPF; *D* — протокол EIGRP; *C* — подключенный маршрут; *S* — статический и *L* — локальный. (Легенда есть в примере 5.4)
5	Идентификатор подсети	10.2.2.0	Номер подсети данного маршрута
6	Длина префикса	/30	Префиксная маска, используемая данной подсетью
7	Административное расстояние	110	Если маршрутизатор получил маршруты для данной подсети из нескольких источников информации о маршрутизации, то он использует источник с самым низким административным расстоянием
8	Метрика	128	Метрика данного маршрута
9	Следующий транзитный маршрутизатор	10.2.2.5	IP-адрес следующего маршрутизатора, на который должен быть перенаправлен пакет, соответствующий этому маршруту
10	Таймер	14:31:52	Для маршрутов OSPF и EIGRP это время с момента получения маршрута
11	Исходящий интерфейс	Serial0/0/1	Интерфейс, на который должен быть послан пакет, соответствующий этому маршруту

Проблемы маршрутизации, вызванные неправильным планом адресации

Существование накладывающихся маршрутов в таблице маршрутизации маршрутизатора не обязательно означает наличие проблемы. И автоматическое суммирование маршрутов, и суммирование маршрутов вручную создают накладывающиеся маршруты на некоторых маршрутизаторах, и это не вызывает проблем. Но некоторые перекрытия, особенно связанные с ошибками адресации, вполне могут создать проблемы для пользовательского трафика. Поэтому, обнаружив при поиске и устранении неисправностей накладывающиеся маршруты, инженер должен выяснить конкретные причины перекрытия и проверить, не создает ли оно проблем.

Даже простые ошибки в плане IP-адресации или его реализации вполне могут привести к перекрытию, а это создаст проблемы. В этих случаях один маршрутизатор утверждает, что он подключен к подсети с одним диапазоном адресов, в то время как другой маршрутизатор утверждает, что подключен к другой подсети с перекрывающимся диапазоном, что нарушает правила IP-адресации. В результате маршрутизатор иногда перенаправляет пакеты на хост правильно, а иногда нет.

Эта проблема может произойти независимо от того, используются ли маски VLSM (маски подсети переменной длины). Однако найти такую проблему при использовании масок VLSM существенно труднее. В данном разделе приведены при-

меры проблем как в случае применения масок VLSM, так и без них, а также обсуждаются команды проверки и настройки, связанные с этими проблемами.

Когда используются маски VLSM

Считается, что объединенная сеть использует маски VLSM, когда для различных подсетей *одной классовой сети* используется несколько разных масок подсети. Например, если в одной объединенной сети все подсети создаются из сети 10.0.0.0 и используются маски /24, /26 и /30, то объединенная сеть использует маски VLSM.

Иногда люди ошибочно полагают, что любая объединенная сеть, использующая несколько масок, применяет маски VLSM, но это не всегда так. Например, если объединенная сеть использует подсети сети 10.0.0.0, все из которых используют маску 255.255.240.0, и подсети сети 172.16.0.0, все из которых используют маску 255.255.255.0, то проект не использует масок VLSM. Используются две разные маски, но каждая в своей одной классовой сети. Чтобы использовать маски VLSM, проект должен использовать несколько масок для подсетей одной классовой сети.

Только бесклассовые протоколы маршрутизации способны поддерживать маски VLSM. В настоящее время сертификация CCENT и CCNA Routing and Switching рассматривает только бесклассовые протоколы маршрутизации (OSPF и EIGRP), поэтому все обсуждаемые здесь протоколы маршрутизации поддерживают маски VLSM. Но в реальной жизни помните, что протокол RIPv2 (как бесклассовый протокол маршрутизации) также поддерживает маски VLSM, а такие классовые протоколы маршрутизации, как RIPv1 и IGRP (Interior Gateway Routing Protocol — протокол маршрутизации внутреннего шлюза), — нет.

Перекрытия без использования масок VLSM

Даже когда маски VLSM не используются, ошибки, связанные с перекрывающимися подсетями, вполне могут произойти. Например, рис. 5.12 демонстрирует пример сети с информацией об IP-адресе и маске маршрутизатора LAN. Перекрытие существует, но на первый взгляд это не очевидно.

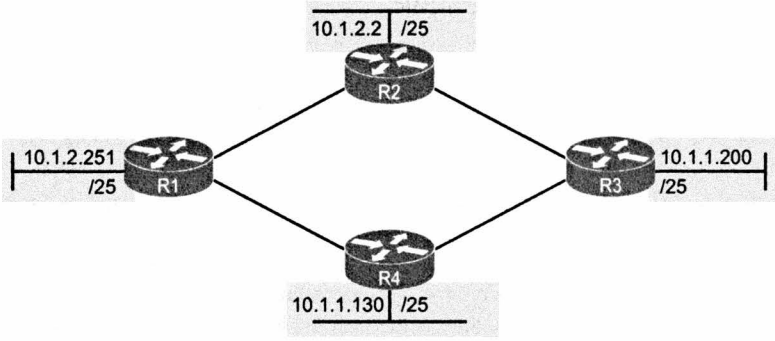


Рис. 5.12. IP-адреса интерфейсов LAN с единой маской (/25) в сети 10.0.0.0

При перекрытии в сети, где все подсети используют единую маску, у перекрывающаяся подсетей тот же идентификатор подсети и тот же диапазон IP-адресов. Для поиска перекрытия достаточно вычислить идентификатор каждой подсети и сравнить значения. Например, на рис. 5.13 показана измененная версия рис. 5.12 с идентификаторами подсети и их совпадением у локальных сетей, подключенных к маршрутизаторам R3 и R4.

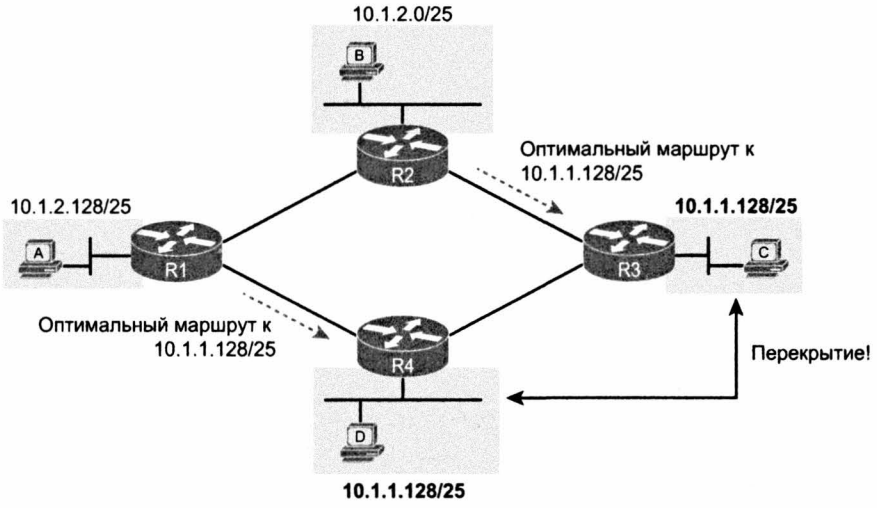


Рис. 5.13. Идентификаторы подсети, вычисленные по рис. 5.12

Использование той же подсети в двух разных местах (как на рис. 5.13) нарушает правила IPv4-адресации, поскольку маршрутизаторы не смогут решить, куда посылать пакеты. В данном случае одни маршрутизаторы передадут пакеты, посланные в подсеть 10.1.1.128/25, через маршрутизатор R3, а другие предпочтут маршрут к маршрутизатору R4. С учетом, что все маршрутизаторы используют такой протокол маршрутизации, как OSPF, оба маршрутизатора, R3 и R4, анонсируют маршрут к подсети 10.1.1.128/25.

В данном случае маршрутизаторы R1 и R2 передают пакеты на два разных экземпляра подсети 10.1.1.128/25. При таких маршрутах хосты за маршрутизатором R1 смогут общаться с хостами LAN 10.1.1.128/25 за маршрутизатором R4, но не с таковыми за маршрутизаторами R3, и наоборот.

И наконец, хотя признаки указывают на проблемы маршрутизации, первопричина в плохом плане IP-адресации. Та же подсеть никогда не должна использоваться в двух разных локальных сетях, как в данном случае. Решение: изменить конфигурацию маршрутизаторов R3 и R4 так, чтобы использовались разные неперекрывающиеся подсети на своих интерфейсах LAN.

Перекрытия при использовании масок VLSM

Использование масок VLSM к перекрывающимся подсетям может привести к тем же ошибкам адресации, но только заметить их будет значительно труднее.

Во-первых, перекрытие подсетей с различными масками обычно является только частичным. Поэтому у перекрывающихся подсетей будут разные размеры и, возможно, разные идентификаторы подсети. Перекрытие происходит между всеми адресами меньшей подсети, но только части адресов большей подсети. Во-вторых, проблемы возникают только на некоторых хостах (а именно в подмножестве накладывающихся адресов), что еще больше затрудняет идентификацию проблемы.

Например, на рис. 5.14 приведен пример перекрытия при использовании масок VLSM. На рисунке представлены только IP-адреса и маски пар интерфейсов хоста и маршрутизатора. Посмотрите на пример и попытайтесь найти перекрытие на основании IP-адресов.

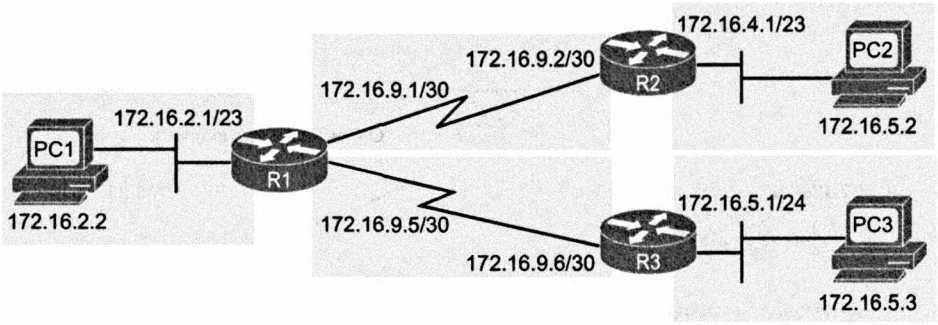


Рис. 5.14. План IP-адресации VLSM в сети 172.16.0.0

При поиске перекрытия в этом случае следует проанализировать каждую подсеть, найти не только идентификатор подсети, но и широковещательный адрес подсети, и диапазон адресов в подсети. Если остановиться только на идентификаторах подсети, то обнаружить перекрытие нельзя (как в данном примере).

Рис. 5.15 демонстрирует начало анализа каждой подсети — вычисленные идентификаторы подсети. Обратите внимание, что у двух перекрывающихся подсетей разные идентификаторы подсети, но правая нижняя подсеть (172.16.5.0/24) полностью накладывается на часть правой верхней подсети (172.16.4.0/23). (Подсеть 172.16.4.0/23 имеет широковещательный адрес 172.16.5.255, а подсеть 172.16.5.0/24 — широковещательный адрес 172.16.5.255.)

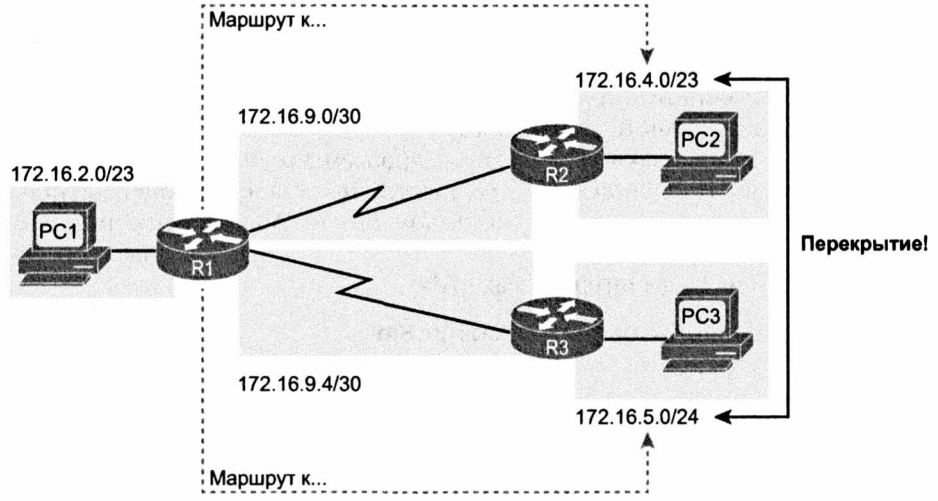


Рис. 5.15. Пример наложения при разных идентификаторах подсети

Безусловно, проект подсетей с перекрывающимися диапазонами адресов неправилен и подлежит изменению. Но при реализации он создает симптомы, схожие с проблемами маршрутизации, как в случае, описанном выше. Команды `ping` и `traceroute` действительно терпят неудачу, но только для определенных хостов, а не для всех.

Перекрытия подсетей VLSM в конфигурации

Правила создания подсетей IP требуют, чтобы диапазоны адресов в подсетях объединенной сети не перекрывались. Операционная система IOS иногда способна распознать, когда новая команда `ip address` создает перекрывающуюся подсеть, а иногда — нет. Это происходит в следующих случаях.

Случаи, когда операционная система IOS способна и неспособна распознать перекрытия IP-адресов в конфигурации



- **Перекрытие на одном маршрутизаторе пресекается**. Операционная система IOS обнаруживает перекрытие, когда команда `ip address` создает пересечение диапазонов адресов с другой командой `ip address` *на том же маршрутизаторе*.
- **Перекрытие на разных маршрутизаторах допускается**. Операционная система IOS не может обнаружить перекрытие, когда команда `ip address` создает пересечение диапазонов адресов с другой командой `ip address` *на другом маршрутизаторе*.

Представленный в примере 5.6 маршрутизатор пресекает создание конфигурации с накладывающимися подсетями. В примере приведена настройка на интерфейсе Fa0/0 маршрутизатора R3 IP-адреса 172.16.5.1/24, а также попытка установки на интерфейсе Fa0/1 адреса 172.16.5.193/26. Диапазоны адресов в каждой подсети таковы.

Подсеть 172.16.5.0/24. 172.16.5.1 – 172.16.5.254
Подсеть 172.16.5.192/26. 172.16.5.193 – 172.16.5.254

Пример 5.6. Один маршрутизатор не допускает наложения подсетей

```
R3# configure terminal
R3(config)# interface Fa0/0
R3(config-if)# ip address 172.16.5.1 255.255.255.0
R3(config-if)# interface Fa0/1
R3(config-if)# ip address 172.16.5.193 255.255.255.192
% 172.16.5.192 overlaps with FastEthernet0/0
R3(config-if)#
```

Операционной системе IOS известно, что наложение диапазонов адресов создаваемых подсетей недопустимо. В данном случае, поскольку обе подсети были бы соединены, этот маршрутизатор знает, что эти две подсети не смогут сосуществовать, так как это нарушило бы правила создания подсетей. Таким образом, операционная система IOS отклоняет вторую команду.

Кроме того, операционная система IOS проверяет такие ошибки, как перекрытие подсетей, только для интерфейсов, не находящихся в отключенном состоянии. При настройке интерфейса в отключенном состоянии операционная система IOS примет команду `ip address`, что приведет к перекрытию. Впоследствии, когда будет введена команда `no shutdown`, операционная система IOS проверит перекрытие подсетей и выдаст сообщение об ошибках, подобное представленному в примере 5.6. Она оставит интерфейс в отключенном состоянии, пока проблема перекрытия не будет устранена.

Операционная система IOS не сможет обнаружить конфигурацию с перекрывающимися подсетями на разных маршрутизаторах, как демонстрируется в примере 5.7. Здесь представлена конфигурация двух перекрывающаяся подсетей на маршрутизаторах R2 и R3, согласно рис. 5.15.

Пример 5.7. Два маршрутизатора допускают накладывающиеся подсети

```
! Сначала на маршрутизаторе R2
R2# configure terminal
R2(config)# interface G0/0
R2(config-if)# ip address 172.16.4.1 255.255.254.0
! ----------------------------------------------
! Далее на маршрутизаторе R3
R3# configure terminal
R3(config)# inter face G0/0
R3(config-if)# ip address 172.16.5.1 255.255.255.0
```

Состояние интерфейса маршрутизатора WAN

Один из этапов процесса поиска неисправностей маршрутизации IP, описанный ранее в разделе "Интерфейс LAN маршрутизатора и проблемы LAN", подразумевает проверку состояния интерфейса, гарантирующую работоспособность необходимого интерфейса. У работающего интерфейса маршрутизатора оба кода состояния интерфейса up или, как упоминают обычно, up/up.

До сих пор и в книге по ICND1, и по ICND2 рассматривалась только основная информация о работе последовательных каналов. На настоящий момент известно, что последовательные интерфейсы обоих маршрутизаторов должны находиться в рабочем состоянии (up/up), прежде чем они смогут передавать пакеты IPv4 друг другу. Кроме того, у последовательных интерфейсов обоих маршрутизаторов должны быть IP-адреса в той же подсети.

В части IV рассматриваются подробности каналов связи WAN, включая то, что необходимо маршрутизаторам для использования этих каналов связи при перенаправлении пакетов IP.

Фильтрация пакетов списками управления доступом

Списки управления доступом (ACL) — причина ряда самых больших проблем при поиске и устранении неисправностей в реальных сетях. Пакеты, посланные приложениями конечного пользователя, не совсем похожи на пакеты, посылаемые при проверке такими инструментами, как `ping` и `traceroute`. Списки ACL иногда отфильтровывают трафик команд `ping` и `traceroute`, заставляя сетевого инженера полагать, что есть проблема другого вида, тогда как никакой проблемы нет вообще. Или проблема с трафиком конечного пользователя действительно вызвана списками ACL, но трафик команд `ping` и `traceroute` прекрасно проходит, поскольку список ACL фильтрует пользовательский трафик, но не трафик команд `traceroute` и `ping`.

Ниже описан алгоритм, с помощью которого следует искать и устранять ошибки в списках управления доступом (ACL).

Этап 1 Определите, на каких интерфейсах установлены списки управления доступом и в каком направлении (с помощью команд `show running-config`, `show ip interfaces`)

Этап 2 Определите, какие правила списков срабатывают (с помощью команд `show access-lists`, `show ip access-lists`)

Этап 3 Проанализируйте списки ACL, чтобы предсказать, какие пакеты будут срабатывать согласно каким правилам, учитывая указанные ниже особенности работы списков.

A. В списках ACL проверка правил происходит до первого срабатывания.

B. Чтобы упростить процесс поиска соответствий в правилах, можно преобразовать записи адреса и шаблона маски в списках управления доступом в стандартный формат адреса и маски, как было показано в главе 22 первого тома.

C. Определите направление потока пакетов относительно сервера (пакет пересылается серверу или от сервера). Убедитесь, что для соответствующего потока пакетов правильно указан IP-адрес отправителя и порт или IP-адрес получателя и что порт получателя и направление списка ACL совпадает с направлением потока пакетов.

D. Проверьте, правильно ли используются ключи `tcp` и `udp` в расширенных списках, правила которых проверяют номера портов. (В табл. 8.3 перечислены наиболее популярные номера портов TCP и UDP.)

E. Помните, что пакеты ICMP не используют службы TCP и UDP, поэтому для фильтрации таких пакетов нужно указывать ключ `icmp` (а не `tcp` или `udp`).

F. Вместо неявного запрещающего правила в конце списков управления доступом укажите запрещающее или разрешающее правило в явном виде, чтобы с помощью команды `show` можно было увидеть счетчики пакетов, отброшенных или переданных согласно такому правилу

Если есть подозрение, что проблема вызвана списками ACL, первый этап локализации проблемы — выяснить, на каком интерфейсе установлен список управления доступом и в каком направлении. Быстрее всего можно выполнить такое действие с помощью команды `show running-config`, в выводе которой следует поискать команды `ip access-group` для интерфейсов. В некоторых случаях привилегированный режим может быть недоступен, поэтому придется использовать другие команды группы `show`. Как определить, в каком направлении, прямом или обратном, настроен список управления доступом с помощью команды `show ip interfaces`, показано в примере 5.8.

Пример 5.8. Вывод команды `show ip interface`

```
R1> show ip interface s0/0/1
Serial0/0/1 is up, line protocol is up
   Internet address is 10.1.2.1/24
   Broadcast address is 255.255.255.255
   Address determined by setup command
   MTU is 1500 bytes
   Helper address is not set
   Directed broadcast forwarding is disabled
   Multicast reserved groups joined: 224.0.0.9
   Outgoing access list is not set
   Inbound access list is 102
! Около 26 строк вывода опущены для краткости
```

Обратите внимание: показанная выше команда выводит информацию о том, включен ли список ACL, в каком направлении и его номер или название. В примере 5.8 приведен вариант команды с указанием конкретного интерфейса `show ip interface S0/0/1`, чтобы уменьшить количество выводимой информации. Команда `show ip interface` выводит ту же информацию, но для всех интерфейсов устройства.

На этапе 2 алгоритма поиска ошибок в списках управления доступом следует просмотреть сам список. Опять же быстрее всего можно выполнить такое действие с помощью команды `show running-config`. Если привилегированный режим недоступен, то аналогичный результат можно получить с помощью команд `show access-lists` и `show ip access-lists`, выводящих те же подробности, что и команды конфигурации, а также счетчик количества пакетов, соответствующих каждой строке списка ACL (пример 5.9).

Пример 5.9. Пример вывода команды `show ip access-lists`

```
R1# show ip access-lists
Extended IP access list 102
    10 permit ip 10.1.2.0 0.0.0.255 10.1.1.0 0.0.0.255 (15 matches)
```

После того как были определены интерфейс, к которому привязан список управления доступом, и направление списка (т.е. выполнены этапы 1 и 2), начинается самая сложная часть процесса — интерпретация списка ACL.

Всегда обращайте внимание на значения счетчиков в списках управления доступом. Так, в примере 5.9 можно заметить, что 15 пакетов по своим характеристикам совпали с указанным правилом в списке с номером 102. Часть пакетов, вполне вероятно, была отброшена, поскольку в конце списка управления доступом есть неявное запрещающее правило, которое в выводе команды не отображается. Задав правило `access-list 102 deny ip any any` для такого списка ACL, выполняющего те же функции, что и неявное правило, в выводе команды `show ip access-lists` можно было бы увидеть счетчик отброшенных пакетов. Компания Cisco зачастую рекомендует указывать явное запрещающее правило в конце каждого списка управления доступом вместо неявного, чтобы упростить процесс поиска ошибок в списках ACL.

И наконец, имеет смысл напомнить об интерпретации команд ACL. Когда известно, что команда исходит от маршрутизатора, довольно просто решить, что диапазон адресов соответствует адресам и шаблонам маски. Нижняя граница диапазона — это адрес (первое число), а верхняя — сумма адреса и шаблона маски. Например, ACL 102 в примере 5.9, вполне очевидно, настроен на неком маршрутизаторе, поэтому диапазоны следующие:

Отправитель 10.1.2.0, шаблон 0.0.0.255. Соответствует адресам от 10.1.2.0 до 10.1.2.255

Получатель 10.1.4.0, шаблон 0.0.1.255. Соответствует адресам от 10.1.4.0 до 10.1.5.255

Обзор

Резюме

- На хосте, на стандартном маршрутизаторе и между ними возможно множество проблем.
- Типичный хост получает четыре своих ключевых параметра IPv4 либо статически, либо динамически.
- Начинайте поиск и устранение неисправностей хоста с команды `ipconfig` или `ifconfig`, чтобы проверить правильность параметров IPv4. Если используется протокол DHCP, то команда `ipconfig` или `ifconfig` позволит увидеть, способен ли протокол DHCP предоставить все необходимые параметры IPv4.
- Хост и маршрутизатор должны быть подключены к той же подсети, т.е. иметь одинаковый идентификатор подсети и одинаковый диапазон IP-адресов.
- Когда на хосте задан неправильный список IP-адресов серверов DNS, симптомы вполне очевидны: неудачей заканчиваются любые действия пользователя, требующие преобразования имен.
- Любая проверка сети при помощи команд `ping` и `traceroute` с использованием имен закончится отказом, но с IP-адресами вместо имен все работает исправно.
- При указании на хосте неправильного IP-адреса стандартного маршрутизатора возникнут проблемы.
- Конфигурация стандартного маршрутизатора может вызвать в сети проблемы, включая несоответствие конфигураций магистралей VLAN, проблемы ретрансляции DHCP, интерфейса LAN маршрутизатора и проблемы локальной сети.
- Если на интерфейсе LAN маршрутизатора (или субинтерфейсе при использовании ROAS, или интерфейсе VLAN при конфигурации с многоуровневой коммутацией (MLS)) отсутствует команда `ip helper-address`, служба DHCP будет недоступна клиентам.
- Еще одна проблема сетевых подключений может быть связана с маршрутизацией или с тем, как маршрутизатор перенаправляет пакет.
- Команда `show ip route` играет главную роль в поиске и устранении неисправностей маршрутизации IP и проблем протокола маршрутизации IP.
- В некоторых случаях наложение маршрутов создает проблемы, а в других случаях — это нормальный результат применения некоторых средств.

Ключевые темы

Повторите все ключевые темы данной главы, отмеченные пиктограммой "Ключевая тема". Ключевые темы и соответствующие им страницы перечислены в табл. 5.4.

Таблица 5.4. Ключевые темы главы 5

Элемент	Описание	Страница
Список	Две первопричины проблем DNS	208
Список	Правила настройки ROAS	210
Список	Элементы конфигурации магистрального соединения коммутатора, проверяемые на соответствие конфигурации ROAS маршрутизатора	213
Список	Условия передачи сообщений с клиента DHCP на сервер DHCP	214
Табл. 5.1	Наиболее распространенные причины нерабочего состояния интерфейсов LAN	216
Определение	Когда адресу получателя пакета соответствует несколько маршрутов, используется наиболее специфический маршрут	217
Список	Случаи, когда операционная система IOS способна и неспособна распознать перекрытия IP-адресов в конфигурации	225

Заполните таблицы и списки по памяти

Распечатайте приложение Г с веб-сайта или его раздел, относящийся к этой главе, и заполните таблицы и списки по памяти. В приложении Д приведены заполненные таблицы и списки для самоконтроля.

Глава 6

Создание резервного маршрутизатора первого транзитного участка

Современные компании в работе полагаются на свои сети. Одни из них зависят от сетей больше, чем другие, и потеря соединения между сетями напрямую связана с потерей дохода. Например, при отказе сети некоторые компании теряют клиентов или продажи либо не могут отправить свои товары, что непосредственно затрагивает объемы продаж и в настоящем и в будущем. Компании могут разработать свои сети так, чтобы использовать дополнительные, избыточные устройства и каналы связи и чтобы при отказе устройства или канала связи сеть сохранила работоспособность. Дополнительные устройства стоят дополнительных денег, но по сравнению с ценой потерь это может быть оправдано.

Сети с избыточными устройствами и каналами связи иногда требуют применения дополнительных протоколов, чтобы справиться с внесенными изменениями и обеспечить поддержку сетевых функций при наличии избыточности. В этой главе обсуждается один из такой протоколов — *протокол резервирования первого транзитного участка* (First Hop Redundancy Protocol — FHRP).

Протокол FHRP позволяет сетевым инженерам установить в подсети несколько маршрутизаторов, действующих как один стандартный маршрутизатор. С точки зрения хостов такие маршрутизаторы выглядят как единый стандартный маршрутизатор, позволяя хостам, совершенно не заботясь об избыточности маршрутизаторов, получать все преимущества этой избыточности. Для координации работы, распознавания проблем и принятия на себя функций другого маршрутизатора (при необходимости) маршрутизаторы обмениваются сообщениями.

Данная глава разделена на два основных раздела. В первом рассматриваются причины применения протокола FHRP и его возможности: протокол маршрутизации горячего резервирования (Hot Standby Routing Protocol — HSRP), протокол резервирования виртуального маршрутизатора (Virtual Router Redundancy Protocol — VRRP) и протокол балансировки нагрузки шлюза (Gateway Load Balancing Protocol — GLBP). Второй раздел посвящен настройке и проверке протоколов HSRP и GLBP.

В этой главе рассматриваются следующие экзаменационные темы
Технологии маршрутизации IP
Выявление технологии высокой доступности (FHRP)
VRRP
HSRP
GLBP

Основные темы

Концепции протокола FHRP

Когда в проекте сети есть избыточные маршрутизаторы, коммутаторы, каналы связи LAN и WAN, чтобы использовать преимущества и избежать связанных с избыточностью проблем, в некоторых случаях требуются дополнительные протоколы. Представьте, например, глобальную сеть со множеством дистанционных филиалов. Если у каждой дистанционной ветви есть два канала WAN, подключающие ее к остальной части сети, то для выбора наилучших маршрутов эти маршрутизаторы могут использовать протокол маршрутизации IP. При отказе одного канала связи WAN протокол маршрутизации может задействовать маршруты через оставшийся канал связи WAN, воспользовавшись наличием избыточного канала связи.

В качестве другого примера рассмотрим сеть LAN с избыточными коммутаторами и каналами связи (см. главы 1 и 2 этой книги). Если коммутаторы не используют *протокол распределенного связующего дерева* (Spanning Tree Protocol — STP), в этих локальных сетях будут проблемы. Протокол STP предотвращает проблемы, создаваемые циклически передаваемыми фреймами по избыточным путям в локальной сети.

В этой главе рассматривается еще один тип протокола, позволяющий избежать проблем, на сей раз при использовании избыточных стандартных маршрутизаторов. Когда к той же подсети LAN подключены два или более маршрутизатора, все они применяются как стандартный маршрутизатор для хостов в подсети. Однако для этого необходим другой протокол, FHRP. *Протокол резервирования первого транзитного участка* (First Hop Redundancy Protocol — FHRP) относится к категории протоколов, позволяющих воспользоваться преимуществами наличия в подсети избыточных маршрутизаторов.

В первом из двух главных разделов этой главы рассматриваются базовые концепции протокола FHRP. Раздел начинается с обсуждения необходимости избыточности в сети вообще и необходимости в избыточных стандартных маршрутизаторах в частности. Далее демонстрируется, как три доступных возможности протокола FHRP позволяют решить проблемы, связанные с использованием избыточных стандартных маршрутизаторов.

Необходимость избыточности в сетях

Сети нуждаются в избыточных каналах связи для улучшения своей доступности. В конце концов, в сети что-то регулярно отказывает: может пропасть питание маршрутизатора или коммутатора, кабель может оборваться или выйти из разъема. Каналы связи WAN, изображаемые в большинстве рисунков этой книги как простые линии, фактически являются самыми сложными частями сети со множеством отдельных элементов, которые также могут отказать.

В зависимости от проекта сети отказ одного компонента может означать отключение, по крайней мере, части пользовательской сети. Любой компонент, отказ которого приводит к отключению части сети, называется *единой точкой отказа* (single point of failure). Например, локальные сети на рис. 6.1 обладают некой избыточно-

стью, а глобальная часть сети — нет. На рисунке показано, что между передающими трафик площадками существует множество единых точек отказа.

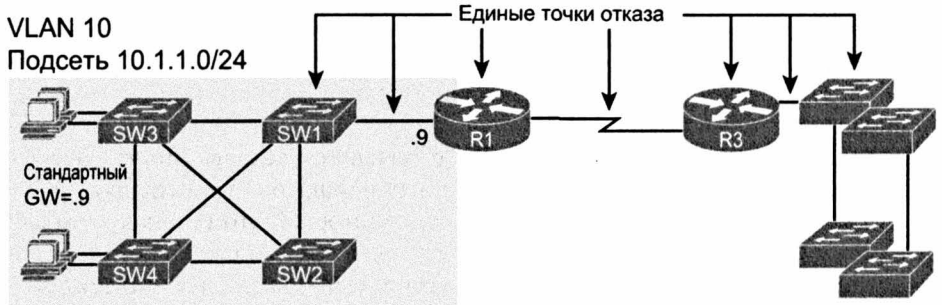


Рис. 6.1. Маршрутизатор R1 и единственный канал связи WAN как единые точки отказа

На рисунке несколько компонентов представлены как единые точки отказа. Если откажет любой из указанных компонентов, пакеты из левой части сети не смогут попасть в правую.

Обычно, чтобы улучшить доступность, сетевой инженер просматривает проект сети и находит единые точки отказа. Затем он решает, что и где добавить к сети, чтобы у одной (или нескольких) единой точки отказа появились избыточные компоненты, увеличивающие доступность. В частности, можно сделать следующее:

- добавить избыточные устройства и каналы связи;
- реализовать все функции, необходимые для применения избыточных устройств или каналов связи.

Например, из всех единых точек отказа на рис. 6.1 самой дорогой, вероятно, является канал связи WAN (из-за высокой ежемесячной оплаты). Кстати, каналы связи WAN — это наиболее вероятная причина отказа. Таким образом, наиболее разумной модификацией сети на рис. 6.1 является добавление канала связи WAN, возможно, даже подключенного к другому маршрутизатору в правой части сети (рис. 6.20.

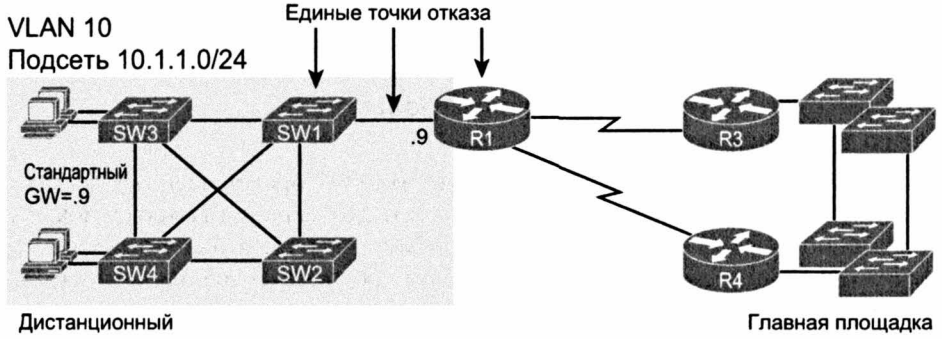


Рис. 6.2. Более высокая доступность, но маршрутизатор R1 — все еще единая точка отказа

Большинство проектов реальных корпоративных сетей похоже на рис. 6.2: один маршрутизатор на каждой дистанционной площадке и два канала связи WAN, соединяющих дистанционную площадку с избыточными маршрутизаторами на глав-

ной площадке (см. рис. 6.2, *справа*). По сравнению с рис. 6.1, у проекта на рис. 6.2 меньше единых точек отказа. Оставшиеся единые точки отказа создают риск, но это осознанный риск. Большинство связанных с ними проблем решает перезагрузка маршрутизатора, приводящая лишь к краткосрочному отключению. Но все еще существует риск полного выхода из строя аппаратных средств коммутатора или маршрутизатора, что требует времени на покупку, доставку и замену устройства, прежде чем площадка сможет возобновить работу.

Предприятия, способные позволить себе большие расходы, могут обеспечить еще более высокую доступность дистанционных площадок, защитившись от катастрофического отказа маршрутизатора или коммутатора. В этом конкретном случае добавляется еще один маршрутизатор в левую часть сети на рис. 6.2, что устраняет все отмеченные ранее единые точки отказа. На рис. 6.3 представлен проект со вторым маршрутизатором, подключенным к другому коммутатору LAN, чтобы коммутатор SW1 не был больше единой точкой отказа.

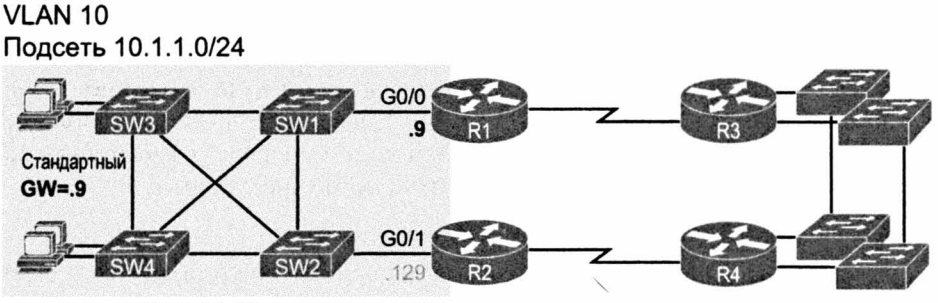


Рис. 6.3. Устранение всех единых точек отказа в проекте сети

ВНИМАНИЕ!

В проектах сетей крупных и средних предприятий довольно сложно найти баланс между необходимыми средствами технологий высокой доступности и доступными бюджетными средствами. На веб-сайте Cisco представлено много документов по проектам с применением технологий высокой доступности. Если есть желание узнать больше, ищите на `cisco.com` "high availability campus network design".

Необходимость в протоколе резервирования первого транзитного участка

Теперь вернемся к теме настоящей главы. Из всех представленных до сих пор проектов только в проекте на рис. 6.3, *слева*, есть два маршрутизатора в локальной сети, а именно в той же подсети и сети VLAN. Хотя наличие избыточных маршрутизаторов в той же подсети весьма полезно, оно также требует использования протокола FHRP.

Для демонстрации потребности и преимуществ использования протокола FHRP рассмотрим сначала, как эти избыточные маршрутизаторы используются в качестве стандартных маршрутизаторов хостами в сети VLAN 10 подсети 10.1.1.0/24. Логика хоста остается неизменной, поэтому у каждого хоста будет только один параметр

стандартного маршрутизатора. Поэтому для параметров стандартного маршрутизатора применимы следующие возможности.

- Все хосты в подсети используют как стандартный маршрутизатор R1 (10.1.1.9), а в случае его отказа статически перенастраивают свой параметр стандартного маршрутизатора на маршрутизатор R2 (10.1.129).
- Все хосты в подсети используют как стандартный маршрутизатор R2 (10.1.1.129), а в случае его отказа статически перенастраивают свой параметр стандартного маршрутизатора на маршрутизатор R1 (10.1.1.9).
- Половина хостов использует как стандартный маршрутизатор R1, а половина — маршрутизатор R2, и если любой из маршрутизаторов терпит неудачу, то половина пользователей статически перенастраивает параметр стандартного маршрутизатора.

Чтобы было понятней, на рис. 6.4 показана третья возможность, когда половина хостов использует как стандартный маршрутизатор R1, а другая — маршрутизатор R2. Коммутаторы LAN на рисунке удалены, чтобы не загромождать его. Хосты A и B используют как стандартный маршрутизатор R1, а хосты C и D — маршрутизатор R2.

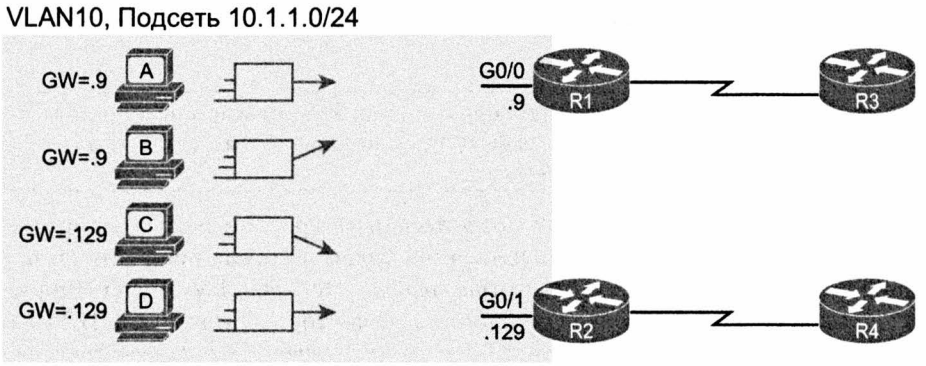


Рис. 6.4. Балансировка трафика за счет назначения разных стандартных маршрутизаторов разным клиентам

У всех этих возможностей есть недостатки: меры должны принять пользователи. Они должны знать, что произошло отключение, уметь перенастроить свой параметр стандартного маршрутизатора и знать, когда изменить его на первоначальный.

Протокол FHRP справляется с этой работой лучше. Оба эти маршрутизатора выглядят как один стандартный маршрутизатор. Пользователи никогда ничего не должны делать: их параметр стандартного маршрутизатора остается тем же, и их таблица ARP также остается той же.

Чтобы избавить хосты от изменений, маршрутизаторы должны предпринять еще несколько действий, определенных в соответствии с одним из протоколов FHRP. Все протоколы FHRP имеют следующие общие характеристики.

Ключевая тема **Общие характеристики всех протоколов FHRP**

1. Все хосты действуют так, как будто все они имеют один стандартный маршрутизатор, параметр которого никогда не нужно изменять.
2. Стандартные маршрутизаторы совместно используют виртуальный IP-адрес в подсети, определенной протоколом FHRP.
3. В качестве адреса стандартного маршрутизатора хосты используют виртуальный IP-адрес протокола FHRP.
4. Чтобы согласовать работу, выполняемую каждым маршрутизатором в каждый момент времени, маршрутизаторы обмениваются сообщениями протокола FHRP.
5. Когда маршрутизатор отказывает или возникает другая проблема, другие маршрутизаторы используют протокол FHRP для выбора, какой маршрутизатор примет на себя обязанности отказавшего.

Три решения для избыточности первого транзитного участка

По сути, *протокол резервирования первого транзитного участка* (First Hop Redundancy Protocol — FHRP) — это название не протокола, а целого семейства протоколов, играющих ту же роль. Для сети, показанной на рис. 6.4, *слева*, инженер выбрал бы один из протоколов семейства FHRP.

ВНИМАНИЕ!

Часть *первый транзитный участок* (first hop) в названии — это упоминание стандартного маршрутизатора, являющегося первым маршрутизатором или первым транзитным участком, через который должен проследовать пакет.

В табл. 6.1 три протокола FHRP представлены в хронологическом порядке, на основании времени начала их использования. Сначала компания Cisco ввела собственный *протокол резервного маршрутизатора* (Hot Standby Router Protocol — HSRP), и он хорошо работал для большинства клиентов. Впоследствии IETF выпустил документ RFC для очень похожего протокола — *протокола резервирования виртуального маршрутизатора* (Virtual Router Redundancy Protocol — VRRP). И наконец, компания Cisco разработала еще более надежную версию — *протокол балансировки нагрузки шлюза* (Gateway Load Balancing Protocol — GLBP).

Ключевая тема **Таблица 6.1. Три протокола семейства FHRP**

Акроним	Полное название	Источник	Подход к избыточности	Балансировка нагрузки
HSRP	Протокол резервного маршрутизатора	Cisco	Активный/резервный	По подсетям
VRRP	Протокол резервирования виртуального маршрутизатора	IETF (RFC 5798)	Активный/резервный	По подсетям
GLBP	Протокол балансировки нагрузки шлюза	Cisco	Активный/активный	По хостам

Далее рассматриваются концепции и работа протоколов HSRP и GLBP. У протоколов HSRP и VRRP много сходств, поэтому в данной книге есть раздел, посвя-

щенный протоколу HSRP, и нет раздела, посвященного протоколу VRRP. В этих и последующих разделах рассматриваются значение различных подходов к избыточности (активный/резервный и активный/активный), а также различия в способах балансировки нагрузки.

Концепции протокола HSRP

Протокол HSRP работает в соответствии с моделью *активный/резервный* (или *активный/пассивный*). Протокол HSRP позволяет взаимодействовать двум (или более) маршрутизаторам, выступая в роли единого стандартного маршрутизатора. Но в каждый конкретный момент только один маршрутизатор активно поддерживает трафик конечного пользователя. Пакеты, посланные хостами на стандартный маршрутизатор, поступают на этот активный маршрутизатор. Другие маршрутизаторы, находящиеся в состоянии ожидания (HSRP Standby), терпеливо ждут, пока откажет активный маршрутизатор HSRP, и они вступят в дело.

Маршрутизатор в активном состоянии (HSRP Active) реализует виртуальный IP-адрес и соответствующий виртуальный MAC-адрес. Этот виртуальный IP-адрес является частью конфигурации HSRP и дополнительным элементом по сравнению с обычной подкомандой интерфейса `ip address`. Виртуальный IP-адрес находится в той же подсети, что и IP-адрес интерфейса, но это другой IP-адрес. Затем маршрутизатор автоматически создает виртуальный MAC-адрес. Всем взаимодействующим маршрутизаторам HSRP известны эти виртуальные адреса, но в каждый момент времени эти адреса использует только активный маршрутизатор HSRP.

В качестве адреса стандартного маршрутизатора хосты используют этот виртуальный IP-адрес, а не IP-адрес интерфейса конкретного маршрутизатора. Например, маршрутизаторы R1 и R2 на рис. 6.5 используют протокол HSRP. Виртуальный IP-адрес HSRP 10.1.1.1 комплектуется виртуальным MAC-адресом, для простоты обозначенным как VMAC1.

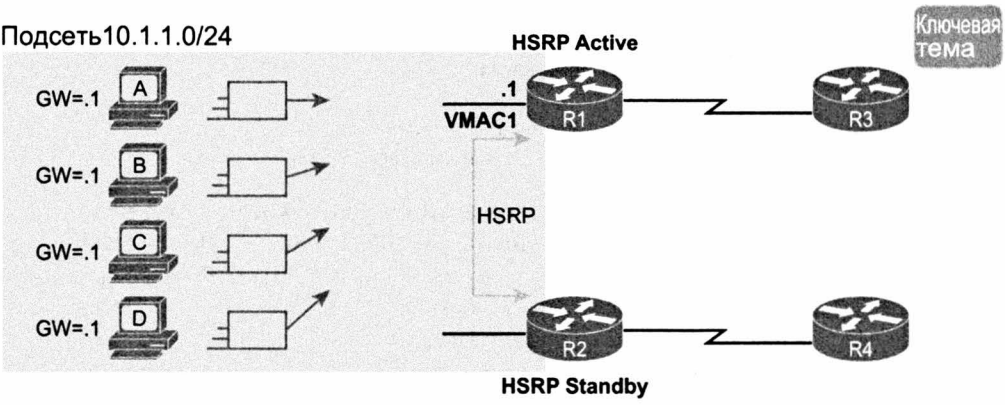


Таблица ARP хоста

IP	MAC
10.1.1.1	**VMAC1**

Рис. 6.5. Весь трафик поступает на адрес .1 (маршрутизатор R1 — активный, R2 — резервный)

Отказоустойчивая архитектура HSRP

Чтобы протокол HSRP выполнял в сети функции, показанные на рис. 6.5, на каждом маршрутизаторе следует выполнить некие действия. Оба маршрутизатора нуждаются в конфигурации HSRP, включая виртуальный IP-адрес. Чтобы провести переговоры и решить, какой маршрутизатор в настоящее время должен быть активным, а какой резервным, маршрутизаторы обмениваются сообщениями HSRP. Маршрутизаторы продолжают обмениваться сообщениями, чтобы резервный маршрутизатор мог узнать об отказе текущего активного маршрутизатора и стал новым активным маршрутизатором.

На рис. 6.6. представлен момент отказа маршрутизатора R1, находившегося в состоянии HSRP Active. Маршрутизатор R1 прекращает использовать виртуальные IP- и MAC-адреса, а новый активный маршрутизатор R2 начинает их использовать. Хосты не должны изменять свои параметры стандартного маршрутизатора вообще, трафик теперь пойдет через маршрутизатор R2 вместо маршрутизатора R1.

Ключевая тема

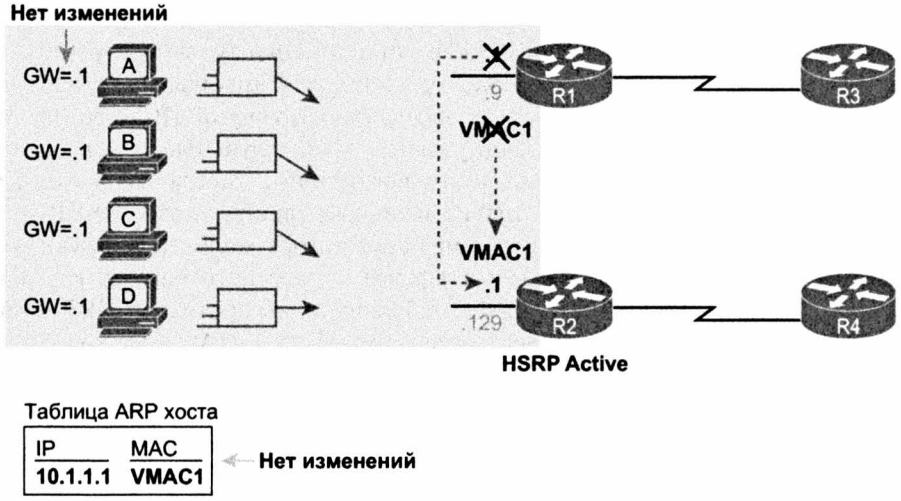


Рис. 6.6. Как только откажет маршрутизатор R1, посланные пакеты пройдут через маршрутизатор R2 (новый активный)

В случае применения отказоустойчивой архитектуры некоторые изменения действительно происходят, но ни одно из них не затрагивает хосты. На хостах остается тот же параметр стандартного маршрутизатора — виртуальный IP-адрес (в данном случае 10.1.1.1). Таблица ARP хоста также останется неизменной — MAC-адресом останется MAC-адрес виртуального маршрутизатора HSRP.

Изменения в безотказной архитектуре затрагивают маршрутизаторы и коммутаторы LAN. Безусловно, новый активный маршрутизатор должен быть готов получать пакеты (заключенные во фреймы), используя виртуальные IP- и MAC-адреса. Однако коммутаторы LAN, скрытые на нескольких последних рисунках, прежде передавали фреймы на виртуальный адрес VMAC1 маршрутизатору R1. Теперь коммутаторам следует указать, чтобы они передавали фреймы на новый активный маршрутизатор, R2.

Чтобы заставить коммутаторы изменить записи своих таблиц MAC-адресов для адреса VMAC1, маршрутизатор R2 посылает фрейм Ethernet с адресом VMAC1 в качестве MAC-адреса отправителя. Коммутаторы, как обычно, изучают MAC-адреса отправителей (VMAC1), но с новыми портами к маршрутизатору R2. Фрейм является широковещательным, поэтому все коммутаторы заносят в свои таблицы MAC-адресов адрес VMAC1 к маршрутизатору R2. (Между прочим, этот фрейм Ethernet содержит сообщение ARP Reply, называемое *беспричинным* (gratuitous), поскольку маршрутизатор посылает его без первоначального запроса ARP Request.)

Балансировка нагрузки HSRP

Модель HSRP активный/резервный означает, что все хосты в одной подсети передают пакеты во вне подсети только через один маршрутизатор. Другими словами, маршрутизаторы не делят нагрузку, все пакеты обрабатывает один маршрутизатор. Например, на рис. 6.5 маршрутизатор R1 был активным, поэтому все хосты в подсети передавали свои пакеты через него, и ни один из них не передавал пакеты через маршрутизатор R2.

Протокол HSRP обеспечивает балансировку нагрузки за счет предпочтения разных маршрутизаторов в качестве активных в разных подсетях. Большинство площадок, требующихся для избыточности второго маршрутизатора, достаточно велики для использования нескольких сетей VLAN, подсетей и площадок. Эти два маршрутизатора, вероятно, соединены со всем сетями VLAN, действуя в роли стандартного маршрутизатора в каждой VLAN. Протокол HSRP может быть настроен так, чтобы в одной сети VLAN предпочтительным на роль активного был один маршрутизатор, а в другой сети VLAN — другой маршрутизатор, что балансирует трафик.

Например, на рис. 6.7 представлен измененный проект LAN, теперь уже с двумя хостами в сети VLAN 1 и двумя хостами в сети VLAN 2. Оба маршрутизатора, R1 и R2, подключены к локальной сети, оба используют магистральное соединение VLAN и конфигурацию "маршрутизатор на палочке" (ROAS). Оба маршрутизатора используют протокол HSRP в каждой из двух подсетей, поддерживая друг друга. Но маршрутизатор R1 нарочно был настроен так, чтобы выиграть переговоры и стать активным в сети VLAN 1, а маршрутизатор R2 был настроен так, чтобы победить в сети VLAN 2.

Обратите внимание: когда каждый из маршрутизаторов является активным в некоторых подсетях, проект задействует оба маршрутизатора и оба канала связи WAN.

ВНИМАНИЕ!

В проектах, использующих коммутаторы уровня 3, как стандартный маршрутизатор хостов действуют именно они. В этом случае конфигурация HSRP располагается на коммутаторе уровня 3. Альтернативная конфигурация представлена на рис. 6.7, она подразумевает использование магистрального соединения VLAN на маршрутизаторах с коммутаторами уровня 2 в локальной сети.

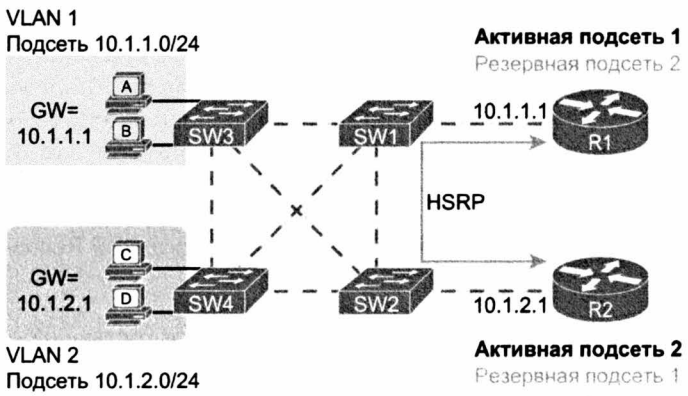


Рис. 6.7. Балансировка нагрузки протоколом HSRP при использовании разных активных маршрутизаторов в подсетях

Концепции протокола GLBP

Протоколы HSRP и VRRP, появившиеся перед протоколом балансировки нагрузки шлюза (GLBP), балансировали нагрузку между подсетями, как показано на рис. 6.7. Но поскольку объем трафика в разных сетях непредсказуем, компании Cisco потребовался новый протокол семейства FHRP с лучшими возможностями по балансировке нагрузки, чем просто балансировка по подсетям, как у протоколов HSRP и VRRP. Для удовлетворения этой потребности компания Cisco разработала протокол GLBP.

Протокол GLBP балансирует нагрузку по каждому хосту, используя в каждой подсети модель активный/активный. Каждый маршрутизатор GLBP в подсети получает пакеты для внешних подсетей от хостов внутри подсети. На каждом хосте все еще можно настроить одинаковый параметр стандартного шлюза и не вносить изменений при его отказе.

Протокол GLBP создает обстановку, которая на первый взгляд выглядит как при использовании протокола HSRP, но с некоторыми отличиями, позволяющими балансировать трафик. На всех маршрутизаторах задается виртуальный IP-адрес, используемый хостами как адрес их стандартного маршрутизатора. Как и при протоколе HSRP, хосты используют параметр стандартного маршрутизатора, указывающий на виртуальный IP-адрес, и этот параметр не должен изменяться. Протокол GLBP отличается от протокола HSRP используемыми MAC-адресами и процессом ARP, поскольку для балансировки трафика от разных хостов к разным маршрутизаторам протокол GLBP фактически использует сообщения ARP Reply.

При использовании протокола GLBP один маршрутизатор действует как *активный виртуальный шлюз* (Active Virtual Gateway — AVG). Шлюз AVG отвечает на все запросы ARP о виртуальном IP-адресе. У каждого маршрутизатора есть индивидуальный виртуальный MAC-адрес, чтобы один шлюз AVG мог отвечать на запросы ARP с одним виртуальным MAC-адресом, а другой — с другим. В результате одни хосты в подсети посылают фреймы на MAC-адрес Ethernet одного маршрутизатора, а другие хосты — на MAC-адрес второго маршрутизатора.

В качестве примера на рис. 6.8 представлен процесс балансировки протоколом GLBP трафика хоста на основании ответных сообщений протокола преобразования

адресов (ARP Reply), посланных шлюзом AVG (маршрутизатором R1). На рисунке использованы те же IP-адреса, что и ранее в примерах протокола HSRP на рис. 6.5 и 6.6. Оба маршрутизатора поддерживают виртуальный IP-адрес 10.1.1.1, а хосты используют его как параметр стандартного маршрутизатора.

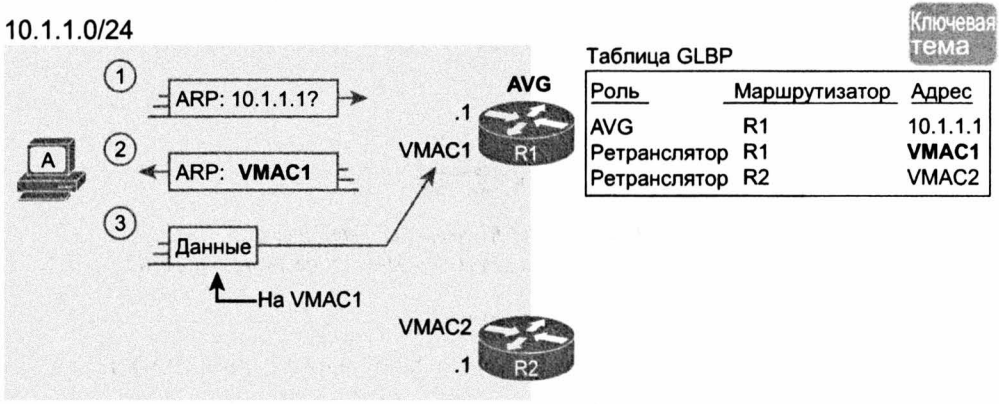


Рис. 6.8. Протокол GLBP настраивает хост A, возвращая сообщение ARP Reply с адресом VMAC1 маршрутизатора R1

На рисунке (сверху вниз) представлены три следующих сообщения.

1. В таблице ARP хоста A нет записи для стандартного маршрутизатора (10.1.1.1), поэтому хост A посылает запрос ARP Request, чтобы узнать его MAC-адрес.
2. Шлюз AVG протокола GLBP (в данном случае R1) отвечает сообщением ARP Reply, содержащим его собственный виртуальный MAC-адрес VMAC1.
3. Следующие внешние пакеты IP, посланные хостом A, инкапсулируются во фреймы Ethernet, направляющиеся на адрес VMAC1 маршрутизатору R1.

С этого момента хост A посылает внешние пакеты на маршрутизатор R1, поскольку в его таблице ARP уже есть запись для стандартного шлюза (10.1.1.1). Запись в таблице ARP хоста A для адреса 10.1.1.1 ссылается теперь на MAC-адрес маршрутизатора R1 (VMAC1), поэтому посланные во вне пакеты отправляются через маршрутизатор R1.

Для балансировки нагрузки шлюз AVG отвечает на каждый новый запрос ARP сообщением с MAC-адресом другого маршрутизатора. На рис. 6.9 представлена балансировка нагрузки с запросом ARP по адресу 10.1.1.1, исходящим от хоста B. Выступающий в роли шлюза AVG маршрутизатор (R1) снова отсылает ответ ARP, но уже с виртуальным MAC-адресом маршрутизатора R2 (VMAC2).

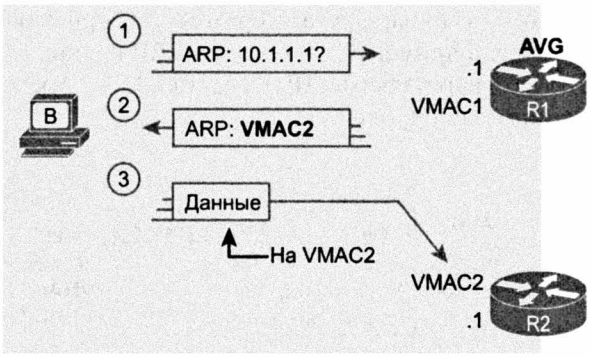


Таблица GLBP

Роль	Маршрутизатор	Адрес
AVG	R1	10.1.1.1
Ретранслятор	R1	VMAC1
Ретранслятор	R2	**VMAC2**

Рис. 6.9. Протокол GLBP настраивает хост B, возвращая сообщение ARP Reply с адресом VMAC2 маршрутизатора R2

На рисунке представлены следующие этапы.

1. Хост B посылает запрос ARP, чтобы узнать MAC-адрес шлюза 10.1.1.1.
2. Шлюз AVG протокола GLBP (R1) отвечает сообщением ARP Reply, содержащим виртуальный MAC-адрес VMAC2 маршрутизатора R2.
3. Следующие внешние пакеты IP, посланные хостом B, инкапсулируются во фреймы Ethernet, направляющиеся на адрес VMAC2 маршрутизатору R2.

Представленный на рис. 6.8 и 6.9 процесс балансирует трафик по каждому хосту, но маршрутизаторы должны также быть готовы принять на себя функции другого маршрутизатора, если он откажет. Протокол GLBP рассматривает каждый маршрутизатор как ретранслятор. Пока все работает нормально, каждый маршрутизатор действует как ретранслятор для их собственного виртуального MAC-адреса, но они прослушивают сообщения GLBP, чтобы удостовериться в работоспособности других ретрансляторов. Если другой ретранслятор откажет, то все еще работающий ретранслятор примет на себя роль отказавшего и продолжит перенаправлять трафик.

Настройка и проверка FHRP

Во втором разделе этой главы рассматриваются настройка базовых функций протоколов HSRP и GLBP, а также соответствующие команды `show`. В разделе будет продемонстрирована работа каждого инструмента, чтобы закрепить понимание концепций, обсуждаемых в предыдущем разделе.

Настройка и проверка протокола HSRP

Настройка протокола HSRP требует только одной команды на двух (или более) маршрутизаторах, предназначенных для совместного выполнения обязанностей стандартного маршрутизатора, — это подкоманда интерфейса `standby` *`номер_группы`* `ip` *`виртуальный-ip`*. Первое значение задает номер группы HSRP, он должен совпадать на обоих маршрутизаторах. Номер группы позволяет одному маршрутизатору поддерживать несколько групп HSRP одновременно, а также позволяет маршрутизаторам идентифицировать друг друга на основании группы. Ко-

манда задает также виртуальный IP-адрес, совместно используемый маршрутизаторами той же группы.

В примере 6.1 показана конфигурация, соответствующая схемам на рис. 6.5 и 6.6. Оба маршрутизатора используют группу 1 с виртуальным IP-адресом 10.1.1.1 и подкоманду интерфейса `standby 1 ip 10.1.1.1`.

Пример 6.1. Конфигурация HSRP на маршрутизаторах R1 и R2, совместно использующих IP-адрес 10.1.1.1

```
R1# show running-config
! Строки опущены для краткости
interface GigabitEthernet0/0
  ip address 10.1.1.9 255.255.255.0
  standby version 2
  standby 1 ip 10.1.1.1
  standby 1 priority 110
  standby 1 name HSRP-group-for-book
! ------------------------------------------------------------
! Следующая конфигурация, на маршрутизаторе R2, идентична, за исключением
! приоритета, IP-адреса интерфейса и приоритета HSRP
R2# show running-config
! Строки опущены для краткости
interface GigabitEthernet0/0
  ip address 10.1.1.129 255.255.255.0
  standby version 2
  standby 1 ip 10.1.1.1
  standby 1 name HSRP-group-for-book
```

Конфигурация демонстрирует и другие необязательные параметры. Например, маршрутизатор R1 имеет в этой группе приоритет 110, а маршрутизатор R2 — стандартное значение 100. Если при использовании протокола HSRP оба маршрутизатора одновременно находятся в состоянии `up`, то роль активного выигрывает маршрутизатор с более высоким приоритетом. Конфигурация демонстрирует также присвоенное группе имя (при использовании `show` команды) и версию (2) протокола HSRP.

После настройки маршрутизаторы договариваются о параметрах HSRP и выбирают, какой маршрутизатор в настоящее время будет активным, а какой резервным. В представленной выше конфигурации на выборах победит маршрутизатор R1 и станет активным из-за более высокого приоритета. Оба маршрутизатора сделали тот же выбор, как подтверждает вывод команды `show standby brief`, на маршрутизаторах R1 и R2 в примере 6.2.

Пример 6.2. Состояние протокола HSRP на маршрутизаторах R1 и R2 согласно выводу команды `show standby brief`

```
! Сначала состояние группы на маршрутизаторе R1
R1# show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P  State    Active    Standby     Virtual IP
Gi0/0       1    110    Active   local     10.1.1.129  10.1.1.1
! ------------------------------------------------------------------
! Вывод далее подтверждает, что маршрутизатор R2 согласен с R1.
R2# show standby brief
```

```
                    P indicates configured to preempt.
                    |
Interface   Grp  Pri P  State    Active    Standby     Virtual IP
Gi0/0       1    100    Standby  10.1.1.9  local       10.1.1.1
```

Сначала рассмотрим столбец `Grp` каждой команды. Он содержит номер группы HSRP, поэтому при просмотре вывода нескольких маршрутизаторов следует искать строки с тем же номером группы, чтобы выяснить данные, относящиеся к этой группе HSRP. В данном случае у обоих маршрутизаторов только один номер группы (1), поэтому найти информацию просто.

Каждая строка вывода отображает состояние HSRP данного маршрутизатора для этой группы. В частности, столбцы в выводе команды `show standby brief` отображают следующую информацию.

Ключевая тема **Интерпретация вывода команды `show standby brief`**

- `Interface`. Интерфейс локального маршрутизатора, на котором настроена группа HSRP.
- `Grp`. Номер группы HSRP.
- `Pri`. Приоритет локального маршрутизатора HSRP.
- `State`. Текущее состояние локального маршрутизатора HSRP.
- `Active`. IP-адрес интерфейса активного в настоящее время маршрутизатора HSRP (или слово "local", если активен локальный маршрутизатор).
- `Standby`. IP-адрес интерфейса резервного в настоящее время маршрутизатора HSRP (или слово "local", если резервным является локальный маршрутизатор).
- `Virtual IP`. Виртуальный IP-адрес, заданный для этой группы.

Например, согласно выделенным фрагментам в примере 6.2, маршрутизатор R2 считает свое текущее состояние резервным, а активен маршрутизатор с адресом интерфейса 10.1.1.9, что и подтверждает слово "local" в столбце `Standby` вывода команды на маршрутизаторе R2.

Как можно заметить, вывод команды `show standby brief` содержит много подробностей в каждой строке. По сравнению с ней команда `show standby` выводит более подробное описание текущего состояния. Пример 6.3 демонстрирует новую информацию, выводимую командой `show standby`, включая несколько счетчиков и таймеров, относящихся к самому протоколу HSRP, плюс виртуальный MAC-адрес 0000.0c9f.f001.

Пример 6.3. Состояние протокола HSRP на маршрутизаторах R1 и R2 согласно выводу команды `show standby`

```
R1# show standby
GigabitEthernet0/0 - Group 1 (version 2)
  State is Active
    6 state changes, last state change 00:12:53
  Virtual IP address is 10.1.1.1
  Active virtual MAC address is 0000.0c9f.f001
```

```
    Local virtual MAC address is 0000.0c9f.f001 (v2 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.696 secs
  Preemption disabled
  Active router is local
  Standby router is 10.1.1.129, priority 100 (expires in 8.096 sec)
  Priority 110 (configured 110)
  Group name is "HSRP-group-for-book" (cfgd)
! ------------------------------------------------
! Вывод далее подтверждает, что R2 согласен с R1.
R2# show standby
GigabitEthernet0/0 - Group 1 (version 2)
  State is Standby
    4 state changes, last state change 00:12:05
  Virtual IP address is 10.1.1.1
  Active virtual MAC address is 0000.0c9f.f001
    Local virtual MAC address is 0000.0c9f.f001 (v2 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.352 secs
  Preemption disabled
  Active router is 10.1.1.9, priority 110 (expires in 9.136 sec)
    MAC address is 0200.0101.0101
  Standby router is local
  Priority 100 (default 100)
  Group name is "HSRP-group-for-book" (cfgd)
```

Настройка и проверка протокола GLBP

Настройка протокола GLBP очень похожа на таковую у протокола HSRP. Фактически, если взять конфигурацию в примере 6.1, удалить команду `standby version 2` (применимую только для протокола HSRP) и заменить каждое `standby` на `glbp`, получится совершенно правильная конфигурация GLBP.

Протокол GLBP требует только одной подкоманды интерфейса на каждом маршрутизаторе: `glbp` *`номер_группы`* `ip` *`виртуальный-ip`*. Идея этой команды точно такая же, как и у протокола HSRP: все маршрутизаторы используют одинаковый номер группы, на всех маршрутизаторах настроен тот же виртуальный IP-адрес.

Пример 6.4 демонстрирует типичную конфигурацию GLBP, характерную при переходе с конфигурации HSRP, показанной в примере 6.1, на эквивалентную конфигурацию GLBP. Оба маршрутизатора используют группу 1 и виртуальный IP-адрес 10.1.1.1, согласно подкоманде интерфейса `glbp 1 ip 10.1.1.1`.

Пример 6.4. Конфигурация GLBP на маршрутизаторах R1 и R2, совместно использующих IP-адрес 10.1.1.1

```
! Сначала конфигурация на маршрутизаторе R1
R1# show running-config
! Строки опущены для краткости
interface GigabitEthernet0/0
  ip address 10.1.1.9 255.255.255.0
  glbp 1 ip 10.1.1.1
  glbp 1 priority 110
  glbp 1 name GLBP-group-for-book
! ------------------------------------------------------------------
! Следующая конфигурация, на маршрутизаторе R2, идентична, за исключением
```

```
! приоритета, IP-адреса интерфейса и приоритета GLBP

R2# show running-config
! Строки опущены для краткости
interface GigabitEthernet0/0
  ip address 10.1.1.129 255.255.255.0
  glbp 1 ip 10.1.1.1
  glbp 1 name HSRP-group-for-book
```

После настройки оба маршрутизатора ведут переговоры о том, кто станет шлюзом AVG. Как и при использовании протокола HSRP, если оба работоспособны, то победит маршрутизатор R1 благодаря заданному командой `glbp 1 priority 110` приоритету 110, по сравнению со стандартным приоритетом 100 у маршрутизатора R2. Но если первый маршрутизатор откажет, то роль шлюза AVG примет на себя другой.

Ввод команды `show` для протокола GLBP содержит немного больше подробностей. Сначала рассмотрим команду `show glbp brief` на маршрутизаторе R1, представленную в примере 6.5. (Обратите внимание, что у многих команд `show glbp` те же возможности, что и у эквивалентных команд `show standby` протокола HSRP.)

Пример 6.5. Состояние протокола GLBP на маршрутизаторе R1 согласно выводу команды `show glbp brief`

```
R1# show glbp brief
Interface Grp Fwd Pri State   Address         Active router   Standby router
Gi0/0     1   -   110 Active  10.1.1.1        local           10.1.1.129
Gi0/0     1   1   -   Listen  0007.b400.0101  10.1.1.129      -
Gi0/0     1   2   -   Active  0007.b400.0102  local
```

Прежде чем изучать правую сторону вывода, рассмотрим контекст. Вывод содержит строку заголовка и три строки данных. Колонки `Grp` и `Fwd` содержат данные о группе и ретрансляторе. Поскольку настроена только одна группа GLBP, строки вывода для маршрутизатора R1 указывают только группу 1. Важней всего то, что каждая строка содержит целый набор различных подробностей GLBP.

Ключевая тема

Смысл значений в колонке `Fwd` вывода команды `show glbp brief`

- -. Эта строка не относится ни к одному из ретрансляторов, она описывает шлюз AVG.
- 1. Эта строка описывает ретранслятор GLBP 1 (маршрутизатор).
- 2. Эта строка описывает ретранслятор GLBP 2 (маршрутизатор).

Строка о шлюзе AVG (с черточкой в столбце `Fwd`) обычно выводится первой. Теперь рассмотрим выделенные части в правой стороне примера 6.5. Здесь представлен виртуальный IP-адрес и идентифицированы активный и резервный шлюзы AVG. Данная конкретная команда, на маршрутизаторе R1, указывает как активный шлюз AVG текущий маршрутизатор, R1, ("local").

Строка каждого ретранслятора идентифицирует маршрутизатор, в настоящее время использующий виртуальный MAC-адрес, указанный в столбце `Active router`. В примере 6.5 адрес 0007.b400.0101 используется маршрутизатором с IP-

адресом интерфейса 10.1.1.129 (в данном случае R2). Адрес 0007.b400.0102 поддерживается локальным маршрутизатором (на котором была введена команда), и это маршрутизатор R1.

Краткий вывод команды `show glbp brief` содержит много подробностей, но требует неких усилий для понимания. Для полноты картины пример 6.6 содержит вывод той же команды `show glbp brief`, но на сей раз на маршрутизаторе R2. Обратите внимание, что в столбце `Fwd` снова первой расположена строка о шлюзе AVG, а две следующие посвящены двум ретрансляторам.

Пример 6.6. Состояние протокола GLBP на маршрутизаторе R2 согласно выводу команды `show standby brief`

```
R1# show glbp brief
Interface   Grp  Fwd Pri State   Address         Active router   Standby router
Gi0/0       1    -   100 Standby 10.1.1.1        10.1.1.9        local
Gi0/0       1    1   -   Active  0007.b400.0101  local           -
Gi0/0       1    2   -   Listen  0007.b400.0102  10.1.1.9        -
```

Столбец `State` в примерах 6.5 и 6.6 вывода способен объединить концепции GLBP. Для определения смысла значений состояния ниже приведен краткий список состояний, ожидаемых в первой строке вывода о шлюзе AVG, а затем о каждом ретрансляторе GLBP.

Различные состояния, ожидаемые для шлюза AVG и ретрансляторов GLBP

Ключевая тема

AVG. Один маршрутизатор должен быть активным шлюзом AVG, а другие должны находиться в резерве и быть готовыми принять роль шлюза AVG, если текущей шлюз откажет.

Ретрансляторы. Один маршрутизатор должен быть активным, а другой должен слушать, будучи готовым принять этот виртуальный MAC-адрес, если активный ретранслятор откажет.

В табл. 6.2 представлены значения столбца `State` из примеров 6.5 и 6.6. Для простоты они приведены рядом. Обратите внимание на наличие в строках пар active/standby (активный/резервный) для AVG или active/listen (активный/прослушивающий) — для ретрансляторов.

Таблица 6.2. Сравнение локальных состояний в командах `show glbp brief`

Строка о ...	Значения в столбце `Fwd`	Состояние R1	Состояние R2
AVG	-	Active	Standby
Ретранслятор 1	1	Listen	Active
Ретранслятор 2	2	Active	Listen

И наконец, команда `show glbp` выводит текущее состояние GLBP более подробно. В примере 6.7 показан вывод на маршрутизаторе R1. Обратите внимание, что в первой половине вывода содержится информация, подобная таковой у команды `show standby`, плюс IP- и MAC-адреса маршрутизаторов в группе GLBP. В конце вывода содержится группа сообщений по каждому ретранслятору GLBP.

Пример 6.7. Состояние протокола GLBP на маршрутизаторе R1 согласно выводу команды `show glbp`

```
R1# show glbp
GigabitEthernet0/0 - Group 1
  State is Active
    2 state changes, last state change 00:20:59
  Virtual IP address is 10.1.1.1
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.112 secs
  Redirect time 600 sec, forwarder timeout 14400 sec
  Preemption disabled
  Active is local
  Standby is 10.1.1.129, priority 100 (expires in 8.256 sec)
  Priority 110 (configured)
  Weighting 100 (default 100), thresholds: lower 1, upper 100
  Load balancing: round-robin
  IP redundancy name is "GLBP-group-for-book"
  Group members:
    0200.0101.0101 (10.1.1.9) local
    0200.0202.0202 (10.1.1.129)
  There are 2 forwarders (1 active)
  Forwarder 1
    State is Listen
      2 state changes, last state change 00:20:34
  MAC address is 0007.b400.0101 (learnt)
  Owner ID is 0200.0202.0202
  Redirection enabled, 598.272 sec remaining (maximum 600 sec)
  Time to live: 14398.272 sec (maximum 14400 sec)
  Preemption enabled, min delay 30 sec
  Active is 10.1.1.129 (primary), weighting 100 (expires in 8.352 sec)
  Client selection count: 1
Forwarder 2
  State is Active
    1 state change, last state change 00:24:25
  MAC address is 0007.b400.0102 (default)
  Owner ID is 0200.0101.0101
  Redirection enabled
  Preemption enabled, min delay 30 sec
  Active is local, weighting 100
  Client selection count: 1
```

Обзор

Резюме

- Термин *протокол резервирования первого транзитного участка* обозначает не протокол, а целое семейство протоколов, играющих ту же роль.
- Сети нуждаются в избыточных каналах связи для улучшения доступности сети.
- Для улучшения доступности сетевой инженер просматривает проект сети и находит единые точки отказа.
- При использования протокола FHRP стандартные маршрутизаторы в подсети совместно используют виртуальный IP-адрес, и этот адрес используется хостами как их адрес стандартного маршрутизатора.
- Протокол HSRP работает в соответствии с моделью активный/резервный (или активный/пассивный).
- Чтобы провести переговоры и решить, какой маршрутизатор в настоящее время должен быть активным, а какой резервным, маршрутизаторы обмениваются сообщениями HSRP.
- Протокол HSRP обеспечивает балансировку нагрузки за счет предпочтения разных маршрутизаторов в качестве активных в разных подсетях.
- Протокол GLBP балансирует нагрузку по каждому хосту, используя в каждой подсети модель активный/активный. Каждый маршрутизатор GLBP в подсети получает пакеты для внешних подсетей от хостов внутри подсети.
- Для балансировки трафика от разных хостов к разным маршрутизаторам протокол GLBP фактически использует сообщения ARP Reply.
- Если другой ретранслятор откажет, то все еще работающий ретранслятор примет на себя роль отказавшего и продолжит перенаправлять трафик.

Контрольные вопросы

Ответьте на эти вопросы. Ответы можно найти на последней странице главы. Полное объяснение ответов приведено в приложении B на веб-сайте.

1. Маршрутизаторы R1 и R2 подключены к той же сети VLAN Ethernet, с подсетью 10.1.19.0/25 и адресами 10.1.19.1 и 10.1.19.2 соответственно, заданными подкомандой интерфейса `ip address`. Хост A использует стандартный маршрутизатор 10.1.19.1, а хост B — стандартный маршрутизатор 10.1.19.2. Маршрутизаторы не используют протокол FHRP. Какая из следующих проблем присуща этой сети LAN?

   А) Проект нарушает правила IPv4-адресации, поскольку два маршрутизатора не могут быть подключены к той же подсети LAN.

   Б) Если откажет один маршрутизатор, ни один из хостов не сможет передавать пакеты вне подсети.

В) Если откажет один маршрутизатор, то оба хоста будут использовать оставшийся маршрутизатор как стандартный.

Г) Если откажет один маршрутизатор, использовавший его хост не сможет посылать пакеты вне подсети.

2. Маршрутизаторы R1 и R2 подключены к той же сети VLAN Ethernet, с подсетью 10.1.19.0/25 и адресами 10.1.19.1 и 10.1.19.2 соответственно, заданными подкомандой интерфейса `ip address`. Маршрутизаторы используют протокол FHRP. Хосты A и B подключены к той же сети LAN и имеют правильные параметры стандартного маршрутизатора в конфигурации FHRP. Какое из следующих утверждений истинно для этой сети LAN?

   А) Проект нарушает правила IPv4-адресации, поскольку два маршрутизатора не могут быть подключены к той же подсети LAN.

   Б) Если откажет один маршрутизатор, ни один из хостов не сможет передавать пакеты вне подсети.

   В) Если откажет один маршрутизатор, то оба хоста будут использовать оставшийся маршрутизатор как стандартный.

   Г) Если откажет один маршрутизатор, то только один из двух хостов все еще будет в состоянии посылать пакеты вне подсети.

3. Какой из следующих протоколов семейства FHRP использует модель активный/активный (по подсетям) для поддержки передачи трафика через первый транзитный участок (стандартный маршрутизатор) с двумя маршрутизаторами в той же сети LAN?

   А) GLBP.

   Б) HSRP.

   В) BFD.

   Г) VRRP.

4. Маршрутизаторы R1 и R2 подключены к той же сети VLAN Ethernet, с подсетью 10.1.19.0/25 и адресами 10.1.19.1 и 10.1.19.2 соответственно, заданными подкомандой интерфейса `ip address`. Маршрутизаторы используют протокол HSRP. Сетевой инженер предпочитает иметь стандартным маршрутизатор R1, когда оба маршрутизатора находятся в работоспособном состоянии. Что из следующего является параметром стандартного маршрутизатора для хостов в этой подсети?

   А) 10.1.19.1.

   Б) 10.1.19.2.

   В) Другой IP-адрес в подсети 10.1.19.0/25, отличный от 10.1.19.1 и 10.1.19.2.

   Г) Имя хоста, преобразуемое мини-DNS FHRP в адрес 10.1.19.1.

5. Ниже приведен вывод на маршрутизаторе R3, использующем протокол HSRP. Подсеть 10.1.12.0 использует маску 255.255.255.0. На основании вывода этой команды укажите, что из следующего истинно?

```
R3# show standby brief
Interface Grp Pri P State Active Standby Virtual IP
Gi0/0   1  105  Active local 10.1.12.1 10.1.12.2
```

А) Хосты с параметром стандартного маршрутизатора 10.1.12.1 посылают свои пакеты на маршрутизатор R3.

Б) Хосты с параметром стандартного маршрутизатора 10.1.12.2 посылают свои пакеты на маршрутизатор R3.

В) На интерфейсе G0/0 маршрутизатора R3 введена команда `ip address 10.1.12.2 255.255.255.0`.

Г) На интерфейсе G0/0 маршрутизатора R3 введена команда `ip address 10.1.12.1 255.255.255.0`.

6. Ниже приведен вывод на маршрутизаторе R3, использующем протокол GLBP. Подсеть 10.1.12.0 использует маску 255.255.255.0. На основании вывода этой команды укажите, что из следующего истинно?

```
R3# show glbp brief
Interface Grp Fwd Pri State   Address         Active router   Standby router
Gi0/0     1   -   100 Standby 10.1.12.2       10.1.12.4       local
Gi0/0     1   1   -   Active  0007.b400.0101  local           -
Gi0/0     1   2   -   Listen  0007.b400.0102  10.1.12.4       -
```

А) Маршрутизатор R3 является активным виртуальным шлюзом.

Б) Маршрутизатор с IP-адресом интерфейса 10.1.12.2, заданным командой `ip address`, является активным виртуальным шлюзом.

В) Маршрутизатор с IP-адресом интерфейса 10.1.12.4, заданным командой `ip address`, является активным виртуальным шлюзом.

Г) Вывод не идентифицирует активный виртуальный шлюз, поскольку концепция AVG относится к протоколу VRRP, а не GLBP.

Ключевые темы

Повторите все ключевые темы данной главы, отмеченные пиктограммой "Ключевая тема". Ключевые темы и соответствующие им страницы перечислены в табл. 6.3.

Таблица 6.3. Ключевые темы главы 6

Элемент	Описание	Страница
Список	Общие характеристики всех протоколов FHRP	236
Табл. 6.1	Три протокола семейства FHRP	236
Рис. 6.5	Весь трафик поступает на адрес .1 (маршрутизатор R1 — активный, R2 — резервный)	237
Рис. 6.6	Как только откажет маршрутизатор R1, посланные пакеты пройдут через маршрутизатор R2 (новый активный)	238
Рис. 6.8	Протокол GLBP настраивает хост A, возвращая сообщение ARP Reply с адресом VMAC1 маршрутизатора R1	241
Список	Интерпретация вывода команды show standby brief	244
Список	Смысл значений в колонке Fwd вывода команды show glbp brief	246
Список	Различные состояния, ожидаемые для шлюза AVG и ретрансляторов GLBP	247

Заполните таблицы и списки по памяти

Распечатайте приложение Г с веб-сайта или его раздел, относящийся к этой главе, и заполните таблицы и списки по памяти. В приложении Д приведены заполненные таблицы и списки для самоконтроля.

Ключевые термины

После первого прочтения главы попытайтесь дать определения следующим ключевым терминам. Но не расстраивайтесь, если не все получится сразу, в главе 22 описано, как использовать эти термины на завершающем этапе подготовки к экзамену.

единая точка отказа (single point of failure), протокол резервирования первого транзитного участка (First Hop Redundancy Protocol — FHRP), протокол резервного маршрутизатора (Hot Standby Router Protocol — HSRP), протокол резервирования виртуального маршрутизатора (Virtual Router Redundancy Protocol — VRRP), протокол балансировки нагрузки шлюза (Gateway Load Balancing Protocol — GLBP), виртуальный IP-адрес (virtual IP address), виртуальный MAC-адрес (virtual MAC address), состояние HSRP active (HSRP active), состояние HSRP standby (HSRP standby), состояние GLBP active (GLBP active), состояние GLBP standby (GLBP standby), ретранслятор GLBP (GLBP forwarder), активный виртуальный шлюз (Active Virtual Gateway — AVG)

Таблицы команд

Хоть и не обязательно заучивать информацию из таблиц данного раздела, ниже приведен список команд конфигурации и пользовательских команды главы. Фактически команды стоит запомнить, чтобы лучше понять содержимое главы и выполнить задачи по подготовке к экзамену. Чтобы проверить, насколько хорошо вы запомнили команды, закройте левую сторону таблицы листом бумаги, читайте описания с правой стороны и пытайтесь вспоминать команду.

Таблица 6.4. Конфигурационные команды главы 6

Команда	Описание
`standby` *`номер_группы`* `ip` *`виртуальный-ip`*	Подкоманда интерфейса, разрешающая протокол HSRP, определяющая виртуальный IP-адрес и ассоциирующая его с конкретной группой HSRP
`standby` *`номер_группы`* `priority` *`0...255`*	Подкоманда интерфейса, задающая приоритет, влияющий на то, какой маршрутизатор станет активным маршрутизатором HSRP. Побеждает более высокое значение, причем стандартным является значение 100. Команда ассоциирует параметр с конкретной группой HSRP
`standby` *`номер_группы`* `name` *`описательное_имя`*	Подкоманда интерфейса, определяющая имя и ассоциирующая его с конкретной группой HSRP
`standby version 1 | 2`	Подкоманда интерфейса, устанавливающая версию HSRP, используемую для всех групп на интерфейсе
`glbp` *`номер_группы`* `ip` *`виртуальный-ip`*	Подкоманда интерфейса, разрешающая протокол GLBP, определяющая виртуальный IP-адрес и ассоциирующая его с конкретной группой GLBP

Окончание табл. 6.4

Команда	Описание
`glbp` *`номер_группы`* `priority` *`0..255`*	Подкоманда интерфейса, задающая приоритет, влияющий на то, какой маршрутизатор станет активным маршрутизатором GLBP. Побеждает более высокое значение, причем стандартным является значение 100. Команда ассоциирует параметр с конкретной группой GLBP
`glbp` *`номер_группы`* `name` *`описательное_имя`*	Подкоманда интерфейса, определяющая имя и ассоциирующая его с конкретной группой GLBP

Таблица 6.5. Команды EXEC главы 6

Команда	Описание
`show standby`	Выводит подробности о состоянии HSRP, включая виртуальный IP-адрес, активные и резервные в настоящее время маршрутизаторы, виртуальные MAC-адресы и счетчики
`show standby brief`	Выводит по одной строке информации о состоянии для каждой группы HSRP, активные и резервные в настоящее время маршрутизаторы и виртуальные IP-адреса
`show glbp`	Выводит подробности о состоянии GLBP, включая виртуальный IP-адрес, текущий активный виртуальный шлюз (AVG), каждый ретранслятор (маршрутизатор), а также какие маршрутизаторы в настоящее время поддерживают каждый виртуальный MAC-адрес
`show glbp brief`	Выводит для каждой группы GLBP по одной строке информации о состоянии шлюз AVG и второй строке для каждого ретранслятора (маршрутизатора) в группе GLBP. Данные идентифицируют активный шлюз AVG, резервный шлюз AVG, виртуальные MAC-адреса, а также какие маршрутизаторы являются активными в настоящее время и прослушивающими каждый виртуальный MAC-адрес

Ответы на контрольные вопросы:

1 Г. 2 В. 3 А. 4 В. 5 Б. 6 В.

Глава 7

Виртуальные частные сети

Некоторая компания с одной главной и десятью дистанционными площадками может арендовать несколько разных типов служб WAN для соединения центральной площадки со всеми филиалами, включая выделенные линии, технологию Frame Relay и, что наиболее вероятно сегодня, мультипротокольную коммутацию по меткам (MPLS). Тем не менее для соединения дистанционных площадок есть и другая возможность — достаточно просто подключить каждую площадку к Интернету по такой высокоскоростной технологии доступа, как кабель или цифровой абонентский канал (DSL). Теперь площадки могут передавать друг другу пакеты IP по Интернету, используя его как сеть WAN.

К сожалению, соединение через Интернет не настолько безопасно, как через выделенные линии или сети на базе служб сети WAN. Например, если злоумышленник задумал перехватить копии пакетов данных, передающихся по выделенному каналу, то ему необходимо физически подключиться к кабелю, который зачастую находится внутри защищенного здания, под дорожным полотном или же в АТС телекоммуникационной компании. Попытка получения доступа к сети в таком случае повлечет за собой уголовную ответственность. Используя возможности Интернета, злоумышленник может найти более простые способы получения желанных копий пакетов данных. Для этого не нужно отходить от компьютера, а риск оказаться в тюрьме много меньше.

Виртуальные частные сети (Virtual Private Network — VPN) предоставляют оптимальное решение проблем безопасности, которые возникают при использовании открытого Интернета в качестве частной службы сети WAN. В этой главе рассматриваются основные концепции и терминология сетей VPN.

Эта глава имеет два главных раздела. В первом разделе речь пойдет о фундаментальной концепции сетей VPN и некоторых подробностях двух их основных типов: *защищенного протокола IP* (IP Security — IPsec) и *уровня защищенных сокетов* (Secure Sockets Layer — SSL). Второй раздел посвящен одному из краеугольных камней сетей VPN — концепции туннеля между двумя маршрутизаторами, создаваемого сетью IP.

В этой главе рассматриваются следующие экзаменационные темы
Технологии WAN
Различные технологии WAN
VPN

Основные темы

Основы сетей VPN

Выделенным линиям присущи некоторые очень полезные особенности, связанные с безопасностью. Например, маршрутизатору на одном конце достоверно известен идентификатор маршрутизатора на другом конце линии. У принимающего поток данных маршрутизатора нет оснований полагать, что злоумышленник перехватил информацию или же изменил ее при передаче, чтобы причинить вред владельцам или другим лицам.

Сети VPN должны обеспечивать такой же уровень безопасности передачи данных, как и выделенная линия, будучи открытыми для других сторон. Фактически данные нередко передаются по Интернету. При передаче данных по таким открытым сетям, как Интернет, сеть VPN обеспечивает следующее.

Средства безопасности сетей VPN

Ключевая тема

- **Конфиденциальность** (Privacy). Третье лицо не сможет скопировать данные или ознакомиться с информацией, которая передается по Интернету.
- **Аутентификация** (Authentication). Проверка того, действительно ли отправитель пакетов VPN — истинное устройство, а не такое, которое используется злоумышленником.
- **Целостность данных** (Data integrity). Проверка того, не подвергался ли изменениям пакет при передаче через Интернет.
- **Защита от повторного использования** (Anti-replay). Третье лицо не сможет копировать пакеты данных, отосланные истинным отправителем, а затем пересылать эти пакеты, выдавая себя за истинного отправителя.

Таким образом, для решения перечисленных выше задач двумя устройствами создается виртуальная частная сеть, которую иногда называют *туннелем VPN* (VPN tunnel). Такие устройства добавляют еще один заголовок к оригинальному пакету. В этот заголовок включаются поля, наличие которых позволяет устройствам VPN выполнять перечисленные выше функции. Устройства также отвечают за шифрование оригинальных пакетов IP. Таким образом, подразумевается, что никто не дешифровал содержимое пакетов, даже если удалось скопировать пакеты при передаче через Интернет.

На рис. 7.1 представлена схема работы туннеля VPN. На рисунке показана сеть VPN, которая построена между филиалом и *адаптивным устройством безопасности* компании Cisco (Adaptive Security Appliance — ASA). В этом случае виртуальная частная сеть VPN называется корпоративной, поскольку объединяет два отдельных хоста компании. Такую сеть еще называют сетью интранет, поскольку она соединяет хосты одной и той же организации.

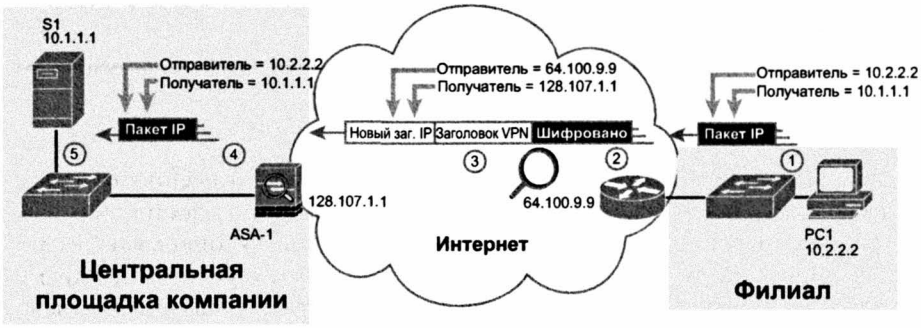


Рис. 7.1. Концепция туннеля VPN между площадками в Интранете

Ниже приведена показанная на рисунке последовательность передачи и получения пакетов данных.

1. Хост PC1 (10.2.2.2), показанный справа, пересылает пакет веб-серверу (10.1.1.1) так, как если бы сети VPN не было.
2. Маршрутизатор шифрует пакет, добавляет заголовки VPN и еще один заголовок IP (с открытым IP-адресом) и перенаправляет пакет.
3. Третье лицо перехватывает пакет, но не может изменить его, не будучи обнаруженным, а также не может прочитать содержимое пакета.
4. Устройство ASA-1 получает пакет, подтверждает аутентичность отправителя и тот факт, что пакет не был изменен, а затем расшифровывает оригинальный пакет данных.
5. Сервер S1 получает расшифрованный пакет.

Термин *туннель* относится ко всем пакетам протокола, которые передаются в других пакетах. Под термином туннель *VPN* подразумевается, что инкапсулированный пакет был зашифрован, тогда как термин *туннель* не означает, что пакет был зашифрован.

При построении сети VPN можно использовать множество устройств; область применения таких сетей также широка. На рис. 7.2 приведена схема трех разновидностей сетей VPN.



Рис. 7.2. Внутрикорпоративные сети VPN (Intranet VPN), межкорпоративные сети VPN (Extranet VPN) и сети VPN с дистанционным доступом (Access VPN)

В верхней части рисунка изображены центральная площадка и удаленный региональный офис вымышленной компании (Fredsco), которые соединены с внутрикорпоративной сетью VPN (Intranet VPN). В середине рисунка сеть компании Fredsco соединена с сетью компании-поставщика. Такая сеть уже называется межкорпоративной (Extranet VPN). А когда собственник (или сотрудник) компании Fredsco приносит свой ноутбук домой и в конце рабочего дня подключает его к Интернету, безопасное соединение между компьютером и корпоративной сетью Fredsco называется сетью VPN дистанционного доступа (Access VPN). В этом случае ноутбук является конечным устройством туннеля VPN, но не маршрутизатором, обеспечивающим доступ к Интернету. В табл. 7.1 приведены три вида виртуальных частных сетей.

Таблица 7.1. Три типа сетей VPN и их использование

Ключевая тема

Тип сети VPN	Назначение
Внутрикорпоративные сети (intranet)	Соединяют все компьютеры двух площадок сети одной организации; используется одно устройство VPN в каждой из площадок
Межкорпоративные сети (extranet)	Соединяют все компьютеры двух площадок сетей разных организаций, поддерживающих партнерские отношения; используется одно устройство VPN в каждой из площадок
Сети дистанционного доступа (remote access)	Соединяют отдельных пользователей с корпоративной сетью

Чтобы построить сеть VPN, на одном из компонентов каждой площадки необходимо установить соответствующее программное обеспечение и/или приобрести аппаратные средства, поддерживающие стандарты и протоколы защиты частных сетей. Ниже перечислены такие компоненты и устройства.

Маршрутизаторы. Кроме пересылки пакетов, маршрутизатор может обеспечивать функции сетей VPN. В маршрутизатор интегрированы специальные платы расширения, с помощью которых процесс шифрования происходит быстрее.

Адаптивные устройства безопасности (Adaptive Security Appliances — ASA). Это основные устройства компании Cisco, которые обеспечивают безопасность компьютерных систем. Их можно настроить на выполнение множества функций по защите информационных ресурсов, в том числе использовать для построения сетей VPN.

Клиент VPN. Если компьютер — часть сети VPN с дистанционным доступом, то он должен выполнять соответствующие функции. Для выполнения дополнительных функций необходимо установить специальное программное обеспечение, которое называется клиентом VPN.

И наконец, по сравнению с другими технологиями WAN, у сетей VPN есть несколько преимуществ. Рассмотрим, например, компанию с 1000 небольших отделений. Компания может создать частную сеть WAN, используя выделенные линии либо технологии Frame Relay, Ethernet WAN, MPLS и т.д. Но вместо этого каждое отделение могло бы просто подключиться к Интернету и использовать технологию VPN, экономя деньги по сравнению с другим возможностями. Вот некоторые из преимуществ.

Стоимость. Решение на базе VPN обычно дешевле альтернативных возможностей.

Защита. Решение на базе VPN может быть столь же безопасным, как и частные соединения WAN.

Масштабируемость. Решение на базе VPN распространяется на многие площадки за разумную стоимость. Каждая площадка подключается через любое соединение Интернета, а большинство деловых центров имеет по несколько конкурирующих компаний, обеспечивающих доступ к Интернету.

Далее рассматривается использование для создания сетей VPN набора протоколов под общим названием *IPsec*, а также приведено краткое описание VPN SSL.

Сети VPN на базе технологии IPSec

IPSec — это архитектура или набор концепций, используемых для защиты сетей IP. Это название — не аббревиатура, а сокращенная версия наименования в серии документов RFC (RFC 4301; архитектура безопасности протокола Интернета — Security Architecture for the Internet Protocol), для которой употребляется название IPSecurity, или сокращенный вариант — IPSec.

Протокол IPsec определяет, как два подключенных к Интернету устройства способны достичь основных целей сетей VPN, описанных в начале этой главы: конфиденциальность, аутентификация, целостность данных и защита от повторного использования. Он не определяет способ реализации сети VPN, позволяя использовать для каждой конкретной сети VPN несколько разных средств. Одно из преимуществ архитектуры IPSec — возможность изменения и добавления технологий, когда разрабатываются новые и усовершенствованные протоколы систем защиты.

В этой главе не рассматриваются подробности каждого элемента IPsec, в ней дано лишь общее представление об их работе. В данном разделе будет показано, как две конечных точки IPsec шифруют данные и добавляют заголовки IPsec VPN к зашифрованным данным.

Концепция шифрования IPsec может показаться запутанной, но если игнорировать математику (а это, к счастью, можно), то понять шифрование IPsec не слишком трудно. Для шифрования протокол IPsec использует пару алгоритмов шифрования, являющихся по существу математическими формулами, удовлетворяющими нескольким требованиям. Прежде всего, формулы нужно выбирать так, чтобы:

- одна использовалась для шифрования данных;
- другая — для расшифровки данных.

Но есть еще и не такие очевидные моменты. Допустим, злоумышленник перехватил зашифрованный текст, но не владеет секретным паролем, который называется *ключом шифрования* (encryption key). Поэтому формулы следует выбирать так, чтобы постороннее лицо не смогло дешифровать пакет данных или текст. Также есть еще одно важное требование: даже если злоумышленнику удалось дешифровать пакет, это никак не должно способствовать дешифрованию последующих пакетов данных.

Шифрование данных в сетях VPN на базе технологии IPSec происходит так, как показано на рис. 7.3.

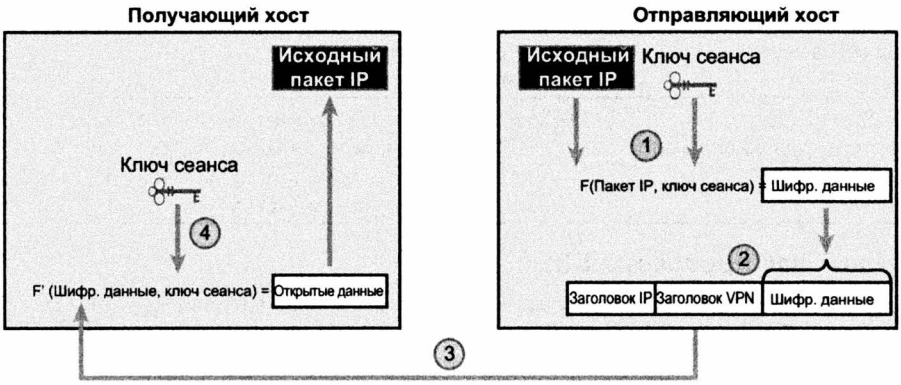


Рис. 7.3. Основные этапы процесса шифрования IPsec

Опишем каждый из четырех этапов шифрования.

1. Устройство-отправитель в сети VPN (аналогично дистанционному маршрутизатору на рис. 7.1) подставляет исходные данные и ключ шифрования в формулу, по которой производится шифрование.
2. Устройство-отправитель инкапсулирует зашифрованные данные в пакет с новым заголовком IP и заголовком VPN.
3. Устройство-отправитель пересылает этот пакет устройству-получателю сети VPN (аналогично устройству ASA-1 на рис. 7.1).
4. Устройство-получатель в сети VPN расшифровывает пакет, используя соответствующую формулу. В нее подставляются зашифрованные данные и ключ шифрования, значение которого совпадает с тем, которое использовалось в устройстве-отправителе сети VPN.

Протокол IPsec обладает высокой гибкостью, он изменялся на протяжении длительного времени, чтобы поддерживать все более новые и лучшие стандарты шифрования. Например, у новых стандартов есть новые алгоритмы, и зачастую они используют более длинные ключи. Эти изменения затрудняют злоумышленникам расшифровку скопированных данных, передаваемых по Интернету. Некоторые из этих возможностей и длины ключей приведены в табл. 7.2.

Таблица 7.2. Алгоритмы шифрования в сетях VPN

Алгоритм шифрования	Разрядность ключа, биты	Комментарий
Стандарт шифрования данных (Data Encryption Standard — DES)	56	Устаревший и не такой надежный, как другие алгоритмы, описанные ниже
3-DES (Triple DES)	56x3	Последовательно применяются три разных ключа DES длиной 56 бит. Таким образом, улучшается надежность по сравнению с алгоритмом DES

Окончание табл. 7.2

Алгоритм шифрования	Разрядность ключа, биты	Комментарий
Улучшенный стандарт шифрования (Advanced Encryption Standard — AES)	128–256	Наиболее эффективный на сегодняшний день. Обеспечивает высокую стойкость шифрования, потребляет меньше ресурсов, чем 3-DES

Сети VPN на базе протокола SSL

Протокол защищенных сокетов (Secure Socket Layer — SSL) является альтернативной технологией IPsec для VPN. В частности, современные веб-браузеры поддерживают протокол SSL как средство динамического создания защищенного соединения между веб-браузером и веб-сервером для осуществления, например, финансовых транзакций.

В этом небольшом разделе рассматриваются некоторые подробности использования протокола SSL для создания удаленного доступа к сети VPN.

Для подключения к веб-серверам веб-браузеры используют протокол HTTP. Но когда требуется защищенное соединение с веб-сервером, браузеры переходят на протокол SSL. Протокол SSL использует зарезервированный порт 443, шифрование передаваемых между браузером и сервером данных, а также аутентификацию пользователя. Далее сообщения HTTP передаются по соединению SSL VPN.

Встроенные в веб-браузер функции SSL создают один безопасный сеанс, но это — та же технология SSL, применяемая для создания удаленного доступа VPN, используемого клиентом VPN Cisco. AnyConnect, клиент VPN Cisco, является программным обеспечением, которое находится на компьютере пользователя и использует протокол SSL для создания одного конца туннеля удаленного доступа VPN. В результате шифруются все пакеты, посланные на другой конец туннеля, а не только посланные по одному соединению HTTP веб-браузера.

И наконец, обратите внимание, что на стороне сервера (и другом конце соединения SSL) могут находиться устройства многих типов. Конечной точкой соединения SSL веб-браузера может быть веб-сервер, но чтобы улучшить производительность сервера, туннель SSL на стороне сервера зачастую завершается таким специализированным устройством, как Cisco ASA.

На рис. 7.4 объединены все концепции SSL на примере с двумя туннелями SSL. Один туннель SSL VPN соединяет веб-браузер на хосте A с устройством ASA справа, обеспечивая один сеанс связи. Хост B использует клиент VPN Cisco, поэтому все пакеты от хоста B к площадке справа будут передаваться по защищенному соединению SSL.

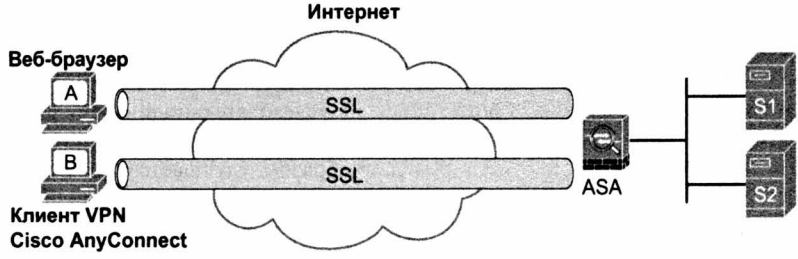


Рис. 7.4. Туннели SSL VPN

Теперь, изучив несколько возможностей сетей VPN, рассмотрим создание туннеля VPN и его настройку на маршрутизаторе.

Туннели GRE

Устройство на конечной точке VPN получает нормальный незашифрованный пакет и, прежде чем перенаправить его, выполняет несколько действий, а именно: шифрование пакета, его инкапсуляцию и снабжение новым заголовком IP. В новом заголовке IP используются адреса, позволяющие маршрутизаторам перенаправлять пакеты IP в незащищенной сети между двумя конечными точками туннеля VPN. Первоначальный пакет IP, включая исходный заголовок IP, зашифрован и нечитабелен.

Во втором разделе этой главы используется несколько иной подход к настройке туннеля VPN; рассматривается только туннельная часть, а функции шифрования игнорируются. В частности, рассматриваются концепции создания маршрутизаторами туннеля за счет инкапсуляции первоначального пакета IP в другом пакете IP. Цель заключается в том, чтобы дать лишь общее представление о работе туннеля, поскольку подробности настройки защиты относятся к другой сертификации, CCNA Security.

Концепции туннеля GRE

В данной главе рассматривается один тип туннеля IP: *обобщенная маршрутная инкапсуляция* (Generic Routing Encapsulation — GRE). Инкапсуляция GRE определена в документе RFC 2784, который определяет дополнительный заголовок, наряду с новым заголовком IP, используемым при инкапсуляции первоначального пакета. Создав туннель IP GRE, два маршрутизатора взаимодействуют в соответствии с параметрами конфигурации. Далее, для шифрования трафика, может быть добавлена конфигурация IPsec.

При обсуждении туннелей GRE эти концепции рассматриваются с нескольких точек зрения. Сначала рассматривается перенаправление пакетов по туннелю GRE как по последовательному каналу в защищенной корпоративной сети, а затем работа туннеля GRE.

Маршрутизация по туннелям GRE

С точки зрения передаваемого пакета туннель GRE между двумя маршрутизаторами очень похож на последовательный канал. Поэтому, прежде чем обсуждать туннели GRE, рассмотрим сначала уже знакомые факты о маршрутизаторах и последовательных каналах, используя как пример рис. 7.5.

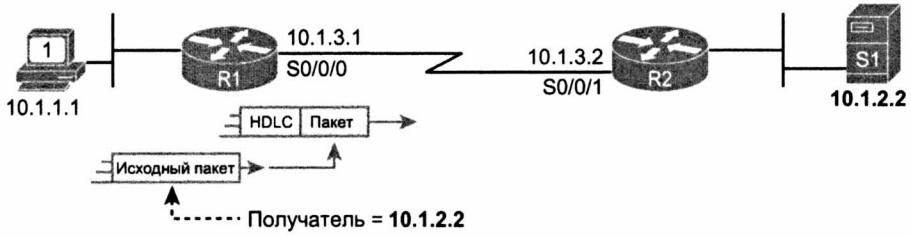


Рис. 7.5. Маршрутизация пакета IP по последовательному каналу

Небольшая сеть на рис. 7.5 выглядит как часть многих корпоративных сетей. Она использует частные IP-адреса (сеть 10.0.0.0). На каждом интерфейсе маршрутизатора есть IP-адрес, включая каждый последовательный интерфейс. IP-адреса на последовательных интерфейсах (10.1.3.1 и 10.1.3.2) находятся в той же подсети. Когда компьютер PC1 посылает пакет на IP-адрес получателя 10.1.2.2, маршрутизатор R1 инкапсулирует исходный пакет в пакет используемого на канале связи протокола канала связи, например стандартного *высокоуровневого протокола управления каналом* (HDLC), представленного на рисунке.

Кроме того, обратите внимание на то, что все части сети этого малого предприятия расположены в защищенных пространствах. У этой сети нет никакой необходимости в шифровании данных, используемых VPN.

Инкапсуляция GRE обеспечивает концепцию, подобную последовательному каналу на рис. 7.5, по крайней мере, с точки зрения маршрутизации IP. Вместо последовательного канала связи с последовательными интерфейсами маршрутизаторы используют виртуальные *туннельные интерфейсы* (tunnel interface). Два маршрутизатора имеют на туннельных интерфейсах IP-адреса в той же подсети. В примере на рис. 7.6 последовательный канал заменен виртуальными туннельными интерфейсами.

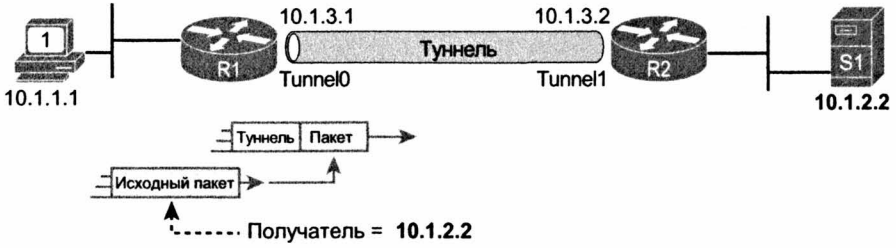


Рис. 7.6. Замена последовательного канала туннелем IP

Ограничившись общими идеями маршрутизации IP, туннель можно считать пока другим каналом связи в безопасной части сети. Туннельные IP-адреса относятся к безопасной части корпоративной сети. Маршрутизаторы инкапсулируют первоначальный пакет в пакете с туннельным заголовком, занимающим место заголовка HDLC последовательного канала. У маршрутизаторов даже будет список маршрутов, где туннельные интерфейсы (в данном случае Tunnel0 и Tunnel1) указаны как исходящие интерфейсы.

Использующие туннель GRE маршрутизаторы рассматривают их просто как другой канал связи с двухточечной топологией. У маршрутизаторов есть IPv4-адреса в той же подсети. Используя протокол маршрутизации, маршрутизаторы становятся соседями и обмениваются маршрутами по туннелю. В полученных по туннелю маршрутах туннельные интерфейсы указаны как исходящие интерфейсы с IP-адресом туннельного интерфейса соседнего маршрутизатора как следующего транзитного маршрутизатора. Пример на рис. 7.7 демонстрирует маршруты, изученные каждым маршрутизатором.

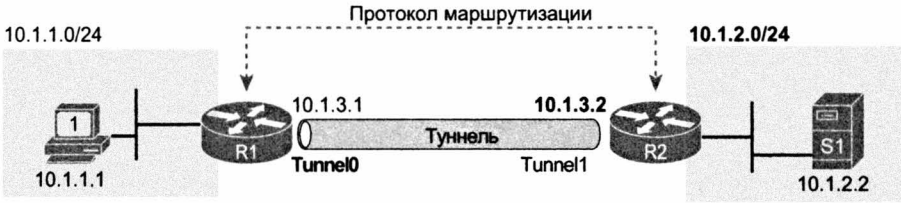


Таблица маршрутизации R1

Подсеть	Интерфейс	След. точка
10.1.2.0/24	**Tunnel0**	**10.1.3.2**

Таблица маршрутизации R2

Подсеть	Интерфейс	След. точка
10.1.1.0/24	Tunnel1	10.1.3.1

Рис. 7.7. Туннельные маршрутизаторы получают маршруты по туннелю IP

Уделим минуту подробному рассмотрению маршрута для подсети 10.1.2.0/24 справа. У маршрутизатора R2 будет подключенный маршрут к этой подсети. Для обмена информацией о маршрутизации маршрутизаторы R1 и R2 используют некий протокол маршрутизации (например, OSPF). Маршрутизатор R1 добавит новый маршрут для подсети 10.1.2.0/24, и в этом маршруте как исходящий интерфейс будет указан собственный туннельный интерфейс (Tunnel0) маршрутизатора R1. В этом маршруте как IP-адрес маршрутизатора следующего транзитного узла указан адрес туннельного интерфейса маршрутизатора R2 (10.1.3.2), о чем свидетельствует запись в таблице маршрутизации IP маршрутизатора R1 в левой нижней части рисунка.

Все эти концепции свидетельствуют о том, что туннель GRE действует как всего лишь еще один канал связи в безопасной части объединенной сети. Далее рассмотрим, как туннели GRE перенаправляют пакеты по незащищенной сети между этими двумя маршрутизаторами.

Туннели GRE в незащищенной сети

На нескольких последних рисунках туннель между двумя маршрутизаторами выглядит просто как труба, что ничего не говорит о физической сети, формирующей туннель. Туннель может быть проложен по любой сети IP. Туннель используется в сети IP для перенаправления первоначальных пакетов, поэтому любая сеть IP между маршрутизаторами R1 и R2 позволила бы создать туннель.

Сети VPN между площадками, как показано на рис. 7.6, в качестве сети IP зачастую используют незащищенную сеть, такую как Интернет. Все дело в деньгах. Ежемесячная плата за высокоскоростной доступ к Интернету для каждой площадки зачастую намного меньше, чем за другие службы WAN. Но независимо от существующего способа подключения к Интернету, маршрутизаторы туннеля вполне могут использовать его для перенаправления пакетов между собой (рис. 7.8).

Маршрутизаторы на концах туннеля GRE создают туннель, согласившись передавать друг другу пакеты по незащищенной сети. На рис. 7.8 представлено большинство подробностей, которые инженер должен знать об этих маршрутизаторах, прежде чем приступать к настройке туннеля GRE на обоих концах. На рисунке представлены интерфейсы маршрутизаторов R1 и R2, используемые для подключения к Интернету, а также их IP-адреса, в данном случае 1.1.1.1 и 2.2.2.2, используемые маршрутизаторами при подключении к Интернету.

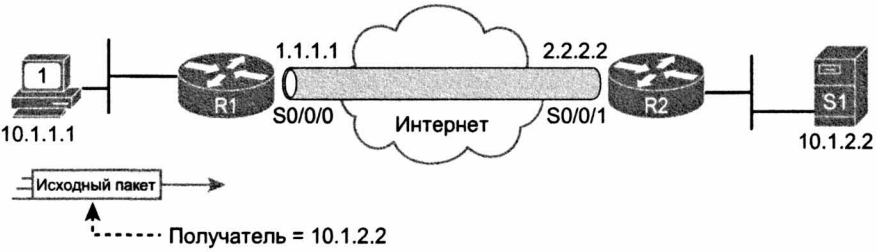


Рис. 7.8. Передача по туннелю через Интернет

В конфигурации маршрутизатора используются виртуальные *туннельные интерфейсы* (tunnel interface). Эти интерфейсы не существуют, пока инженер не создаст туннель командой `interface tunnel`. Например, команда `interface tunnel 0` создает туннельный интерфейс номер 0. Чтобы создать туннель, оба маршрутизатора создают туннельные интерфейсы и используют IP-адреса, как будто туннель является двухточечным каналом связи.

На рис. 7.9 представлена концептуальная схема передачи пакета, поступившего с компьютера PC1 на маршрутизатор R1 для передачи по туннелю GRE на сервер S1 (10.1.2.2). Когда маршрутизатор R1 использует логику перенаправления IP в защищенной части сети (см. рис. 7.6), он должен переслать пакет по туннелю. Инкапсуляция, осуществляемая маршрутизатором R1, представлена на рис. 7.9.

Ключевая тема

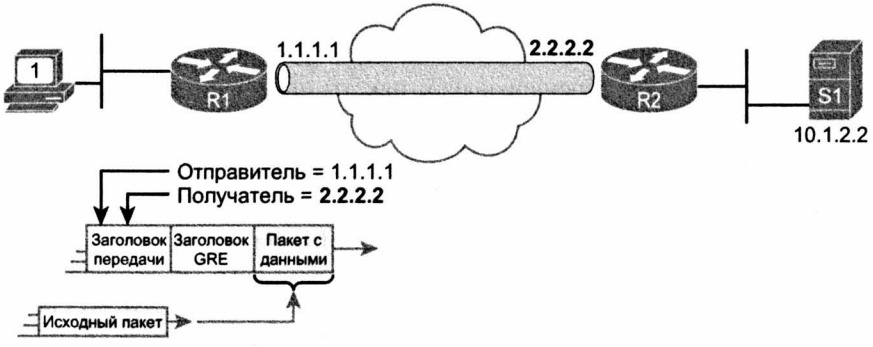


Рис. 7.9. Инкапсуляция первоначального пакета IP в пакет формата GRE

ВНИМАНИЕ!

Если бы на формирующих туннель маршрутизаторах (см. рис. 7.8) было настроено шифрование IPsec, то отправляющий маршрутизатор перед инкапсуляцией сначала зашифровал бы первоначальный пакет.

При создании туннеля инкапсуляция GRE определяет применение двух заголовков. Инкапсуляция GRE определяет собственный заголовок для управления самим туннелем, а также полный 20-байтовый заголовок IP — *заголовок передачи* (delivery header). Этот заголовок использует IP-адреса из небезопасной сети. В данном случае заголовок передачи IP будет содержать IP-адрес маршрутизатора R1 из Интернета (1.1.1.1) в качестве отправителя, а в качестве получателя — IP-адрес маршрутизатора R2 (2.2.2.2) из Интернета.

Когда пакет следует через Интернет, маршрутизаторы в Интернете используют для перенаправления внешний заголовок передачи IP GRE. Тот факт, что этот пакет содержит совершенно другой пакет IP, не имеет никакого значения для процесса перенаправления на этих маршрутизаторах; они просто перенаправляют пакет IP на основании IP-адреса получателя (2.2.2.2). Концепция представлена на рис. 7.10; обратите внимание, что этот пакет может быть перенаправлен многими маршрутизаторами в Интернете, прежде чем он достигнет маршрутизатора R2.

Когда пакет GRE наконец поступает на маршрутизатор R2 (рис. 7.10), он должен извлечь первоначальный пакет IP. Если бы речь шла о физическом канале связи, маршрутизатор R2 просто удалил бы заголовок канала связи. При инкапсуляции GRE маршрутизатор (R2) должен удалить из полученного пакета и заголовок передачи, и заголовок GRE, оставив только первоначальный пакет, как показано на рис. 7.11.

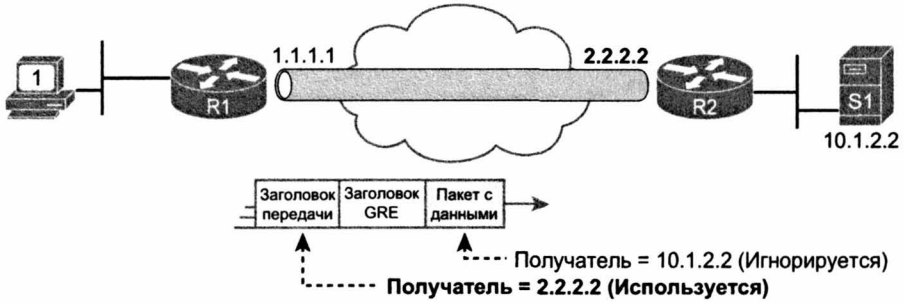


Рис. 7.10. Маршрутизаторы Интернета перенаправляют пакет IP GRE на основании открытых IP-адресов

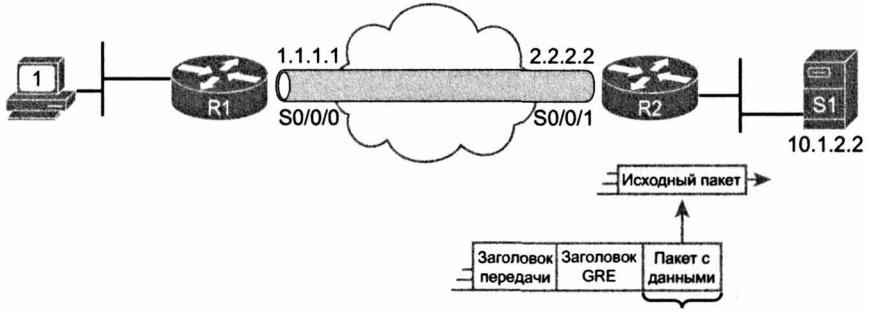


Рис. 7.11 Маршрутизаторы Интернета перенаправляют пакет IP GRE на основании открытых IP-адресов

ВНИМАНИЕ!

Если на формирующих туннель маршрутизаторах (см. рис. 7.11) было настроено шифрование IPsec, то получающий маршрутизатор расшифрует полученный пакет.

Настройка туннелей GRE

Для настройки туннеля GRE достаточно лишь нескольких команд, сложность — в организации параметров конфигурации. Для этого необходимы туннельные интерфейсы с IP-адресами из защищенной части сети, заданные командой интерфейса `ip address`. Необходимо также, чтобы маршрутизаторы объявили и собственный IP-адрес (отправителя), и IP-адрес другого маршрутизатора (получателя), используемые в незащищенной части сети. Организация различных параметров конфигурации представлена на рис. 7.12.

Ключевая тема

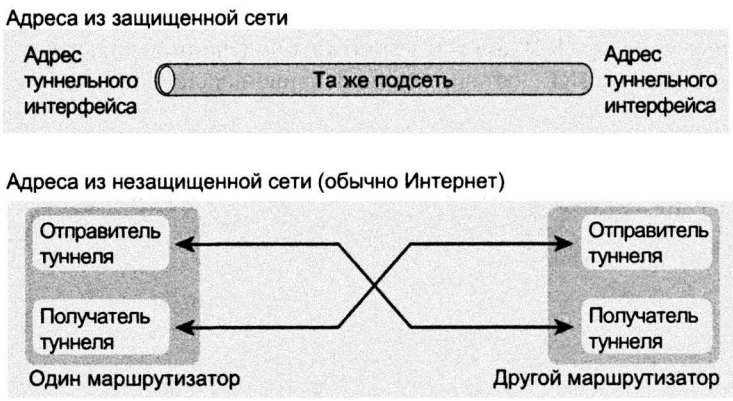


Рис. 7.12. Конфигурация туннеля GRE: отношения между параметрами

Ниже описаны этапы настройки каждого маршрутизатора.

Ключевая тема

Этапы настройки туннеля GRE

Этап 1 Создайте туннельный интерфейс командой `interface tunnel` *`номер_интерфейса`*. Номера интерфейсов имеют только локальное значение и не обязаны совпадать на обоих маршрутизаторах

Этап 2 Присвойте IP-адрес туннельному интерфейсу командой `ip address` *`адрес маска`*, используя подсеть из диапазона адресов защищенной сети. Оба маршрутизатора туннеля должны использовать адреса из той же подсети.

Этап 3 Задайте IP-адрес отправителя туннеля в открытой части сети подкомандой интерфейса `tunnel source` *`номер_интерфейса`* или `tunnel source` *`IP-адрес`*. При обращении к интерфейсу локальный маршрутизатор использует IP-адрес, заданный на указанном интерфейсе. (Это значение должно соответствовать IP-адресу получателя туннеля на другом маршрутизаторе.)

Этап 4 Задайте IP-адрес получателя туннеля в открытой части сети командой `tunnel destination` *`IP-адрес`*. (Это значение должно соответствовать IP-адресу, используемому другим маршрутизатором в качестве IP-адреса отправителя туннеля.)

Этап 5 Настройте на маршрутизаторах использование туннеля с маршрутами IP, разрешив применение протокола динамической маршрутизации или задав маршруты IP статически

Как обычно, разобраться поможет пример, использующий сеть, рассматриваемую на нескольких последних страницах. Маршрутизаторы R1 и R2 формируют

туннель, используя открытые адреса 1.1.1.1 и 2.2.2.2 соответственно. Туннель использует подсеть 10.1.3.0/24, а маршрутизаторы R1 и R2 используют IP-адреса 10.1.3.1 и 10.1.3.2 соответственно. Пример 7.1 демонстрирует конфигурацию на маршрутизаторе R1, а пример 7.2 — на маршрутизаторе R2.

Пример 7.1. Конфигурация туннеля на маршрутизаторе R1

```
R1# show running-config
! Строки опущены для краткости

interface serial 0/0/0
  ip address 1.1.1.1 255.255.255.0
!
interface Tunnel0
  ip address 10.1.3.1 255.255.255.0
tunnel source Serial0/0/0
tunnel destination 2.2.2.2
!
! Конфигурация OSPF разрешает применение протокола OSPF и на туннельном
! интерфейсе.
router ospf 1
  network 10.0.0.0 0.255.255.255 area 0
```

Пример 7.2. Конфигурация туннеля на маршрутизаторе R2

```
R2# show running-config
! Строки опущены для краткости

interface serial 0/0/1
  ip address 2.2.2.2 255.255.255.0
!
interface Tunnel1
  ip address 10.1.3.2 255.255.255.0
tunnel source Serial0/0/1
tunnel destination 1.1.1.1
!
! Конфигурация OSPF разрешает применение протокола OSPF и на туннельном
! интерфейсе.
router ospf 1
  network 10.0.0.0 0.255.255.255 area 0
```

Только чтобы удостовериться в понимании логики, рассмотрим конфигурацию маршрутизатора R2. На интерфейсе S0/0/1 маршрутизатора R2 был задан IP-адрес 2.2.2.2. Далее, на туннельном интерфейсе 1, команда `tunnel source Serial0/0/1` ссылается на тот же интерфейс, делая IP-адресом отправителя туннеля адрес 2.2.2.2 маршрутизатора R2. И наконец, вернемся к конфигурации маршрутизатора R1. Ее команда `tunnel destination 2.2.2.2` явно ссылается на тот же IP-адрес, используемый маршрутизатором R2 как адрес отправителя. То же относится к IP-адресу отправителя 1.1.1.1 маршрутизатора R1 и адресу получателя 1.1.1.1 маршрутизатора R2.

Проверка туннеля GRE

Окончательная проверка туннеля подразумевает передачу трафика конечного пользователя. Однако команда `show` на маршрутизаторе способна сказать достаточно

много о его состоянии, прежде чем пытаться вводить команды `ping` или `traceroute` на устройстве пользователя.

Прежде всего, поскольку туннель действует как последовательный канал между интерфейсами на обоих маршрутизаторах, обычные команды, выводящие состояние интерфейса, IP-адреса и маршруты IP, вполне способны представить информацию о туннеле GRE. Пример 7.3 демонстрирует уже знакомую команду `show ip interface brief` на маршрутизаторе R1. В выводе выделен интерфейс `tunnel0` маршрутизатора R1.

Пример 7.3. Отображение состояния интерфейсов и IP-адресов, включая туннельный интерфейс

```
R1# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     10.1.1.9        YES manual up                    up
GigabitEthernet0/1     unassigned      YES manual administratively down down
Serial0/0/0            1.1.1.1         YES manual up                    up
Serial0/0/1            unassigned      YES manual administratively down down
Tunnel0                10.1.3.1        YES manual up                    up
```

Команда `show interfaces tunnel` *номер_интерфейса* выводит много счетчиков, а также параметры конфигурации и состояние интерфейса. В примере 7.4 снова используется интерфейс Tunnel0 маршрутизатора R1. Обратите внимание, что выведена конфигурация локального маршрутизатора (R1) с IP-адресами отправителя (1.1.1.1) и получателя (2.2.2.2), что подтверждает использование инкапсуляции GRE, как выделено в примере.

Пример 7.4. Подробности туннельных интерфейсов

```
R1# show interfaces tunnel0
Tunnel0 is up, line protocol is up
  Hardware is Tunnel
  Internet address is 10.1.3.1/24
  MTU 17916 bytes, BW 100 Kbit/sec, DLY 50000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 1.1.1.1 (Serial0/0/0), destination 2.2.2.2
  Tunnel Subblocks:
     src-track:
     Tunnel0 source tracking subblock associated with Serial0/0/0
     Set of tunnels with source Serial0/0/0, 1 member (includes itera-
tors), on interface <OK>
  Tunnel protocol/transport GRE/IP
! Строки опущены для краткости
```

Хотя работоспособность туннельного интерфейса важна, маршрутизаторы не будут использовать его как туннельный, если маршруты не попытаются перенаправлять по нему пакеты. Конфигурация в этом примере демонстрирует, что протокол OSPF был разрешен на всех интерфейсах сети класса A 10.0.0.0 — безопасной части объединенной сети. Поэтому маршрутизаторы должны обменяться маршрутами OSPF и изучить те же маршруты, что были представлены на рис. 7.7. Доказательство

демонстрирует пример 7.5, где маршрутизатор R1 вывел изученный по протоколу OSPF маршрут к подсети LAN 10.1.2.0/24 маршрутизатора R2.

Пример 7.5. Маршруты маршрутизатора R1 в сети 10.0.0.0

```
R1# show ip route 10.0.0.0
Routing entry for 10.0.0.0/8, 5 known subnets
  Attached (4 connections)
  Variably subnetted with 2 masks
C       10.1.1.0/24 is directly connected, GigabitEthernet0/0
L       10.1.1.9/32 is directly connected, GigabitEthernet0/0
O       10.1.2.0/24 [110/1001] via 10.1.3.2, 00:07:55, Tunnel0
C       10.1.3.0/24 is directly connected, Tunnel0
L       10.1.3.1/32 is directly connected, Tunnel0
! Строки опущены для краткости
```

Внимание! Команда `show ip route 10.0.0.0` выводит известные маршруты в сети 10.0.0.0.

И наконец, для доказательства способности туннеля перенаправлять трафик пользователь может создать некий собственный трафик или воспользоваться расширенной командой `ping` или `traceroute`. Пример 7.6 демонстрирует расширенную команду `traceroute` с IP-адреса 10.1.1.9 сети LAN маршрутизатора R1 на IP-адрес 10.1.2.2 сервера 1.

Пример 7.6. Расширенная команда `traceroute` демонстрирует работоспособность туннеля

```
R1# traceroute
Protocol [ip]:
Target IP address: 10.1.2.2
Source address: 10.1.1.9
Numeric display [n]:
Timeout in seconds [3]:
Probe count [3]:
Minimum Time to Live [1]:
Maximum Time to Live [30]:
Port Number [33434]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Type escape sequence to abort.
Tracing the route to 10.1.2.2
VRF info: (vrf in name/id, vrf out name/id)
  1 10.1.3.2 0 msec 4 msec 0 msec
  2 10.1.2.2 4 msec 4 msec 0 msec
R1#
```

В примере 7.6 показано, что команда `traceroute` завершилась успешно и вывела туннельный IP-адрес (10.1.3.2) маршрутизатора R2 как адрес первого маршрутизатора в маршруте. Обратите внимание: команда `traceroute` не вывела маршрутизаторы в незащищенной части сети, поскольку созданные ею пакеты передаются между маршрутизаторами R1 и R2 в инкапсулированном виде.

Обзор

Резюме

- Сети VPN обеспечивают защиту, используя конфиденциальность, аутентификацию, проверку целостности данных и предотвращение повторного использования пакетов.
- Сети VPN шифруют данные, чтобы предотвратить их прочтение злоумышленником в случае перехвата. Это конфиденциальность.
- Сети VPN проверяют отправителя данных. Это аутентификация.
- Сети VPN гарантируют, что пакет данных не будет изменен при передаче. Это проверка целостности данных.
- Сети VPN не позволяют злоумышленнику записать данные и воспроизвести их позже, выдавая себя за допустимого пользователя. Это защита от повторного использования.
- Сеть интранет между площадками VPN, объединяющая все компьютеры двух площадок одной организации, обычно использует по одному устройству VPN на каждой площадке.
- Сеть интранет между площадками VPN, объединяющая все компьютеры двух разных площадок, но партнерских организаций, обычно использует по одному устройству VPN на каждой площадке.
- Удаленный доступ позволяет подключить к корпоративной сети индивидуальных пользователей Интернета.
- Сети VPN имеют преимущества по стоимости, защите и масштабируемости.
- Семейство протоколов IPsec определяет не один, а несколько способов реализации сетей VPN, предоставляя несколько разных протоколов для каждой конкретной сети VPN.
- Протокол SSL является альтернативной технологией VPN семейства протоколов IPsec.
- Технология SSL позволяет создать удаленный доступ VPN, используя клиент VPN компании Cisco.
- Инкапсуляция GRE определяет дополнительный заголовок, который наряду с новым заголовком IP применяется для инкапсуляции первоначального пакета.
- Взаимодействуя друг с другом, при соответствии параметров конфигурации, два маршрутизатора создают туннель GRE.

Контрольные вопросы

Ответьте на эти вопросы. Ответы можно найти на последней странице главы. Полное объяснение ответов приведено в приложении В на веб-сайте.

1. Какой из следующих терминов означает виртуальную частную сеть VPN, в которой соединение площадок одной компании осуществляется через Интернет, но не через выделенный канал или протокол Frame Relay?

   А) Внутрикорпоративная сеть VPN.

   Б) Межкорпоративная сеть VPN.

   В) Сеть VPN дистанционного доступа.

   Г) Корпоративная сеть VPN.

2. Что из перечисленного ниже не является функциями защиты, осуществляемыми между сетевыми центрами VPN?

   А) Проверка целостности сообщения.

   Б) Конфиденциальность (шифрование).

   В) Антивирусная защита.

   Г) Аутентификация.

3. Какая из нижеперечисленных не является функцией IPsec?

   А) Аутентификация.

   Б) Предотвращение вторжения.

   В) Проверка целостности сообщения.

   Г) Защита от повторного использования.

4. На маршрутизаторе А туннель настроен с использованием команды `tunnel destination 5.5.5.5`. На другом конце туннеля расположен маршрутизатор В. Какой из следующих ответов наиболее точно описывает конфигурацию маршрутизатора В?

   А) Подкоманда `ip address` на туннельном интерфейсе маршрутизатора В выведет 5.5.5.5.

   Б) Подкоманда `ip address` на интерфейсе маршрутизатора В, отличном от туннельного, выводит 5.5.5.5.

   В) В команде `tunnel source` маршрутизатор А должен использовать IP-адрес из той же подсети, что и адрес 5.5.5.5.

5. Маршрутизаторы А и В настроены на использование туннеля GRE и протокола OSPFv2 для изучения маршрутов IPv4 по этому туннелю. Маршрутизатор А имеет IP-адрес/маску LAN 172.16.1.0/24 и адрес отправителя туннеля 8.8.8.8. Маршрутизатор В имеет IP-адрес/маску LAN 172.16.2.0/24 и адрес отправителя туннеля 9.9.9.9. Какой из следующих маршрутов маршрутизатор А вероятнее всего изучит по протоколу OSPFv2 как исходящий интерфейс к туннелю?

   А) Маршрут к сети 172.16.1.0/24.

   Б) Маршрут к сети 172.16.2.0/24.

   В) Маршрут к сети 8.8.8.8.

   Г) Маршрут к сети 9.9.9.9.

Ключевые темы

Повторите все ключевые темы данной главы, отмеченные пиктограммой "Ключевая тема". Ключевые темы и соответствующие им страницы перечислены в табл. 7.3.

Таблица 7.3. Ключевые темы главы 7

Элемент	Описание	Страница
Список	Средства безопасности сетей VPN	255
Табл. 7.1	Три типа сетей VPN и их использование	257
Рис. 7.3	Основные этапы процесса шифрования IPsec	259
Табл. 7.2	Алгоритмы шифрования в сетях VPN	259
Рис. 7.7	Туннельные маршрутизаторы получают маршруты по туннелю IP	263
Рис. 7.9	Инкапсуляция первоначального пакета IP в пакет формата GRE	264
Рис. 7.12	Конфигурация туннеля GRE: отношения между параметрами	266
Список	Этапы настройки туннеля GRE	266

Заполните таблицы и списки по памяти

Распечатайте приложение Г с веб-сайта или его раздел, относящийся к этой главе, и заполните таблицы и списки по памяти. В приложении Д приведены заполненные таблицы и списки для самоконтроля.

Ключевые термины

После первого прочтения главы попытайтесь дать определения следующим ключевым терминам. Но не расстраивайтесь, если не все получится сразу, в главе 22 описано, как использовать эти термины на завершающем этапе подготовки к экзамену.

технология IPSec (IPsec), общие ключи (shared key), протокол защищенных сокетов (Secure Socket Layer — SSL), виртуальная частная сеть (Virtual Private Network — VPN), клиент VPN (VPN client), обобщенная маршрутная инкапсуляция (Generic Routing Encapsulation — GRE), туннель GRE (GRE tunnel)

Таблицы команд

Хоть и не обязательно заучивать информацию из таблиц данного раздела, ниже приведен список команд конфигурации и пользовательских команд главы. Фактически команды стоит запомнить, чтобы лучше понять содержимое главы и выполнить задания по подготовке к экзамену. Чтобы проверить, насколько хорошо вы запомнили команды, закройте левую сторону таблицы листом бумаги, читайте описания с правой стороны и пытайтесь вспоминать команду.

Таблица 7.4. Конфигурационные команды главы 7

Команда	Описание
`tunnel source` *`тип_интерфейса номер_интерфейса`*	Подкоманда туннельного интерфейса, косвенно определяющая IP-адрес отправителя туннеля на локальном маршрутизаторе; маршрутизатор использует настроенный интерфейс как прослушивающий
`tunnel source` *`IP-адрес`*	Подкоманда туннельного интерфейса, непосредственно определяющая IP-адрес отправителя туннеля на локальном маршрутизаторе
`tunnel destination` *`IP-адрес`*	Подкоманда туннельного интерфейса, определяющая IP-адрес получателя туннеля, расположенного на другом его конце
`tunnel mode gre`	Подкоманда туннельного интерфейса, определяющая режим туннеля, совпадающий на обоих концах туннеля. Стандартное значение — `gre`

Ответы на контрольные вопросы:

1 А. 2 В. 3 Б. 4 Б. 5 Б.

Обзор части II

Проследите свой прогресс изучения материала части по контрольному списку в следующей таблице. Подробно задачи описаны ниже.

Контрольный список обзора части II

Задача	Первая дата завершения	Вторая дата завершения
Повторите вопросы из обзоров глав		
Ответьте на вопросы обзора части		
Повторите ключевые темы		
Создайте диаграмму связей первопричин проблем IPv4		
Создайте диаграмму связей команд FHRP		

Повторите вопросы из обзоров глав

Ответьте снова на вопросы обзоров глав этой части книги, используя программное обеспечение PCPT. Инструкция по запуску программного обеспечения PCPT с вопросами обзоров глав только этой части приведена в разделе "Как просмотреть вопросы только обзоров глав конкретной части" введения к книге.

Ответьте на вопросы обзора части

Ответьте на вопросы обзора этой части книги, используя программное обеспечение PCPT. Инструкция по запуску программного обеспечения PCPT с вопросами обзоров только этой части приведена в разделе "Как просмотреть вопросы только обзоров частей" введения к книге.

Повторите ключевые темы

Снова просмотрите темы прочитанных глав, отмеченные пиктограммой "Ключевая тема". Если понятны не все их подробности, уделите время повторному изучению.

Создайте диаграмму связей первопричин проблем IPv4

Главы 4 и 5 посвящены решению проблем работоспособности сети IPv4. Для первой диаграммы связей обзора части вспомните все возможные причины проблем в сети IPv4. Затем организуйте их в диаграмму связей.

Для организации диаграммы связей, если есть несколько взаимосвязанных первопричин, группируйте их по любым категориям, которые придут на ум. Это могут быть виды симптомов, по которым вы будете искать их при локализации проблемы. Например, можно обратить внимание на первопричины с протоколом динамического конфигурирования хостов (DHCP), на отсутствие конфигурации ретранслятора DHCP (`ip helperaddress`), отсутствие подключения IP к серверу DHCP и

другие причины проблем. Сгруппируйте первопричины DHCP в один раздел, например Host DHCP, как показано в примере на рис. Ч2.1.

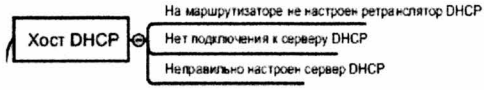


Рис. Ч2.1 Пример диаграммы связей первопричин проблем IPv4

ВНИМАНИЕ!

Более подробная информация по этой теме приведена в разделе "О диаграммах связей" введения к данной книге.

Создайте диаграмму связей команд FHRP

Эта часть детально знакомит с настройкой и проверкой трех элементов: протокола резервного маршрутизатора (HSRP), протокола балансировки нагрузки шлюза (GLBP) и обобщенной маршрутной инкапсуляцией (GRE) туннелей. Создайте диаграмму связей, организующую команды по каждой из этих трех тем, разделяя их по командам конфигурации и командам проверки.

Ответы приведены в приложении E на веб-сайте, но ваши диаграммы связей могут выглядеть иначе.

Сети TCP/IP нуждаются в маршрутах IP. Четыре главы этой части книги посвящены протоколам маршрутизации IPv4, которые рассматриваются в рамках экзамена ICND2: протокол OSPF версии 2 (глава 8), протокол EIGRP (главы 9 и 10). В главе 11 речь пойдет о поиске и устранении неисправностей протоколов OSPFv2 и EIGRP. Заметим, что глава 8 дополняет некоторыми деталями темы из книги по ICND1, а в главах 9 и 10 обсуждаются подробности протокола EIGRP, которых не было в книге по ICND1.

Часть III. Протоколы маршрутизации IP версии 4

Глава 8. “Реализация протокола OSPF для IPv4”

Глава 9. “Концепции протокола EIGRP”

Глава 10. “Реализация протокола EIGRP для IPv4”

Глава 11. “Поиск и устранение неисправностей протоколов маршрутизации IPv4”

Обзор части III

Глава 8

Реализация протокола OSPF для IPv4

Компания Cisco отнесла одни из тем по открытому протоколу поиска первого кратчайшего маршрута версии 2 (OSPFv2) к экзамену ICND1, а другие к экзамену ICND2. Поэтому в данной главе представлены три обсуждаемых в книге по ICND1 точки зрения на протокол OSPFv2 (концепция, настройка и проверка), но уже существенно подробнее.

В частности, в этой главе подробнее обсуждаются концепции протокола OSPFv2 и конкретные типы *анонсов состояния канала* (Link-State Advertisement — LSA), определение протоколом OSPF для путей передачи при вычислении метрик каждого маршрута, а также подробности скрытых процессов OSPF. Во втором главном разделе этой главы рассматривается многообластная конфигурация, а также влияние изменения стоимости интерфейса OSPF на выбор пути. И наконец, обсуждение проверки сосредоточивается на подробностях многообластных конфигураций и новых концепциях анонсов LSA.

В зависимости от вашего личного плана чтения и изучения, данная глава может показаться сложной или не сложной. Те, кто готовился к экзамену CCNA, используя план чтения из книги по ICND1, читал о протоколе OSPFv2 в главе 17. Другие, особенно те, кто готовится к двойному экзамену CCNA Routing and Switching, изучали протокол OSPFv2 совсем недавно.

Глава содержит обзор важнейших концепций и этапов настройки протокола OSPFv2 из книги ICND1. Но если с момента изучения прошло достаточно много времени, то, прежде чем приступать к изучению этой главы, возможно, имеет смысл уделить несколько минут обзору тем по протоколу OSPFv2 из книги ICND1.

В этой главе рассматриваются следующие экзаменационные темы
Технологии маршрутизации IP
Настройка и проверка протокола OSPF (одиночная область)
Соседские отношения
Состояние OSPF
Несколько областей
Настройка OSPF v2
Идентификатор маршрутизатора
Типы сообщений LSA
Различия методов маршрутизации и протоколов маршрутизации
Административное расстояние
Метрика
Следующий транзитный узел

Основные темы

Принцип работы протокола OSPF

Из двух подробно обсуждаемых в этой книге протоколов маршрутизации, OSPF и EIGRP, первый имеет больше правил, процессов и теоретических деталей. В первом из двух главных разделов этой главы рассматривается большинство деталей и концепций протокола OSPF. Эти детальные сведения позволят сетевым инженерам подготовиться к решению сетевых проблем первого и второго уровней, а также к поиску истинных первопричин любой проблемы OSPF.

Данный раздел закладывает концептуальный фундамент, а в следующем разделе рассматриваются новые темы. Некоторые из конкретных сценариев поиска и устранения неисправностей, связанных с протоколом OSPF, рассматриваются в главе 11.

Краткий обзор протокола OSPF

Если вспомнить уже известное о протоколе OSPFv2 (протоколе OSPF для сетей IPv4) из книги по ICND1, то можно логически объединить это в последовательность, представленную на рис. 8.1.

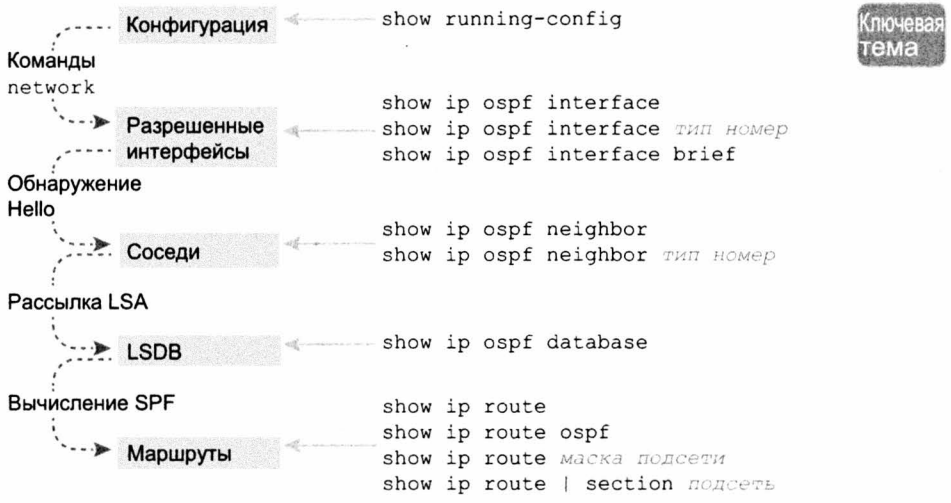


Рис. 8.1. Пакеты Hello состояния канала

Уделим немного времени рассмотрению этапов, приведенных на рисунке. Начнем с конфигурации, где командой `network` разрешен протокол OSPFv2 на некоторых интерфейсах. В результате маршрутизатор посылает и получает на этих интерфейсах пакеты OSPF Hello, надеясь обнаружить соседей OSPF. Как только обнаруживается потенциальный сосед, соседи проверяют параметры друг друга и, если они проходят, рассылают друг другу известные им анонсы LSA, заполняя свои *базы данных состояния каналов* (Link-State Database — LSDB). И наконец, используя алгоритм *поиска первого кратчайшего маршрута* (Shortest Path First — SPF), маршрути-

затор вычисляет наилучший маршрут к каждой подсети, помещая эти маршруты в свою таблицу маршрутизации IPv4.

Фактически на рис. 8.1 представлено большинство концепций и команд проверки из главы 17 книги по ICND1.

Идентификатор маршрутизатора (Router ID — RID) OSPF, представленный в первом томе книги, играет важную роль в большинстве внутренних процессов OSPFv2, обсуждаемых далее в этой главе. Идентификатор маршрутизатора (RID) является индивидуальным идентификатором маршрутизатора для протокола OSPFv2. Маршрутизаторы используют идентификатор RID в следующих целях.

- Когда маршрутизаторы посылают сообщение Hello, они просто заявляют: "Привет, вот мой RID".
- Соседи идентифицируют друг друга по идентификаторам RID, выводимым командой `show ip ospf neighbor`.
- Анонсы LSA содержат RID одного из маршрутизаторов.

Поскольку протокол OSPFv2 использует идентификаторы RID столь широко, большинство сетевых инженеров контролируют параметр RID в конфигурации. Намного проще использовать сеть OSPFv2, если идентификаторы RID каждого маршрутизатора известны или легко предсказуемы. Большинство инженеров составляют план нумерации RID, или создают список маршрутизаторов с их идентификаторами RID, или вырабатывают простой способ предсказания RID каждого маршрутизатора. Например, маршрутизатор R1 мог бы использовать RID 172.16.1.1; маршрутизатор R2 — 172.16.2.2; маршрутизатор R3 — 172.16.3.3 и т.д.

Ниже приведен список этапов выбора маршрутизатором своего идентификатора RID, когда он перезагружается и начинает процесс OSPF:

Ключевая тема

Правила выбора идентификатора маршрутизатора

1. Используется значение из подкоманды OSPF `router-id` *rid*.
2. Если этап 1 неприменим, то из всех петлевых интерфейсов, на которых настроен IP-адрес и находящихся в состоянии up, выберите самое большое числовое значение IPv4-адреса.
3. Если неприменимы этапы 1 и 2, используйте ту же логику, что и на этапе 2, но для всех непетлевых интерфейсов.

И наконец, последнее замечание об идентификаторе RID протокола OSPF: каждый маршрутизатор выбирает свой RID при инициализации OSPF. Инициализация осуществляется при начальной загрузке операционной системы IOS или после ввода команды `clear ip ospf process`. Например, если петлевой интерфейс и IPv4-адрес будут добавлены после настройки протокола OSPFv2, то процесс OSPFv2 не будет рассматривать IP-адрес нового петлевого интерфейса как RID до следующего запуска процесса OSPF.

Обратите также внимание на то, что если процесс OSPF не сможет найти RID для использования, то он просто не будет работать.

Установление соседских отношений при обмене базами LSDB

Основной задачей протокола OSPFv2 является помощь в изучении маршрутов IPv4. Для этого маршрутизаторы OSPFv2 должны стать соседями, а затем обменяться анонсами LSA и базами данных состояния каналов (LSDB). Рассмотрим некоторые частности протокола OSPFv2 и состояния соседей.

ВНИМАНИЕ!

Протоколы OSPF действуют немного по-разному в двухточечных каналах связи (проще) и в каналах связи Ethernet (сложнее). Для простоты обучения в последующих примерах подразумевается применение правил для двухточечных каналов связи. Разновидности OSPF, встречающиеся в других топологиях, например Ethernet, рассматриваются далее, в разделе "Использование выделенных маршрутизаторов на каналах связи Ethernet".

Соглашение о соседских отношениях

Когда двухточечный канал связи отказывает, у протокола OSPF не может быть на нем никаких соседей. Когда канал связи восстанавливается, соседние маршрутизаторы на концах канала связи проходят несколько промежуточных состояний, включая обнаружение соседа, проверку параметров на предмет возможности стать соседями и обмен анонсами LSA. Этот процесс известен как обмен базами данных.

На рис. 8.2 представлено несколько состояний соседей в начале формирования соседских отношений OSPF. В центре рисунка представлены сообщения Hello, а справа и слева обозначены состояния соседей.



Рис. 8.2. Предварительные состояния соседей

Согласно этапам на рисунке, процесс начинается при отключенном канале связи, когда маршрутизаторы ничего не знают ни друг о друге, ни о том, что они соседи OSPF. В результате у них нет никакого состояния, информация друг о друге отсутствует, и они не указывают друг друга в выводе команды `show ip ospf neighbor`. На этапе 2 маршрутизатор R1 посылает первый пакет Hello — так маршрутизатор R2 узнает о существовании маршрутизатора R1 как маршрутизатора OSPF. Теперь маршрутизатор R2 укажет маршрутизатор R1 как соседа с промежуточным состоянием Init (инициализация).

Процесс продолжается на этапе 3, где маршрутизатор R2 возвращает сообщение Hello. Это сообщение оповещает маршрутизатор R1 о существовании маршрутиза-

тора R2 и позволяет маршрутизатору R1 перейти в состояние 2-way (двусторонний канал). На этапе 4 маршрутизатор R2 получает следующее сообщение Hello от маршрутизатора R1 и маршрутизатор R2 также может перейти в состояние 2-way.

Чтобы узнать больше о том, почему маршрутизаторы переходят в следующее состояние, вернемся к деталям этих сообщений и найдем примечание "seen". Когда маршрутизатор получает сообщение Hello от потенциального соседа и убеждается в соответствии его параметров параметрам локального маршрутизатора, локальный маршрутизатор уверяется в наличии нового соседа на канале связи. Например, сообщение от маршрутизатора R2 к маршрутизатору R1 (этап 3 на рисунке) гласит "Seen [1.1.1.1]". Это означает, что маршрутизатор R2 получил прежнее сообщение Hello от маршрутизатора R1 (на этапе 2) и что маршрутизатор R2 считает все параметры подходящими для того, чтобы эти два маршрутизатора могли стать соседями.

Завершив эти предварительные этапы, каждый маршрутизатор достигает состояния 2-way со своим соседом. На настоящий момент истинны два следующих факта:

- маршрутизатор получил от соседа сообщение Hello с идентификатором RID этого маршрутизатора, указанного как его сосед;
- маршрутизатор проверил все параметры в полученном от соседа сообщении Hello и не нашел проблем. Маршрутизатор стал соседом.

Обмен полными анонсами LSA с соседями

Состояние 2-way соседа OSPF означает, что маршрутизатор доступен для обмена с соседом базами LSDB. Другими словами, маршрутизаторы готовы начать двусторонний обмен базами LSDB. Таким образом, как только два маршрутизатора на двухточечном канале связи достигают состояния 2-way, они могут немедленно перейти к обмену базами данных.

Процесс обмена базами данных может задействовать несколько сообщений OSPF и несколько промежуточных состояний соседей. В этой главе упоминается несколько сообщений и состояний, включая состояние full (полная синхронизация), когда обмен базами данных завершен.

После того как два маршрутизатора решают обменяться базами данных, они не просто посылают все содержимое своей базы данных. Сначала они обмениваются списками анонсов LSA из своих баз данных, но не всеми подробностями анонсов LSA, а только их списками. Каждый маршрутизатор проверяет, какие из анонсов LSA у него уже есть, а затем запрашивает у другого маршрутизатора только те анонсы LSA, которых у него еще нет.

Например, маршрутизатор R1 мог бы послать маршрутизатору R2 список из 10 анонсов LSA (используя пакет *описания базы данных OSPF* (OSPF Database Description), или *пакет DD*). Затем маршрутизатор R2 проверяет свою базу LSDB и находит в ней 6 из этих 10 анонсов. Таким образом, маршрутизатор R2 запросит у маршрутизатора R1 (используя пакет Request) только четыре анонса LSA.

К счастью, большинство связанных с протоколом OSPFv2 действий не требует подробного знания конкретных этапов работы протокола. Но некоторые из терминов используются весьма часто, поэтому их следует запомнить. В частности, сообщения OSPF, фактически передающие анонсы LSA между соседями, называют пакетами *обновления состояния канала* (Link-State Update — LSU). Таким образом, пакет LSU содержит структуры данных *анонсов состояния канала* (Link-State Adver-

tisement — LSA). Анонсы LSA являются не пакетами, а скорее описывающими топологию структурами данных, хранящихся в базе LSDB.

Некоторые из этих терминов и процессов приведены в примере на рис. 8.3. Это продолжение примера процесса обмена базами данных между маршрутизаторами R1 и R2 на рис. 8.2 и 8.3. В центре представлены сообщения протокола, а слева и справа — состояния соседей на разных этапах процесса. В частности, рассмотрим два этапа.

- Маршрутизаторы обмениваются анонсами LSA внутри пакетов LSU.
- По завершении процесса маршрутизаторы достигают состояния полной синхронизации, когда они полностью обменялись содержимым своих баз LSDB.

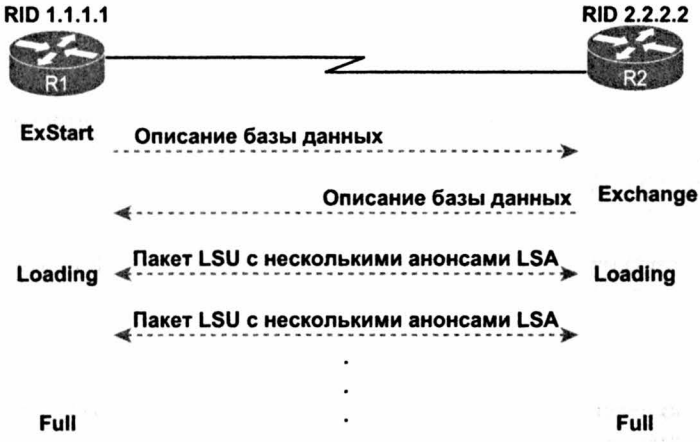


Рис. 8.3. Пример обмена базами данных, завершающийся состоянием полной синхронизации

Поддержка соседей и баз LSDB

Как только соседи достигают состояния полной синхронизации, они завершают все начальные работы по обмену информацией OSPF между двумя соседями. Но для продолжения соседских отношений соседи все еще должны выполнять некоторые небольшие задачи.

В первую очередь маршрутизаторы контролируют соседские отношения, используя сообщения Hello и два взаимосвязанных таймера: Hello и Dead. Маршрутизаторы посылают каждому соседу сообщения Hello через каждый период Hello. Каждый маршрутизатор ожидает сообщения Hello от каждого соседа на протяжении периода Hello, но если сосед не получил сообщения на протяжении периода Dead (обычно равный 4 периодам Hello), то отсутствие сообщений Hello означает отказ соседнего маршрутизатора.

Маршрутизаторы должны реагировать на изменения топологии, и соседские отношения играют ключевую роль в этом процессе. Когда что-то изменяется, один или несколько маршрутизаторов рассылает один или несколько анонсов LSA. Затем маршрутизаторы должны разослать изменения анонсов LSA каждому соседу, чтобы соседи могли изменить свои базы LSDB.

Предположим, например, что на коммутаторе LAN пропало питание, поэтому состояние интерфейса G0/0 соответствующего маршрутизатора изменилось с up/up на down/down. Маршрутизатор создает модифицированные анонсы LSA, в которых интерфейс G0/0 маршрутизатора отмечен как отключенный. Затем этот маршрутизатор рассылает анонсы LSA своим соседям, а они рассылают их соседям, пока у всех маршрутизаторов не будет снова идентичных копий базы LSDB. Теперь база LSDB каждого маршрутизатора отражает тот факт, что первоначальный интерфейс G0/0 маршрутизатора отказал, поэтому каждый маршрутизатор использует алгоритм SPF для повторного расчета любых маршрутов, на которые повлиял отказ интерфейса.

Третья задача поддержки соседских отношений заключается в периодической рассылке анонсов LSA, даже когда сеть совершенно стабильна. Стандартно каждый создающий анонсы LSA маршрутизатор обязан повторно рассылать анонсы LSA каждые 30 минут (стандартно), даже если никаких изменений не происходит. (Обратите внимание, что у каждого анонса LSA есть отдельный таймер, отсчитываемый от момента создания анонса, поэтому в сети не происходит события одномоментного переполнения трафиком рассылаемых анонсов LSA.)

Таким образом, поддержка соседских отношений сводится к трем следующим задачам.

- Контролировать состояние соседа за счет рассылки сообщений Hello на основании таймера Hello, а также прослушивать сообщения Hello в период, определенный таймером Dead.
- Сообщать в анонсах LSA о любых изменениях всем соседям.
- Регулярно рассылать анонсы LSA, даже без изменений, до истечения периода их существования (стандартно каждые 30 минут).

Использование выделенных маршрутизаторов на каналах связи Ethernet

Поведение протокола OSPF отличается на интерфейсах некоторых типов, особенно если сравнивать двухточечные каналы и каналы связи Ethernet. В частности, на каналах связи Ethernet протокол OSPF выбирает в подсети один из маршрутизаторов на роль *выделенного маршрутизатора* (Designated Router — DR). Маршрутизатор DR играет ключевую роль в процессе обмена базами данных по правилам, отличным от таковых у двухточечных каналов связи. Рассмотрим детали на примере (рис. 8.4), где пять маршрутизаторов OSPFv2 находятся в той же сети VLAN Ethernet. Эти пять маршрутизаторов OSPF выбирают один маршрутизатор на роль DR, маршрутизатор A, и один на роль *резервного DR* (Backup DR — BDR), маршрутизатор B.

Обмен базами данных на канале связи Ethernet осуществляется не между каждой парой маршрутизаторов в той же сети VLAN или подсети, а между маршрутизатором DR и каждым другим маршрутизатором. Выделенный маршрутизатор гарантирует получение копии всех анонсов LSA другими маршрутизаторами. Другими словами, обмен базами данных осуществляется по путям, представленным на рис. 8.5.

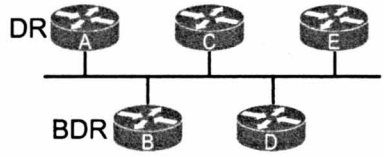


Рис. 8.4. Маршрутизаторы A и B выбраны маршрутизаторами DR и BDR соответственно



Рис. 8.5. Обмен базами данных с выделенным маршрутизатором в сети Ethernet

Протокол OSPF использует концепцию BDR (резервного выделенного маршрутизатора), поскольку выделенный маршрутизатор (DR) очень важен для процесса обмена базами данных. Маршрутизатор BDR отслеживает состояние маршрутизатора DR, а при его отказе принимает на себя его роль. (При отказе DR и передаче его функций BDR выбирается новый маршрутизатор BDR.)

Теперь, когда вы, возможно, немного устали от теории, пришло время продемонстрировать то, что фактически можно увидеть в выводе команд `show` на маршрутизаторе. Поскольку оба маршрутизатора, DR и BDR, осуществляют полный обмен базами данных со всеми другими маршрутизаторами OSPF в локальной сети, они обеспечивают полную синхронизацию со всеми соседями. Однако маршрутизаторы, не являющиеся ни DR, ни BDR, называемые *невыделенными маршрутизаторами* (DROther), никогда не достигают между собой полной синхронизации OSPF, поскольку не обмениваются базами данных. В результате команда `show ip ospf neighbor` на этих маршрутизаторах одних соседей выводит регулярно, других только в состоянии 2-way, но не в состоянии full.

Например, при нормальной работе протокола OSPF в локальной сети Ethernet (см. рис. 8.5) команда `show ip ospf neighbor` на маршрутизаторе C (невыделенный маршрутизатор) показала бы следующее:

- два соседа (маршрутизаторы A и B, DR и BDR соответственно) находятся в состоянии full (полной синхронизации);
- два соседа (D и E) находятся в состоянии 2-way (двустороннего канала).

Это различие в поведении соседей OSPF в локальной сети (когда одни соседи достигли полной синхронизации, а другие нет) обусловливает наличие еще двух терминов OSPF: *согласованный* (adjacent) и *полностью согласованный* (fully adjacent). Полностью согласованные соседи достигают полной синхронизации, обменявшись базами LSDB непосредственно. Согласованные устройства — это невыделенные маршрутизаторы, вполне резонно оставшиеся в состоянии 2-way, но которые нико-

гда не смогут достичь состояния полной синхронизации. Эти ключевые концепции и связанным с ними состояния OSPF представлены в табл. 8.1.

Ключевая тема

Таблица 8.1. Стабильные состояния соседей OSPF и их значения

Состояние соседей	Термин согласованности	Смысл
2-way	Согласованный (adjacent)	Сосед послал сообщение Hello, содержащее RID локального маршрутизатора в списке замеченных маршрутизаторов, причем проверка параметров соседа прошла успешно. Если оба соседа являются невыделенными маршрутизаторами, то оба должны оставаться в этом состоянии
Full	Полностью согласованный (fully adjacent)	Оба маршрутизатора обменялись базами LSDB и полностью согласованы, а значит, они закончили обмен содержимым баз LSDB

Масштабирование OSPF с использованием областей

В некоторых сетях протокол OSPF можно применять не задумываясь особо о проблемах проекта. Достаточно разрешить протокол OSPF на всех маршрутизаторах, поместить все интерфейсы в ту же область (обычно область 0), и все сработает! На рис. 8.6 приведен пример такой сети с 11 маршрутизаторами и всеми интерфейсами в области 0.

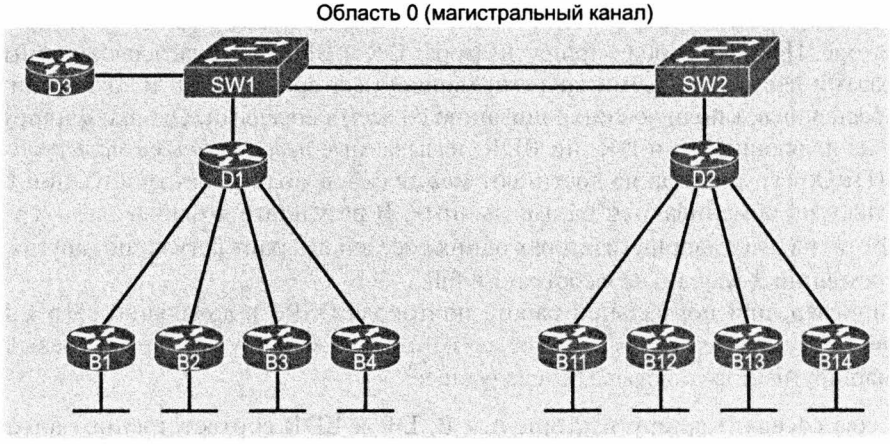


Рис. 8.6. Одиночная область OSPF

Большим сетям OSPFv2 проекты с одиночной областью не подходят. Вообразите, например, корпоративную сеть с 900 маршрутизаторами, а не 11-ю, и несколькими тысячами подсетей. Кроме того, учтите процессорное время, необходимое на выполнение алгоритма SPF для всех топологических данных, — оно весьма продолжительное. В результате время конвергенции OSPFv2 (время, необходимое для реакции на изменения в сети) может стать слишком большим. Маршрутизаторам может даже не хватить оперативной памяти. Возможны и следующие дополнительные проблемы.

- Большие топологические базы занимают больше оперативной памяти маршрутизаторов.
- Обработка больших топологических баз с помощью алгоритма SPF требует большей мощности процессора. Загрузка процессора устройства растет экспоненциально при увеличении размера базы.
- Одно изменение состояния интерфейса (включение или выключение) приводит к запуску на маршрутизаторе алгоритма SPF.

Решение заключается в разделении одной большой базы LSDB на несколько меньших с использованием области OSPF. При использовании областей каждый канал связи помещается в свою область. Алгоритм SPF осуществляет свои сложные математические действия с топологическими данными только области. Например, объединенная сеть из 1000 маршрутизаторов и 2000 подсетей, разделенная на 100 областей, имела бы в среднем область из 10 маршрутизаторов и 20 подсетей. Алгоритму SPF на маршрутизаторе достаточно обработать топологию десятка маршрутизаторов и 20 каналов связи, а не всех 1000 маршрутизаторов и 2000 каналов связи.

Так насколько большой должна быть сеть, чтобы имело смысл делить ее на области OSPF? Ответа на этот вопрос нет, поскольку поведение процесса SPF зависит в значительной степени от скорости процессора, объема оперативной памяти, размера базы LSDB и т.д. Как правило, сети размером более нескольких дюжин маршрутизаторов нуждаются в областях. Некоторые документы рекомендуют использовать области в сетях, насчитывающих более 50 маршрутизаторов.

Далее рассмотрим проект области OSPF, а также причины, по которым области помогают лучше выполнять работу сетей OSPF.

Области OSPF

Проект областей OSPF следует нескольким простым правилам. Для применения правил начните с рисунка объединенной сети, где обозначены маршрутизаторы и все интерфейсы. Затем выберите область для каждого интерфейса маршрутизатора следующим образом.

Правила проекта областей OSPF



- Помещайте в одну область все интерфейсы, подключенные к той же подсети.
- Область должна быть непрерывной.
- Некоторые маршрутизаторы могут быть внутренними относительно области, все их интерфейсы находятся в одной области.
- Некоторые маршрутизаторы могут быть *граничными маршрутизаторами области* (Area Border Router — ABR), поскольку одни их интерфейсы подключены к магистральной области, а другие к не магистральной.
- Все не магистральные области должны соединиться с магистральной областью (областью 0) хотя бы через один маршрутизатор ABR, соединенный и с магистральной, и с не магистральной областью.

Рассмотрим пример, приведенный на рис. 8.7. Инженер начал со схемы сети, на которой представлены все 11 маршрутизаторов и их каналы связи. В область 1 слева инженер поместил четыре последовательных канала и локальные сети, подключен-

ные к маршрутизаторам ветвей B1–B4. Точно так же в область 2 он поместил каналы связи с ветвями через маршрутизаторы B11–B14 и их локальные сети. Обе области должны быть соединены с магистральной областью 0, поэтому он поместил интерфейсы LAN маршрутизаторов D1 и D2 в область 0, наряду с маршрутизатором D3, создав магистральную область.

На рисунке также приведено несколько важных терминов проекта области OSPF. Объяснения этих, а также некоторых других терминов приведены в табл. 8.2.

Ключевая тема

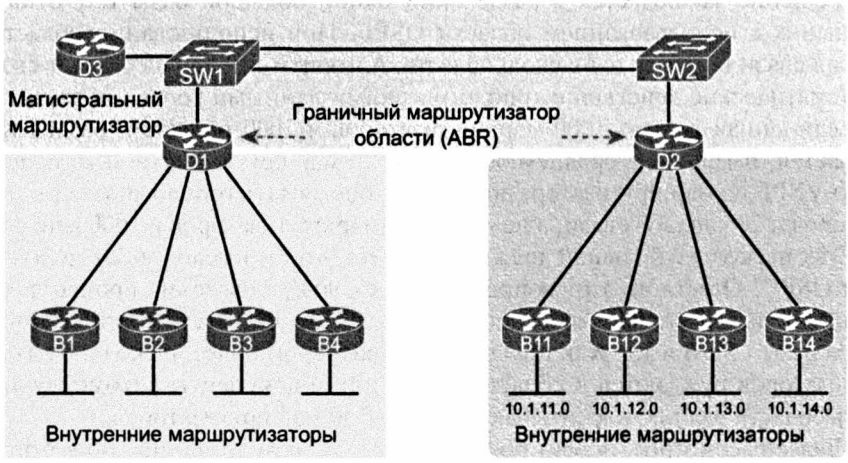


Рис. 8.7. Проект с тремя областями OSPF и маршрутизаторами D1 и D2 в качестве ABR

Ключевая тема

Таблица 8.2. Терминология проекта OSPF

Термин	Описание
Граничный маршрутизатор области (Area Border Router — ABR)	Маршрутизатор OSPF, интерфейсы которого подключены к магистральной области и как минимум к одной обычной
Магистральный маршрутизатор (backbone router)	Маршрутизатор, все интерфейсы которого находятся в одной (магистральной) области
Внутренний маршрутизатор (internal router)	Маршрутизатор, все интерфейсы которого находятся в одной (не магистральной) области
Область (area)	Набор маршрутизаторов и каналов связи, совместно использующих ту же информацию баз LSDB, но в целях эффективности не делящихся ею с маршрутизаторами из других областей
Магистральная область (backbone area)	Специальная область OSPF (область 0), с которой должны быть соединены все остальные области

Окончание табл. 8.2

Термин	Описание
Внутриобластной маршрут (intra-area route)	Маршрут к подсети в той же области, что и маршрутизатор
Межобластной маршрут (interarea route)	Маршрут к подсети в области, отличной от области маршрутизатора

Как области сокращают время вычисления SPF

Рис. 8.7 демонстрирует типичный проект области и связанную с областями терминологию, но он не отображает мощи и преимуществ областей. Чтобы понять, как области сокращают работу алгоритма SPF, необходимо разобраться в том, как происходят изменения в базах LSDB области.

Большую часть времени алгоритм SPF тратит на обработку подробностей топологии, а именно на маршрутизаторы и соединяющие их каналы связи. Области сокращают объем работ алгоритма SPF, поскольку в списке LSDB каждой области указаны маршрутизаторы и каналы связи только этой области (рис. 8.8, *слева*).

Хотя топологической информации в базе LSDB стало меньше, в ней все еще должна быть информация обо всех подсетях во всех областях, чтобы каждый маршрутизатор мог создать маршруты IPv4 для всех подсетей. Таким образом, в проекте областей OSPFv2 используется очень краткая обобщенная информация о подсетях в других областях. Анонсы LSA не включают топологическую информацию о других областях, поэтому они не требуют от алгоритма SPF большого количества работы вообще. Все эти подсети выглядят как подсети, соединенные с маршрутизатором ABR (в данном случае с маршрутизатором D1).

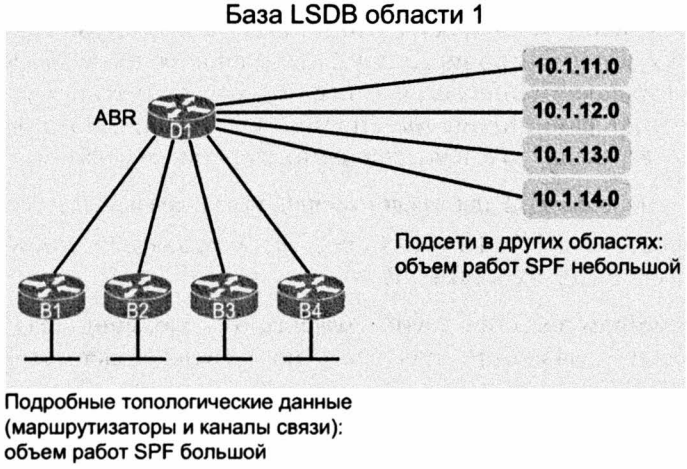


Рис. 8.8. Концепция баз LSDB меньшей области 1

Преимущества областей OSPF

Таким образом, проект с одиночной областью OSPF хорош для малых сетей OSPF, он позволяет избежать дополнительных сложностей и сделать сеть немного проще. Планирование также потребует меньше усилий, поскольку не нужно думать о том, какие части сети в какую область поместить.

В больших сетях использование нескольких областей улучшает работу протокола OSPF несколькими способами. Ниже приведен список ключевых доводов в пользу использования нескольких областей в больших сетях OSPF.

Ключевая тема **Преимущества многообластных проектов в больших объединенных сетях**

- Меньший размер базы LSDB в каждой области требует меньше памяти.
- Процессорам маршрутизаторов требуется меньше циклов на обработку меньших баз LSDB областей по алгоритму SPF, сокращаются дополнительные затраты процессора и улучшается время конвергенции.
- Изменения в сети (например, отказ и восстановление каналов связи) требуют вычислений SPF только на тех соединенных с областью маршрутизаторах, где канал связи изменил состояние, что сокращает количество маршрутизаторов, на которых повторно запускается протокол SPF.
- Между областями можно передавать меньше информации в анонсах, сокращая ширину полосы пропускания, необходимую для передачи анонсов LSA.

Анонсы состояния канала

Анонсы LSA протокола OSPF обычно вызывают затруднение, когда встречаешься с ними впервые. Вывод команды `show ip ospf database` довольно длинен, хоть она и выводит сокращенную информацию. Вывод команд, демонстрирующих конкретный список LSA, намного подробней. Детали представлены как некий код, использующий много чисел. На первый взгляд это выглядит не очень понятно.

Но если рассматривать анонсы LSA с точки зрения областей OSPF и их проекта, то некоторые из наиболее распространенных типов анонсов LSA будут иметь больше смысла. Рассмотрим, например, базу LSDB одной области, представленной на рис. 8.8. К подробностям топологии относятся маршрутизаторы и каналы связи между маршрутизаторами. Кроме того, протокол OSPF определяет первые два типа анонсов LSA, отвечающих за эти подробности, следующим образом.

- Один анонс *router LSA* для каждого маршрутизатора в области.
- Один анонс *network LSA* для каждой сети, обладающей маршрутизатором DR плюс по одному для соседей DR.

Теперь рассмотрим подсети в других областях, расположенных на рис. 8.8, *справа*. Эта краткая обобщенная информация о подсетях в других областях (в основном только идентификаторы подсетей и маски) представляет собой третий тип анонсов LSA.

- Один анонс *summary LSA* для каждого идентификатора подсети, расположенной в другой области.

Рассмотрим эти три типа анонсов LSA немного подробней; краткая информация о них приведена в табл. 8.3.

Таблица 8.3. Три типа анонсов LSA протокола OSPFv2, используемых в многообластных проектах OSPF

Ключевая тема

Название	Номер	Первичная цель	Содержимое LSA
Router LSA	1	Описание маршрутизатора	RID, интерфейсы, IP-адрес/маска, текущее состояние интерфейса
Network LSA	2	Описание сети, обладающей DR	IP-адреса маршрутизаторов DR и BDR, идентификатор подсети, маска
Summary LSA	3	Описание подсети в другой области	Идентификатор подсети, маска, RID маршрутизатора ABR, передавшего анонс LSA

ВНИМАНИЕ!

В некоторых сетях наряду с протоколом OSPF используются и другие протоколы маршрутизации. В этом случае один или несколько маршрутизаторов, выполняющих и протокол OSPF, и другой протокол маршрутизации, действуют как *граничный маршрутизатор автономной системы* (Autonomous System Border Router — ASBR), перераспределяющий информацию о маршрутизации между протоколом OSPF и другим протоколом. В таком случае маршрутизатор ASBR создает анонс LSA типа 4, описывающий сам маршрутизатор ASBR, и анонс LSA типа 5 для каждого внешнего маршрута, полученного от другого протокола маршрутизации и анонсируемого теперь по протоколу OSPF.

Анонсы router LSA составляют большую часть внутриобластной топологии

Протокол OSPF нуждается в очень подробной топологической информации о каждой области. Маршрутизаторы в области X должны знать все подробности о топологии в области X. Для обмена подробностями о маршрутизаторах и каналах связи в области маршрутизаторы создают и рассылают анонсы типа 1 (router LSA) и типа 2 (network LSA).

Анонсы router LSA, известные также как анонсы LSA типа 1, подробно описывают маршрутизатор. Они содержат RID маршрутизатора, его интерфейсы, его IPv4-адреса и маски, состояния его интерфейсов и примечания о том, какие соседи известны маршрутизатору на его интерфейсах.

Прежде чем приступать к просмотру конкретных экземпляров, рассмотрим сначала рис. 8.9. Здесь представлена топология объединенной сети с подсетями. Поскольку объединенная сеть мала, инженер выбрал проект одиночной области со всеми интерфейсами, находящимися в магистральной области 0.

В проекте одиночной области, спланированном для этой небольшой объединенной сети, база LSDB будет содержать четыре анонса router LSA. Каждый маршрутизатор создает анонс router LSA для себя, с его собственным RID как идентификатором. В анонсе LSA указаны его собственные интерфейсы, IP-адреса/маски и указатели на соседей.

Как только у всех четырех маршрутизаторов будут копии всех четырех анонсов router LSA, алгоритм SPF может математически проанализировать анонсы LSA, чтобы создать модель. Концептуально модель будет похожа на рис. 8.10. Обратите внимание на то, что каждый маршрутизатор на рисунке представлен значением его RID. У каждого маршрутизатора есть указатели, представляющие каждый из его интерфейсов, а поскольку анонсы LSA идентифицируют соседей, алгоритм SPF может выяснить, какие интерфейсы с какими другими маршрутизаторами соединены.

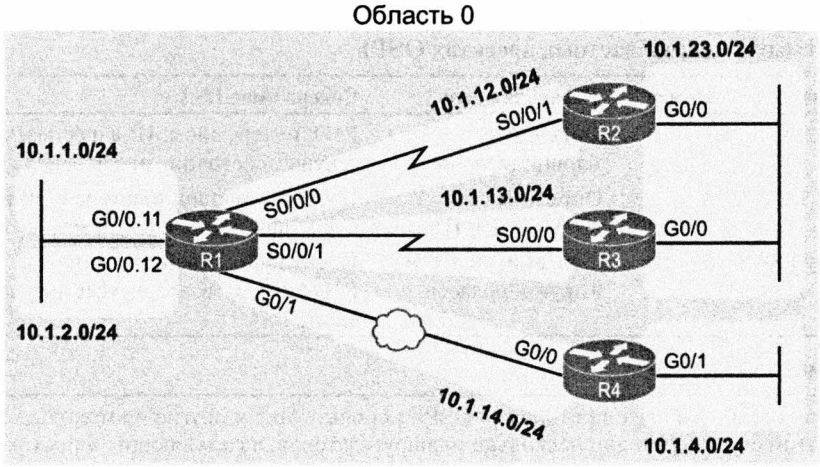


Рис. 8.9. Корпоративная сеть с семью подсетями IPv4

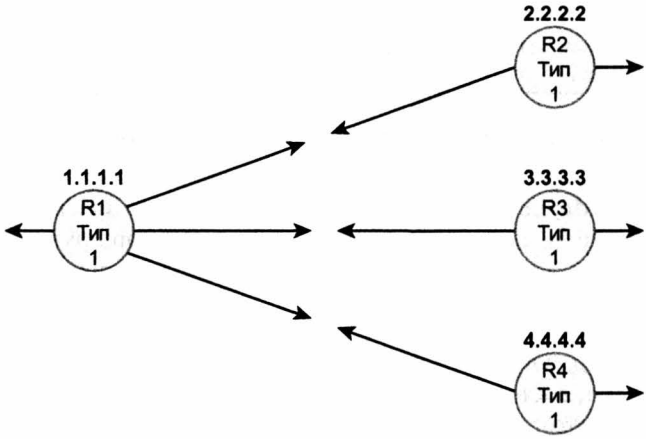


Рис. 8.10. Анонсы LSA типа 1 в проекте одиночной области

Анонсы network LSA завершают внутриобластную топологию

Принимая во внимание, что анонсы router LSA определяют большую часть внутриобластной топологии, анонсы network LSA определяют остальное. Кроме того, когда протокол OSPF выбирает маршрутизатор DR в некой подсети *и* у этого маршрутизатора DR есть по крайней мере один сосед, протокол OSPF рассматривает эту подсеть как еще один узел в математической модели сети. Чтобы представить такую сеть, маршрутизатор DR создает и рассылает анонсы network LSA (тип 2) для этой сети (подсети).

Например, на рис. 8.9 ранее была одна локальная сеть Ethernet и одна глобальная. Локальная сеть Ethernet выберет DR между маршрутизаторами R2 и R3. Эти два маршрутизатора станут соседями; какой бы из них не стал маршрутизатором DR, он создаст анонс network LSA. Точно так же маршрутизаторы R1 и R4 соединены с сетью WAN Ethernet, поэтому маршрутизатор DR на этом канале связи создаст анонс network LSA.

На рис. 8.11 представлена полная версия внутриобластного анонса LSA в области 0 рассматриваемого проекта. Обратите внимание, что анонсы router LSA фактически указывают на анонсы network LSA, когда они существуют, что позволяет процессу SPF объединить все части вместе.

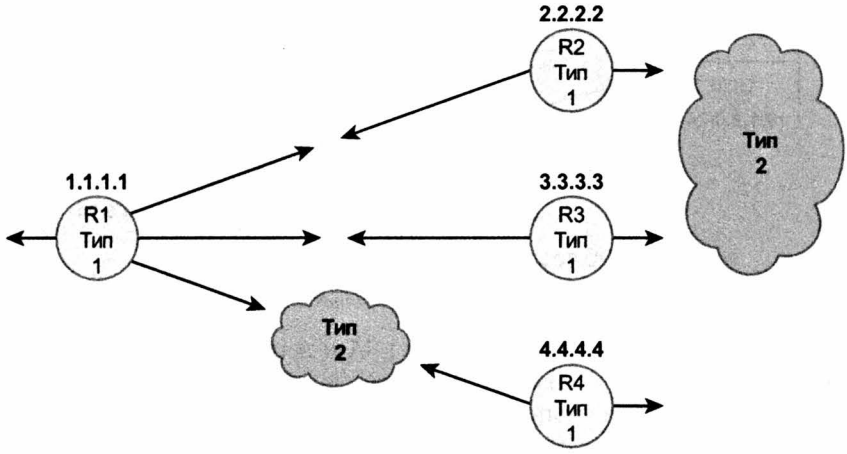


Рис. 8.11. Анонсы LSA типа 1 и 2 в области 0 проекта одиночной области

ВНИМАНИЕ!

Схемы на двух последних рисунках немного напоминают головоломку. Алгоритм SPF просто решает эту головоломку, но, взглянув на все числа в различных анонсах LSA, можно увидеть, какие анонсы LSA за какими следуют.

И наконец, обратите внимание, что в этом примере проекта одиночной области отсутствует анонс summary LSA (тип 3). Эти анонсы LSA представляют подсети в других областях, а здесь других областей нет. Анонсы summary LSA демонстрирует следующий пример.

Анонсы LSA в многообластном проекте

Теперь перейдем от проекта одиночной области к проекту с многими областями, что оказывает следующее влияние на анонсы LSA.

- В каждой области меньше маршрутизаторов и анонсов network LSA.
- У маршрутизаторов ABR есть копии баз LSDB для каждой области, к которой они подключены.
- У каждого маршрутизатора ABR есть анонс router LSA для каждой области в базе LSDB.
- Каждой области необходим анонс summary LSA (тип 3), чтобы описать подсети в других областях.

Прежде чем сосредоточиться на анонсах summary LSA, рассмотрим новый пример на рис. 8.12, использующий ту же топологию объединенной сети, что и рис. 8.9, но теперь с многими областями и маршрутизатором R1 как единственным маршрутизатором ABR.

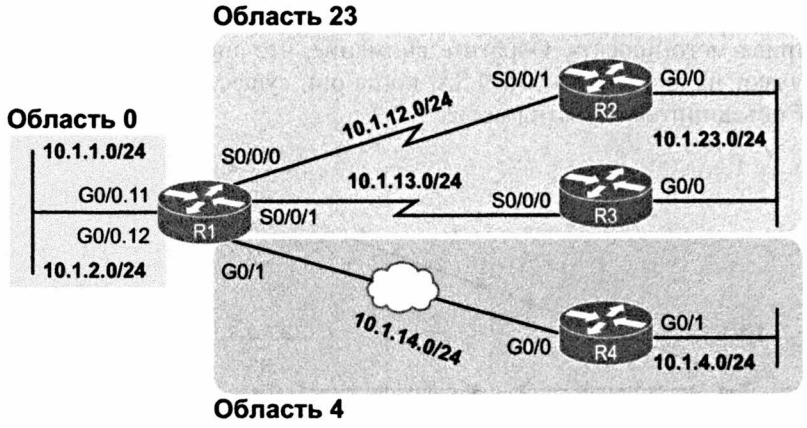


Рис. 8.12. Проект с многими областями той же объединенной сети, что и на рис. 8.9

Теперь рассмотрим, какие анонсы router LSA и network LSA должны быть в базе LSDB области 4. Помните, у базы LSDB области должны быть анонсы router LSA для маршрутизаторов области и анонсы network LSA для сетей в области (ведь у маршрутизатора DR есть по крайней мере один сосед). Таким образом, база LSDB области 4 будет включать два анонса router LSA (для маршрутизаторов R1 и R4) и один анонс network LSA для сети между маршрутизаторами R1 и R4, как показано на рис. 8.13.

Теперь коротко остановимся на подсетях всей объединенной сети. Разделенная на области, она представляет собой следующее:

- три подсети в области 23;
- две подсети в области 4;
- две подсети в области 0.

Маршрутизаторы в области 4 должны знать об этих пяти подсетях, находящихся вне области 4, а для этого маршрутизатор ABR (R1) рассылает анонсы summary LSA в области 4.

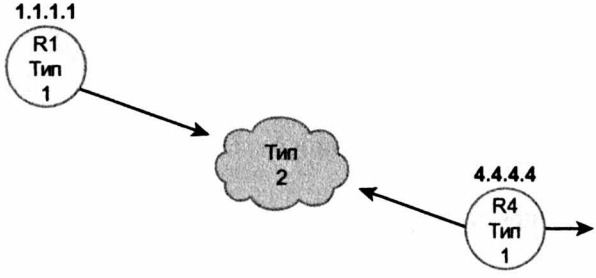
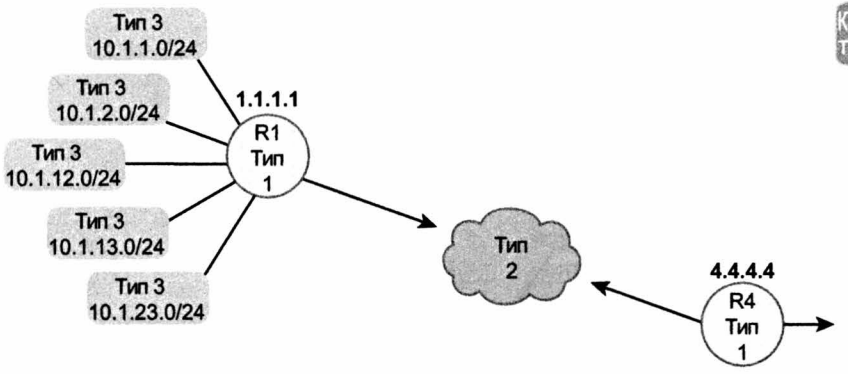


Рис. 8.13. Анонсы router LSA и network LSA только в области 4, согласно проекту с многими областями на рис. 8.12

Анонсы summary LSA (тип 3) описывают подсети, находящиеся в другой области. В первую очередь, они содержат идентификаторы подсети и маски, идентифицирующие конкретные подсети. Анонсы LSA содержат также идентификатор RID маршрутизатора ABR, создающего и рассылающего анонсы summary LSA в области.

Благодаря идентификации маршрутизатора ABR эти подсети с точки зрения топологии выглядят как подключенные к маршрутизатору ABR. В новом примере маршрутизатор ABR R1 создает и рассылает пять анонсов summary LSA, представленных в верхнем левом углу на рис. 8.14.



Ключевая тема

Рис. 8.14. Анонсы LSA типа 3, введенные маршрутизатором ABR R1 в базу LSDB области 4

ВНИМАНИЕ!

Анонс summary LSA протокола OSPF вовсе не означает, что маршрутизатор осуществляет суммирование маршрутов (процесс, в ходе которого несколько маршрутов к нескольким подсетям анонсируются как один маршрут для одной большой подсети).

Вычисление алгоритмом SPF наилучших маршрутов

Как можно заметить, анонсы LSA содержат очень полезную информацию, но не конкретную информацию, которую маршрутизатор должен добавить в свою таблицу маршрутизации IPv4. Другими словами, маршрутизатор не может просто скопировать информацию о маршруте из базы LSDB в запись таблицы маршрутизации IPv4. Вместо этого маршрутизатор запускает математический механизм SPF, чтобы выбрать наилучший маршрут и добавить его в таблицу. Маршрут включает номер подсети и маску, исходящий интерфейс и IP-адрес следующего транзитного маршрутизатора.

Хотя инженеры не обязаны знать математические подробности алгоритма SPF, но предсказать, какие маршруты алгоритм SPF выберет в качестве наилучших, они действительно должны. Алгоритм SPF вычисляет все маршруты для подсети, т.е. все возможные маршруты от маршрутизатора до подсети получателя. Если существует несколько маршрутов, то маршрутизатор сравнивает их метрики, выбирая маршрут с наилучшей (самый низкой) метрикой, и добавляет его к таблице маршрутизации. Хотя математический механизм протокола SPF может быть очень сложным, инженерам для предсказания результата вполне достаточно схемы сети, информации о состоянии маршрутизаторов и простых математических действий.

Ключевая тема

Как протокол OSPF вычисляет стоимость маршрута

Идентифицировав маршрут, алгоритм SPF осуществляет вычисление следующим образом: суммируются стоимости всех исходящих интерфейсов OSPF на маршруте.

На рис. 8.15 приведен пример с тремя возможными маршрутами от маршрутизатора R1 до подсети X (172.16.3.0/24) внизу рисунка.

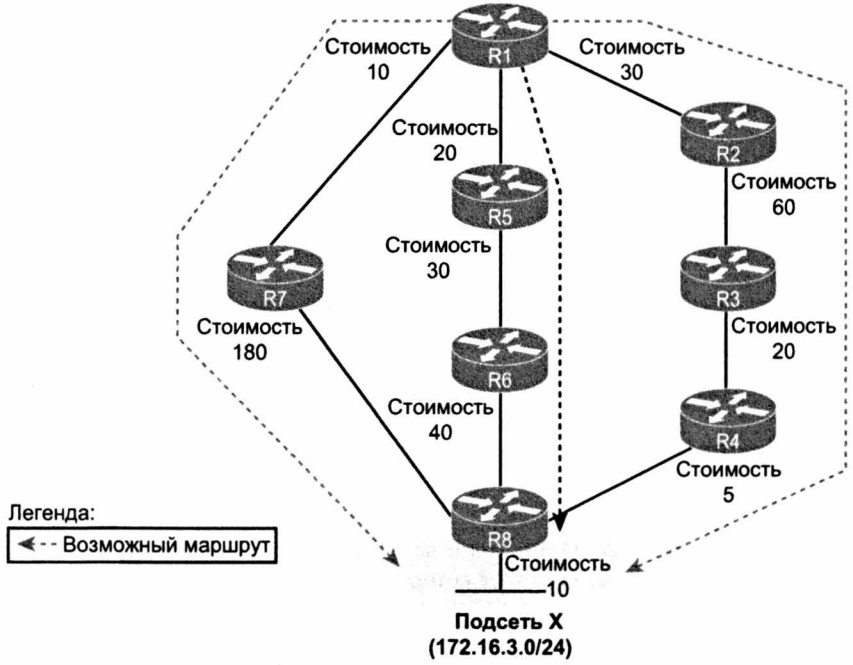


Рис. 8.15. Дерево SPF для выбора маршрута от маршрутизатора R1 к сети 172.16.3.0/24

ВНИМАНИЕ!

Протокол OSPF учитывает стоимость *исходящих* интерфейсов только на каждом маршруте. Он не добавляет стоимость *входящих* интерфейсов на маршруте.

В табл. 8.4 приведены три маршрута, представленные на рис. 8.15, а также их суммарная стоимость. Таблица демонстрирует, что оптимальный маршрут от маршрутизатора R1 к сети 172.16.3.0/24 проходит через маршрутизатор R5.

Таблица 8.4. Сравнение трех альтернативных маршрутов от маршрутизатора R1 к сети 172.16.3.0/24

Маршрут	Место на рис. 8.15	Общая стоимость
R1–R7–R8	Слева	10 + 180 + 10 = 200
R1–R5–R6–R8	Посередине	20 + 30 + 40 + 10 = 100
R1–R2–R3–R4–R8	Справа	30 + 60 + 20 + 5 + 10 = 125

В результате анализа алгоритма SPF базы LSDB маршрутизатора R1 добавляет в таблицу маршрутизации маршрут к подсети 172.16.3.0/24 через следующий транзитный маршрутизатор R5.

В реальных сетях OSPF инженер может выполнить тот же процесс, зная стоимости OSPF каждого интерфейса. Имея схему сети, инженер может исследовать все маршруты, сложить их стоимости и предсказать метрику для каждого маршрута.

ВНИМАНИЕ!

Протокол OSPF вычисляет стоимость, используя разные процессы в зависимости от проекта области. Пример на рис. 8.15 демонстрирует логику OSPF, наилучшим образом подходящую проекту одиночной области.

Административное расстояние

На основании метрик протокол OSPF вполне может выбрать наилучший маршрут к каждой подсети, что уже обсуждалось в этой главе выше. Но операционная система IOS должна также быть в состоянии выбрать наилучший маршрут к подсети, когда маршрутизатор узнает о маршрутах из других источников. Чтобы сделать такой выбор, маршрутизаторы используют концепцию *административного расстояния* (Administrative Distance — AD).

Сначала рассмотрим общий случай, когда все маршрутизаторы используют только протокол OSPF как единый протокол маршрутизации IPv4. Маршрутизатор изучает не только маршруты OSPF, но и подключенные маршруты. На нем также могут быть введены команды `ip route`, задающие статические маршруты IPv4. Маршрутизатор вполне может знать подключенный и статический маршруты, а также маршрут OSPF к той же подсети. Какой из них маршрутизатор выберет для использования?

Каждый раз, когда маршрутизатор должен выбрать между подключенным, статическим и маршрутом OSPF, он стандартно использует подключенный маршрут. Почему? Хоть это и имеет смысл, фактически маршрутизатор выбирает подключенный маршрут из-за его более низкого (лучшего) административного расстояния (0). Административное расстояние статических маршрутов стандартно составляет 1, а маршрутов OSPF — 110.

Но в некоторых случаях компания должна использовать несколько протоколов маршрутизации. Например, если две компании объединяют свои сети, чтобы обмениваться информацией, они должны обмениваться также и информацией о маршрутизации. Если одна компания использует протокол OSPF, а другая EIGRP, то по крайней мере на одном маршрутизаторе должен использоваться и протокол OSPF, и EIGRP. Такой маршрутизатор может получать маршруты по протоколу OSPF, а анонсировать их по протоколу EIGRP, и наоборот. Это процесс *перераспределения маршрутов* (route redistribution).

В зависимости от топологии сети, некий маршрутизатор может получить маршрут к подсети и по протоколу OSPF, и по протоколу EIGRP. В данном случае, поскольку метрика каждого протокола маршрутизации основана на разной информации, операционная система IOS не может их сравнить. В данном случае она снова выбирает наилучший маршрут на основании административного расстояния.

Значения административного расстояния настраиваются на одном маршрутизаторе и не передаются на другой. Различные источники информации о маршрутизации наряду со стандартными значениями административного расстояния приведены в табл. 8.5.

Ключевая тема

Таблица 8.5. Стандартные значения административного расстояния

Тип маршрута	Значение административного расстояния
Подключенный	0
Статический	1
BGP (внешние маршруты)	20
EIGRP (внутренние маршруты)	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
EIGRP (внешние маршруты)	170
BGP (внутренние маршруты)	200
Непригодный	255

ВНИМАНИЕ!

Команда `show ip route` выводит административное расстояние каждого маршрута как первое из двух чисел в скобках. Второе число в скобках — это метрика.

В таблице приведены стандартные значения административного расстояния, но операционная система IOS может быть настроена так, чтобы изменить значение AD конкретного протокола маршрутизации и даже определенного маршрута. Например, команда `distance 80` в режиме конфигурации OSPF устанавливает для всех изученных по протоколу OSPF маршрутов на этом маршрутизаторе значение AD 80.

Настройка и проверка протокола OSPF

Теперь, когда известна большая часть теории OSPF, рассмотрим, как обеспечить работу протокола OSPF в проекте с многими областями и повлиять на выбор маршрута за счет изменения стоимости интерфейса OSPF. Следующая тема посвящена проверке этих средств, а также некоторых из средств OSPF и LSA, обсуждаемых в первой части главы.

Краткий обзор конфигурации OSPFv2

Тем, кто забыл конфигурацию OSPF, описанную в книге ICND1, имеет смысл уделить время обзору в этой главе. Ниже описана последовательность команд с комментариями. Кроме того, обратите внимание, что в следующем примере настройки используются те же команды.

Ключевая тема

Этапы настройки конфигурации OSPF из книги по ICND1

Этап 1 Перейдите в режим конфигурации OSPF для конкретного процесса OSPF, используя глобальную команду `router ospf` *идентификатор_процесса*

Этап 2 Настройка идентификатора маршрутизатора OSPF (необязательно):

A. Введите подкоманду маршрутизатора `router-id` *значение_id*.

B. Задайте IP-адрес на петлевом интерфейсе (выберите самый большой IP-адрес из всех работающих петлевых интерфейсов).

C. Задайте IP-адрес интерфейса (выберите самый высокий IP-адрес из всех работающих не петлевых интерфейсов)

Этап 3 Введите одну или несколько подкоманд маршрутизатора `network` *IP-адрес шаблон_маски* `area` *идентификатор_области* для каждого соответствующего интерфейса с разрешенным протоколом OSPF и присвойте ему номер области

Этап 4 Используя подкоманду интерфейса `passive-interface` *тип номер*, настройте все интерфейсы OSPF как пассивные, если на интерфейсе не могут или не должны быть обнаружены никакие соседи (необязательно)

Из всех этих команд наибольшие затруднения вызывает команда OSPF `network`. Она сравнивает первый параметр с каждым IP-адресом интерфейса локального маршрутизатора, пытаясь найти соответствие. Но вместо того, чтобы сравнивать все номера со всеми IPv4-адресами на интерфейсах, маршрутизатор может сравнивать только подмножество октетов на основании шаблона маски в стиле списка управления доступом (ACL).

Ниже приведен список нескольких команд `network` с описанием соответствующих IP-адресов.

`network 10.1.1.1 0.0.0.0 area 0`. Соответствует интерфейсу только с адресом 10.1.1.1.

`network 10.1.1.0 0.0.0.255 area 0`. Соответствует любому интерфейсу, адрес которого начинается на 10.1.1.

`network 10.0.0.0 0.255.255.255 area 0`. Соответствует любому интерфейсу, адрес которого начинается на 10.

`network 0.0.0.0 255.255.255.255 area 0`. Соответствует любому интерфейсу с любым IP-адресом.

Значение 0 в октете шаблона маски указывает операционной системе IOS сравнивать эти октеты, а значение 255 — игнорировать.

Пример многообластной конфигурации OSPFv2

Прежде чем перейти к многообластной конфигурации, уделим немного времени краткому обзору экзаменационных вопросов по темам OSPF. Откровенно говоря, экзаменационные вопросы по темам OSPF (на момент публикации) относились в основном к настройке протокола OSPF (как OSPFv2, так и OSPFv3) в многообластном проекте. Экзаменационные темы по конфигурации сосредоточены только на одиночной области, в то время как темы поиска и устранения неисправностей могут подразумевать знание и многообластной конфигурации. Хорошая новость: понимая концепции многих областей и конфигурацию одиночной области, разобраться в конфигурации многих областей достаточно просто. Таким образом, в данном разделе описаны детали проекта со многими областями на случай, если они понадобятся на экзамене.

Далее приведен пример конфигурации для проекта OSPF со многими областями на основании проекта с тремя областями, представленного на рис. 8.12. Схема на рис. 8.16 повторяет топологию объединенной сети и идентификаторы подсетей, а на

рис. 8.17 показан проект области. Обратите внимание, что возле каждого интерфейса на рис. 8.16 представлен только последний октет IPv4-адреса каждого маршрутизатора, а не все IPv4-адреса полностью.

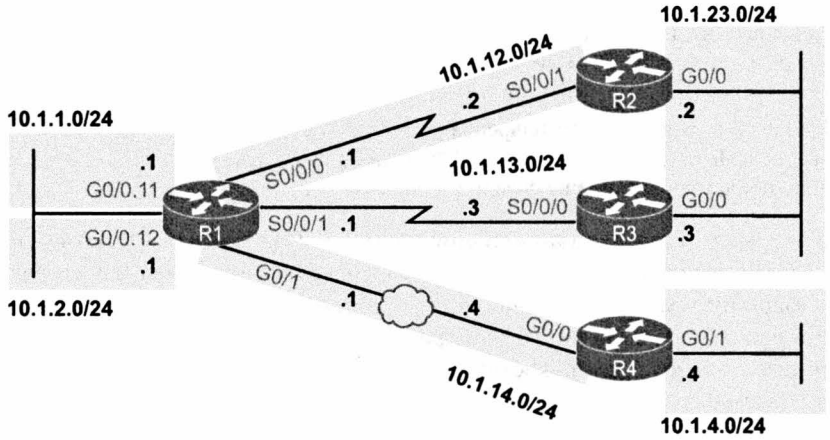


Рис. 8.16. Подсети примера конфигурации OSPF со многими областями

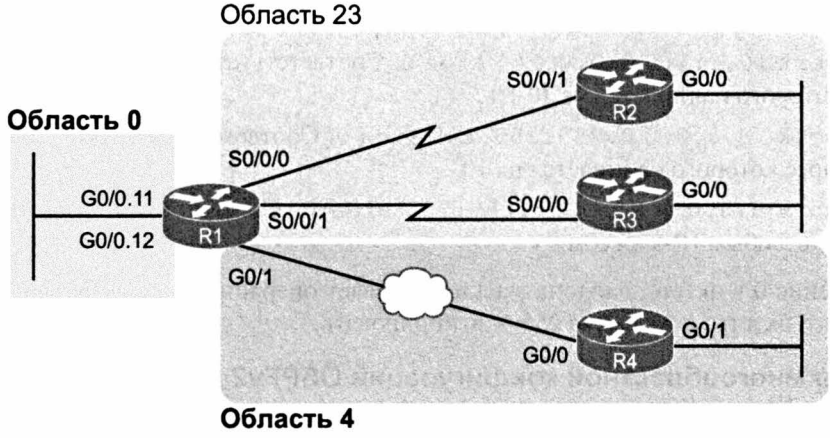


Рис. 8.17. Проект областей примера конфигурации OSPF со многими областями

Конфигурация на четырех маршрутизаторах этого примера используется также и при обзоре конфигурации OSPF на уровне ICND1. Только по причине демонстрации разнообразия параметров конфигурации (и ни по какой другой) здесь показано несколько способов установки идентификатора RID OSPF и несколько разных шаблонов маски в командах OSPF `network`. Кроме того, показано также использование пассивных интерфейсов, когда никакие другие маршрутизаторы OSPF не должны существовать на этих интерфейсах.

Конфигурация одиночной области

Пример 8.1 начинает серию примеров конфигурации с демонстрации настройки конфигурации OSPF и IP-адреса на маршрутизаторе R2. Поскольку маршрутизатор

R2 действует как внутренний маршрутизатор области 23, эта конфигурация относится только к одной области (23). Команда `router-id` непосредственно устанавливает RID маршрутизатора R2 как 2.2.2.2. А поскольку маршрутизатор R2 должен найти соседей на обоих своих интерфейсах, ни один из них не может быть сделан пассивным. Таким образом, в конфигурации маршрутизатора R2 не указаны пассивные интерфейсы.

Пример 8.1. Конфигурация OSPF на маршрутизаторе R2 помещает два интерфейса в область 23

```
interface GigabitEthernet0/0
  ip address 10.1.23.2 255.255.255.0
!
interface serial 0/0/1
 ip address 10.1.12.2 255.255.255.0
!
router ospf 1
  network 10.0.0.0 0.255.255.255 area 23
  router-id 2.2.2.2
```

Пример 8.2 продолжает обзор команд, уже знакомых вам по книге ICND1, демонстрируя конфигурацию для маршрутизаторов R3 и R4. Маршрутизатор R3 помещает оба своих интерфейса в область 23, а его команда `network` устанавливает его RID как 3.3.3.3, используя петлевой интерфейс, в то время как маршрутизатор R2 не может сделать пассивным ни один из своих интерфейсов. Конфигурация маршрутизатора R4 немного отличается, оба его интерфейса помещены в область 4, его RID установлен на основании не петлевого интерфейса (интерфейс G0/0 для RID OSPF 10.1.14.4), а интерфейс G0/1 маршрутизатора R4 сделан пассивным, поскольку никаких других маршрутизаторов OSPF на этом канале связи нет.

Пример 8.2. Конфигурация одиночной области OSPF на маршрутизаторах R3 и R4

```
! Сначала на R3
interface gigabitEthernet0/0
  ip address 10.1.23.3 255.255.255.0
!
interface serial 0/0/0
  ip address 10.1.13.3 255.255.255.0
!
interface loopback 0
  ip address 3.3.3.3 255.255.255.0
!
router ospf 1
  network 10.0.0.0 0.255.255.255 area 23
! ------------------------------------------------------
! Далее на R4
interface GigabitEthernet0/0
  description R4 will use this interface for its OSPF RID
  ip address 10.1.14.4 255.255.255.0
!
interface GigabitEthernet0/1
ip address 10.1.4.4 255.255.255.0
```

```
!
router ospf 1
  network 10.0.0.0 0.255.255.255 area 4
  passive-interface gigabitethernet0/1
```

Конфигурация множества областей

До сих пор многообластная конфигурация фактически не была представлена в примерах. Маршрутизаторы R2, R3 и R4 находятся в одной области, как внутренние маршрутизаторы OSPF. Таким образом, их конфигурация относится только к одной области, и ни один из них не использует многообластную конфигурацию.

Единственный маршрутизатор, у которого есть многообластная конфигурация, — это маршрутизатор ABR, находящийся в основании конфигурации и относящийся к нескольким областям. В этом проекте (см. рис. 8.17) только маршрутизатор R1 действует как маршрутизатор ABR с интерфейсами в трех разных областях. В примере 8.3 показана конфигурация OSPF маршрутизатора R1. Обратите внимание, что в конфигурации нигде не указано, что маршрутизатор R1 является маршрутизатором ABR; вместо этого здесь используются разные команды `network`, помещающие одни интерфейсы в область 0, другие в область 23, а третьи в область 4.

Ключевая тема **Пример 8.3. Многообластная конфигурация OSPF на маршрутизаторе R1**

```
interface GigabitEthernet0/0.11
  encapsulation dot1q 11
  ip address 10.1.1.1 255.255.255.0
!
interface GigabitEthernet0/0.12
  encapsulation dot1q 12
  ip address 10.1.2.1 255.255.255.0
!
interface GigabitEthernet0/1
  ip address 10.1.14.1 255.255.255.0
!
interface serial 0/0/0
  ip address 10.1.12.1 255.255.255.0
!
interface serial 0/0/1
  ip address 10.1.13.1 255.255.255.0
!
router ospf 1
  network 10.1.1.1 0.0.0.0 area 0
  network 10.1.2.1 0.0.0.0 area 0
  network 10.1.12.1 0.0.0.0 area 23
  network 10.1.13.1 0.0.0.0 area 23
  network 10.1.14.1 0.0.0.0 area 4
  router-id 1.1.1.1
  passive-interface gigabitethernet0/0.11
  passive-interface gigabitethernet0/0.12
```

Рассмотрим внимательно выделенные в примере команды `network`. Все пять команд используют шаблон маски 0.0.0.0, поэтому каждая команда требует точного соответствия указанному IP-адресу. Если сравнить эти команды `network` с разны-

ми интерфейсами, то можно заметить, что конфигурация разрешает протокол OSPF для области 0 на субинтерфейсах G0/0.11 и G0/0.12, для области 23 на двух последовательных интерфейсах и области 4 для интерфейса G0/1 маршрутизатора R1.

ВНИМАНИЕ!

В командах OSPF `network` большинства сетей используется шаблон маски 0.0.0.0, требующий точного соответствия каждого IP-адреса интерфейса, как показано в примере 8.3. Такой стиль конфигурации позволяет однозначно указать, какому интерфейсу какая команда `network` соответствует.

И наконец, конфигурация маршрутизатора R1 непосредственно устанавливает свой RID и делает два субинтерфейса LAN пассивными.

Так в чем основное различие между одиночной и многообластной конфигурациями OSPF? Фактически ни в чем. Единственное различие в том, что команды `network` многообластного маршрутизатора ABR используют разные области.

Проверка многообластной конфигурации

Давайте рассмотрим, как проверить некоторые из новых средств протокола OSPF, описанных в этой главе. Для более полной проверки протокола OSPF используйте все команды, предложенные на рис. 8.1 в начале главы. В этом разделе рассматриваются следующие новые темы.

- Проверка расположения интерфейсов маршрутизатора ABR в (нескольких) правильных областях.
- Выявление маршрутизаторов DR и BDR на каналах связи множественного доступа.
- Проверка правильности количества анонсов LSA различных типов в каждой области.
- Проверка маршрутов OSPF.

Проверка расположения интерфейсов маршрутизатора ABR

Проще всего сделать ошибку в многообластной конфигурации — это поместить интерфейс в неправильную область OSPF. Область OSPF упоминают несколько команд. Команда `show ip protocols` в основном повторяет команду конфигурации OSPF `network`, косвенно идентифицирующую интерфейсы и области. Кроме того, команды `show ip ospf interface` и `show ip ospf interface brief` непосредственно представляют область, заданную для интерфейса. Более краткая версия этих команд приведена в примере 8.4.

Пример 8.4. Вывод интерфейсов с поддержкой протокола OSPF и соответствующих областей OSPF

```
R1# show ip ospf interface brief
Interface  PID   Area    IP Address/Mask    Cost  State  Nbrs F/C
Gi0/0.12   1     0       10.1.2.1/24        1     DR     0/0
Gi0/0.11   1     0       10.1.1.1/24        1     DR     0/0
Gi0/1      1     4       10.1.14.1/24       1     BDR    1/1
```

```
Se0/0/1     1     23     10.1.13.1/24      64     P2P     1/1
Se0/0/0     1     23     10.1.12.1/24      64     P2P     1/1
```

Интерфейс в выводе указан в столбце `Interface`, а соответствующая ему область указана в столбце `Area`. Кроме того, представленная в этом примере информация подтверждает конфигурацию, приведенную на рис. 8.16 и 8.17.

Выявление маршрутизаторов DR и BDR

Маршрутизаторы DR и BDR в некотором роде идентифицируют также команды `show`. Фактически вывод команды `show ip ospf interface brief`, приведенный в примере 8.4, отображает состояние локального маршрутизатора в столбце `State`, свидетельствуя о том, что маршрутизатор R1 является маршрутизатором DR на двух субинтерфейсах и маршрутизатором BDR на его интерфейсе G0/1.

В примере 8.5 приведены два других способа выявления маршрутизаторов DR и BDR. Команда `show ip ospf interface` выводит подробные параметры OSPF по каждому интерфейсу, включая RID и адрес интерфейса маршрутизаторов DR и BDR. В то же время команда `show ip ospf neighbor` выводит краткую информацию о роли DR или BDR соседа; о роли локального маршрутизатора эта команда не говорит ничего. В примере 8.5 показаны обе команды.

Пример 8.5. Обнаружение маршрутизаторов DR и BDR

```
R4# show ip ospf interface gigabitEthernet 0/0
GigabitEthernet0/0 is up, line protocol is up
  Internet Address 10.1.14.4/24, Area 4, Attached via Network Statement
  Process ID 1, Router ID 10.1.14.4, Network Type BROADCAST, Cost: 1
  Topology-MTID  Cost  Disabled  Shutdown  Topology Name
      0           1       no        no          Base
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 10.1.14.4, Interface address 10.1.14.4
  Backup Designated router (ID) 1.1.1.1, Interface address 10.1.14.1
!
! Строки опущены для краткости
R4# show ip ospf neighbor

Neighbor ID  Pri  State      Dead Time  Address     Interface
1.1.1.1      1    FULL/BDR   00:00:33   10.1.14.1   GigabitEthernet0/0
```

В первую очередь рассмотрите выделенные строки вывода команды `show ip ospf interface`. Она указывает маршрутизатор DR по его RID 10.1.14.4, что соответствует маршрутизатору R4, а также маршрутизатор BDR как 1.1.1.1, что соответствует маршрутизатору R1. (Напомним, что хотя ранее на концептуальных рисунках маршрутизатор R4 был показан с RID 4.4.4.4, в примере 8.2 он имеет RID 10.1.14.4. Здесь на маршрутизаторе R4 не использовались команда конфигурации `router-id` и петлевой интерфейс.)

В конце примера представлена команда `show ip ospf neighbor` на маршрутизаторе R4, указывающая в столбце `Neighbor` маршрутизатор R4 с единственным соседом с RID 1.1.1.1 (R1). Команда демонстрирует на маршрутизаторе R4 концепцию состояния соседа на примере маршрутизатора R1 (1.1.1.1) с текущим состояни-

ем FULL/BDR. Состояние FULL означает, что маршрутизатор R4 полностью обменялся базами LSDB с маршрутизатором R1. Часть BDR означает, что сосед (R1) действует как маршрутизатор BDR, с учетом, что маршрутизатор R4 (единственный другой маршрутизатор на этом канале связи) действует как маршрутизатор DR.

Проверка правильности количества анонсов LSA

Выше, в разделе "Анонсы состояния канала", подробно обсуждались анонсы LSA типа 1, 2 и 3. В примере многообластной конфигурации используется тот же проект области, что и в прежних примерах анонсов LSA для многих областей, поэтому быстрая проверка баз LSDB OSPF должна подтвердить концепции, обсуждаемые ранее в главе.

Как показано на рис. 8.14, в базе LSDB для области 4 должно быть два анонса router LSA, один анонс network LSA и пять анонсов summary LSA. Введенная на маршрутизаторе R4 команда `show ip ospf database` (пример 8.6) демонстрирует представление базы LSDB маршрутизатора R4 для области 4.

Пример 8.6. Проверка количества и типов анонсов LSA в области 4

```
R4# show ip ospf database

          OSPF Router with ID (10.1.14.4) (Process ID 1)

                Router Link States (Area 4)

Link ID     ADV Router  Age   Seq#        Checksum  Link count
1.1.1.1     1.1.1.1     1252  0x80000015  0x00AE30  1
10.1.14.4   10.1.14.4   1453  0x80000015  0x00A2E7  2

                Net Link States (Area 4)

Link ID     ADV Router  Age   Seq#        Checksum
10.1.14.4   10.1.14.4   1453  0x80000014  0x007259

                Summary Net Link States (Area 4)

Link ID     ADV Router  Age   Seq#        Checksum
10.1.1.0    1.1.1.1     1493  0x80000014  0x00B563
10.1.2.0    1.1.1.1     1493  0x80000014  0x00AA6D
10.1.12.0   1.1.1.1     1493  0x80000014  0x00B41A
10.1.13.0   1.1.1.1     1493  0x80000014  0x00A924
10.1.23.0   1.1.1.1     1493  0x80000014  0x00457D
```

В этом примере выделены три строки заголовка для трех типов LSA, а в области анонса router LSA выделены также идентификаторы канала связи для анонсов router LSA. Выделенные идентификаторы относятся к двум анонсам router LSA: анонсу router LSA для маршрутизатора R1 (RID 1.1.1.1) и для маршрутизатора R4 (RID 10.1.14.4). Если посмотреть в разделе Net (network) LSA области, то можно найти один анонс LSA с идентификатором 10.1.14.4. И наконец, в последнем разделе показано пять анонсов summary LSA в области 4.

ВНИМАНИЕ!

Термины *таблица соседних устройств* (neighbor table), *таблица топологии* (topology table) и *таблица маршрутизации* (routing table) описывают три ключевых списка протокола OSPFv2. Таблица соседних устройств содержит список соседей, а таблица топологии — топологическую базу данных (см. пример 8.6).

Проверка маршрутов OSPF

И наконец, вся эта теория OSPF и все команды `show` не имеют значения, если маршрутизаторы не изучают маршруты IPv4. Чтобы проверить маршруты, в примере 8.7 приведена таблица маршрутизации IPv4 маршрутизатора R4.

Пример 8.7. Проверка маршрутов OSPF на маршрутизаторе R4

```
R4# show ip route
Codes: L - local, 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, H - NHRP, l - LISP
       + - replicated route, % - next hop override

     10.0.0.0/8 is variably subnetted, 9 subnets, 2 masks
O       IA 10.1.1.0/24 [110/2] via 10.1.14.1, 11:04:43, GigabitEthernet0/0
O       IA 10.1.2.0/24 [110/2] via 10.1.14.1, 11:04:43, GigabitEthernet0/0
C       10.1.4.0/24 is directly connected, GigabitEthernet0/1
L       10.1.4.4/32 is directly connected, GigabitEthernet0/1
O       IA 10.1.12.0/24 [110/65] via 10.1.14.1, 11:04:43, GigabitEthernet0/0
O       IA 10.1.13.0/24 [110/65] via 10.1.14.1, 11:04:43, GigabitEthernet0/0
C       10.1.14.0/24 is directly connected, GigabitEthernet0/0
L       10.1.14.4/32 is directly connected, GigabitEthernet0/0
O       IA 10.1.23.0/24 [110/66] via 10.1.14.1, 11:04:43, GigabitEthernet0/0
```

В этом примере приведено несколько новых кодов, особенно интересных с точки зрения OSPF. Как обычно, одиночный символ слева указывает источник маршрута (O означает OSPF). Кроме того, операционная система IOS отмечает все межобластные маршруты кодом IA. (В примере нет внутриобластных маршрутов OSPF, но перед ними просто отсутствовал бы код IA.) Обратите также внимание на то, что у маршрутизатора R4 в этом примере есть маршруты ко всем семи подсетям: два подключенных маршрута и пять межобластных маршрутов OSPF.

Метрики OSPF (стоимость)

Выше, в разделе "Вычисление алгоритмом SPF наилучших маршрутов", обсуждалось, как алгоритм SPF вычисляет наилучший маршрут к каждой подсети на основании метрик. Маршрутизаторы OSPF могут влиять на этот выбор, изменяя стоимости некоторых или всех интерфейсов OSPF.

Маршрутизаторы Cisco позволяют изменять стоимость интерфейса OSPF двумя способами. Стоимость можно установить непосредственно с помощью подкоманды

интерфейса `ip ospf cost x`, а можно позволить операционной системе IOS самой выбрать стандартную стоимость на основании формулы, изменив ее входные данные. Второй случай требует немного больше внимания, поэтому именно он и является основной темой следующего раздела.

Установка стоимости на основании ширины полосы пропускания интерфейса

Фактически стандартные значения стоимости OSPF способны немного запутать, причем по нескольким причинам. Во избежание потенциальных недоразумений этот раздел начинается с нескольких примеров.

Для вычисления стоимости интерфейса OSPF операционная система IOS использует формулу, приведенную ниже. Ширина полосы пропускания интерфейса находится в знаменателе, а ширина полосы пропускания в числителе:

исходная_полоса_пропускания / полоса_пропускания_интерфейса

По этой формуле, чем выше *полоса пропускания интерфейса* (interface bandwidth), тем лучше. Чем выше (быстрее) полоса пропускания интерфейса, тем ниже вычисляемая стоимость OSPF для интерфейса. Чем ниже стоимость интерфейса, тем ниже метрика для маршрута и тем более вероятно использование этого интерфейса в маршруте, выбранном алгоритмом SPF.

Теперь — примеры. Предположим, что стандартная *исходная полоса пропускания* (reference bandwidth) установлена в 100 000 Кбит/с. Стандартные полосы пропускания последовательного интерфейса, интерфейса Ethernet и Fast Ethernet составляют соответственно 1544 Кбит/с, 10 000 Кбит/с (10 Мбит/с) и 100 000 Кит/с (100 Мбит/с), как свидетельствует вывод команды `show interfaces`. Результаты вычисления стоимости OSPF операционной системой IOS для некоторых интерфейсов приведены в табл. 8.6.

Таблица 8.6. Вычисление стоимости OSPF для стандартных полос пропускания

Интерфейс	Стандартная полоса пропускания интерфейса	Формула (Кбит/с)	Стоимость OSPF
Последовательный	1544 Кбит/с	100 000/1544	64
Ethernet	10,000 Кбит/с	100 000/10 000	10
Fast Ethernet	100,000 Кбит/с	100 000/100 000	1

Чтобы изменить стоимость OSPF на интерфейсах, инженеру достаточно ввести подкоманду интерфейса `bandwidth` *скорость*, устанавливающую ширину полосы пропускания на интерфейсе. Это не изменит скорость передачи на уровне 1; значение будет использовано в других целях, включая вычисление метрики протокола маршрутизации. Например, если ввести команду `bandwidth 10000` для последовательного интерфейса при стандартной исходной полосе пропускания, то стоимость OSPF последовательного интерфейса будет вычислена как 100 000/10 000=10.

В примере 8.8 приведены параметры стоимости интерфейсов OSPF на маршрутизаторе R1, вычисленные на основании стандартной исходной полосы пропускания и стандартной полосы пропускания интерфейса.

Пример 8.8. Проверка стоимости интерфейсов OSPF

```
R1# show ip ospf interface brief
Interface  PID   Area   IP Address/Mask   Cost   State   Nbrs F/C
Gi0/0.12   1     0      10.1.2.1/24       1      DR      0/0
Gi0/0.11   1     0      10.1.1.1/24       1      DR      0/0
Gi0/1      1     4      10.1.14.1/24      1      BDR     1/1
Se0/0/1    1     23     10.1.13.1/24      64     P2P     1/1
Se0/0/0    1     23     10.1.12.1/24      64     P2P     1/1
```

Если результат вычисления метрики окажется дробным, он округляется в меньшую сторону до самого близкого целого числа. В примере стоимость интерфейса S0/0/0 представлена как 64. Но при стандартной полосе пропускания последовательного интерфейса 1,544 Мбит/с и исходной полосе пропускания 100 Мбит/с стоимость вычисляется как 100/1,544, что дает 64,7668394. Результат округляется в меньшую сторону до 64.

Потребность в более высокой исходной полосе пропускания

Стандартные значения прекрасно работали, пока самый быстрый канал связи в сети не достигал 100 Мбит/с. Стандартная исходная полоса пропускания устанавливается в 100, что означает 100 Мбит/с, или 100 000 Кбит/с. В результате со стандартными настройками более быстрые интерфейсы маршрутизатора имеют одинаковую стоимость OSPF, как показано в табл. 8.7, поскольку самое низкое допустимое значение стоимости OSPF составляет 1.

Таблица 8.7. Более быстрые интерфейсы с равной стоимостью OSPF

Интерфейс	Стандартная полоса пропускания интерфейса	Формула (Кбит/с)	Стоимость OSPF
Fast Ethernet	100 000 Кбит/с	100 000/100 000	1
Gigabit Ethernet	1 000 000 Кбит/с	100 000/1 000 000	1
10 Gigabit Ethernet	10 000 000 Кбит/с	100 000/10 000 000	1
100 Gigabit Ethernet	100 000 000 Кбит/с	100 000/100 000 000	1

Чтобы избежать этой проблемы и повлиять на результат вычисления стоимости, можно изменить исходную полосу пропускания подкомандой режима OSPF `auto-cost reference-bandwidth` *скорость*, которая устанавливает значение скорости в мегабитах в секунду (Мбит/с). Для устранения представленной в табл. 8.7 проблемы установите значение исходной полосы пропускания равным скорости самого быстрого канала в сети. Например, команда `auto-cost reference-bandwidth 10000` приспосабливает сеть к скорости канала в 10 Гбит/с.

ВНИМАНИЕ!

Компания Cisco рекомендует указывать исходную полосу пропускания на всех маршрутизаторах OSPF в сети.

Для удобства изучения ниже приведены правила установки на маршрутизаторе стоимости интерфейса OSPF:



Как операционная система IOS определяет стоимость интерфейса OSPF

1. Стоимость может быть установлена явно подкомандой интерфейса `ip ospf cost` *x* со значением от 1 до 65 535 включительно.
2. Полосу пропускания интерфейса можно изменить командой `bandwidth` *скорость*, где скоростью задается числом в Кбит/с.
3. Исходную полосу пропускания можно изменить подкомандой OSPF маршрутизатора `auto-cost reference-bandwidth` *исходная_полоса_пропускания*, где значение задается числом в Мбит/с.

Балансировка нагрузки в протоколе OSPF

Когда в протоколе маршрутизации OSPF с помощью алгоритма SPF рассчитываются маршруты к какой-либо подсети и найден маршрут с наименьшей метрикой, такой маршрут помещается в таблицу маршрутизации. Тем не менее, если обнаружено несколько маршрутов с одной и той же метрикой, то все они могут быть помещены в таблицу маршрутизации. При стандартных настройках четыре маршрута с одной метрикой устанавливаются в таблицу маршрутизации, а всего может быть установлено до 16 маршрутов, в зависимости от того, какое значение указано в команде `maximum-paths` *число*. Например, если в сети есть 6 одинаковых маршрутов и инженер хочет, чтобы все они использовались для передачи данных одновременно, он может ввести команду `maximum-paths 6` после команды `router ospf`.

Если в таблице маршрутизации есть несколько одинаковых маршрутов, устройство выполняет балансировку нагрузки по ним. Один из методов балансировки — пакетный. Например, если у маршрутизатора есть три одинаковых маршрута OSPF к одной подсети, то первый пакет будет отправлен по одному маршруту, второй — по следующему, третий — по следующему, а четвертый — опять по первому и т.д. Второй метод, который обычно включен в современных маршрутизаторах, — потоковый. В нем потоки пакетов балансируют между разными каналами, например, поток пакетов к определенному IP-адресу получателя идет по одному каналу, к другому — по следующему и т.д.

Обзор

Резюме

- OSPF — это протокол состояния канала.
- Маршрутизатор использует идентификатор RID OSPF во многих целях, в том числе он играет важную роль в большинстве внутренних процессов протокола OSPFv2.
- Большинство инженеров составляют план нумерации RID, или создают список маршрутизаторов с их идентификаторами RID, или вырабатывают простой способ предсказания RID каждого маршрутизатора.
- Если два маршрутизатора не станут соседями, они не будут обмениваться информацией.
- По достижении состояния двустороннего канала два маршрутизатора могут обмениваться базами данных о состоянии каналов.
- Как только соседи достигают состояния полной синхронизации, они завершают все начальные работы по обмену информацией OSPF.
- После выбора маршрутизатора DR все остальные маршрутизаторы обмениваются данными о состоянии каналов только с ним, но не друг с другом.
- Протокол OSPF использует концепцию BDR (резервного выделенного маршрутизатора), поскольку выделенный маршрутизатор (DR) столь важен для процесса обмена базами данных.
- Для многих систем вполне подходит проект с одиночной областью OSPF.
- Анонсы LSA содержат очень полезную информацию, но не конкретную информацию, которую маршрутизатор должен добавить в свою таблицу маршрутизации IPv4.
- Каждый раз, когда маршрутизатор должен выбрать между подключенным, статическим и маршрутом OSPF, он стандартно использует подключенный маршрут.
- При равенстве метрик для нескольких маршрутов к той же подсети маршрутизатор может поместить в таблицу маршрутизации несколько маршрутов с равной стоимостью.

Контрольные вопросы

Ответьте на эти вопросы. Ответы можно найти на последней странице главы. Полное объяснение ответов приведено в приложении B на веб-сайте.

1. В базе LSDB области 51 протокола OSPFv2 внутреннего маршрутизатора области R1 есть анонсы LSA типа 1, типа 2 и типа 3. Какой из этих типов анонсов LSA маршрутизатор R1 не смог бы создать в области 51?

   А) Тип 1.

   Б) Тип 2.

В) Тип 3.

Г) Маршрутизатор R1 смог бы создать все три типа.

2. Сеть компании использует 15 маршрутизаторов, 40 подсетей и протокол OSPFv2. Что из следующего считается преимуществом использования проекта одиночной области по сравнению с проектом нескольких областей?

   А) Сокращены дополнительные затраты по обработке на большинстве маршрутизаторов.

   Б) Изменение состояния одного канала связи не потребует запуска алгоритма SPF на всех остальных маршрутизаторах.

   В) Проще планирование и обслуживание.

   Г) Разрешает суммирование маршрутов, что сокращает размер таблиц маршрутизации IP.

3. Какое из следующих состояний соседа OSPF ожидается по завершении обмена топологической информацией между двумя соседями OSPF?

   А) 2-way.

   Б) Full.

   В) Up/up.

   Г) Final.

4. Маршрутизаторы R1, R2 и R3 являются внутренними маршрутизаторами областей 1, 2 и 3 соответственно. Маршрутизатор R4 является маршрутизатором ABR, соединенным с магистральной областью (0) и с областями 1, 2 и 3. Какой из следующих ответов описывает конфигурацию на маршрутизаторе R4, отличающемся от других трех маршрутизаторов?

   А) Подкоманда маршрутизатора `abr enable`.

   Б) Подкоманда маршрутизатора `network` относится к одиночной не магистральной области.

   В) Подкоманда маршрутизатора `network` относится к нескольким областям, включая магистральную.

   Г) У маршрутизатора есть интерфейс в области 0, тогда как интерфейс соседа OSPF находится в другой области.

5. Какой из следующих параметров конфигурации на маршрутизаторе не влияет на маршрут, выбираемый маршрутизатором IPv4 для добавления в таблицу маршрутизации IPv4 при использовании протокола OSPFv2?

   А) `auto-cost reference-bandwidth`.

   Б) `Delay`.

   В) `Bandwidth`.

   Г) `ip ospf cost`.

6. Инженер подключился к маршрутизатору R1 и ввел команду `show ip ospf neighbor`. Состоянием соседа 2.2.2.2 оказалось Full/BDR. Что означает часть BDR?

   А) Маршрутизатор R1 является граничным маршрутизатором области (Area Border Router).

Б) Маршрутизатор R1 является резервным выделенным маршрутизатором (Backup Designated Router).

В) Маршрутизатор 2.2.2.2 является граничным маршрутизатором области.

Г) Маршрутизатор 2.2.2.2 является резервным выделенным маршрутизатором.

Ключевые темы

Повторите все ключевые темы данной главы, отмеченные пиктограммой "Ключевая тема". Ключевые темы и соответствующие им страницы перечислены в табл. 8.8.

Таблица 8.8. Ключевые темы главы 8

Элемент	Описание	Страница
Рис. 8.1	Пакеты Hello состояния канала	279
Список	Правила выбора идентификатора маршрутизатора	280
Табл. 8.1	Стабильные состояния соседей OSPF и их значения	286
Список	Правила проекта областей OSPF	287
Рис. 8.7	Проект с тремя областями OSPF и маршрутизаторами D1 и D2 в качестве ABR	288
Табл. 8.2	Терминология проекта OSPF	288
Список	Преимущества многообластных проектов в больших объединенных сетях	290
Табл. 8.3	Три типа анонсов LSA протокола OSPFv2, используемых в многообластных проектах OSPF	291
Определение	Как протокол OSPF вычисляет стоимость маршрута	295
Рис. 8.15	Дерево SPF для выбора маршрута от маршрутизатора R1 к сети 172.16.3.0/24	296
Табл. 8.5	Стандартные значения административного расстояния	298
Список	Этапы настройки конфигурации OSPF из книги по ICND1	298
Прим. 8.3	Многообластная конфигурация OSPF на маршрутизаторе R1	302
Список	Как операционная система IOS определяет стоимость интерфейса OSPF	309

Заполните таблицы и списки по памяти

Распечатайте приложение Г с веб-сайта или его раздел, относящийся к этой главе, и заполните таблицы и списки по памяти. В приложении Д приведены заполненные таблицы и списки для самоконтроля.

Ключевые термины

После первого прочтения главы попытайтесь дать определения следующим ключевым терминам. Но не расстраивайтесь, если не все получится сразу, в главе 22 описано, как использовать эти термины на завершающем этапе подготовки к экзамену.

двусторонний канал (2-way state), состояние полной синхронизации (full state), граничный маршрутизатор области (Area Border Router — ABR), выделенный маршрутизатор (Designated Router — DR), резервный выделенный маршрутизатор (Backup Designated Router — BDR), состояние с полностью согласованной тополо-

гией (fully adjacent), интервал Hello (Hello interval), интервал Dead (Dead interval), анонс состояния канала, или анонс LSA (link-state advertisement), обновление состояния канала (link-state update), соседний маршрутизатор (neighbor), идентификатор маршрутизатора (Router ID — RID), топологическая база данных (topology database), алгоритм первого кратчайшего маршрута (Shortest Path First — SPF), внутренний маршрутизатор (internal router), анонс network LSA (network LSA), анонс router LSA (router LSA), анонс summary LSA (summary LSA), опорная область (backbone area)

Таблицы команд

Хоть и не обязательно заучивать информацию из таблиц данного раздела, ниже приведен список команд конфигурации и пользовательских команд главы. Фактически команды стоит запомнить, чтобы лучше понять содержимое главы и выполнить задания по подготовке к экзамену. Чтобы проверить, насколько хорошо вы запомнили команды, закройте левую сторону таблицы листом бумаги, читайте описания с правой стороны и пытайтесь вспомнить команду.

Таблица 8.9. Конфигурационные команды главы 8

Команда	Описание
`router ospf` *`идентификатор_процесса`*	Переводит интерфейс командной строки в режим конфигурации протокола OSPF с указанным номером процесса
`network` *`IP-адрес шаблон_маски`* `area` *`идентификатор_области`*	Подкоманда маршрутизатора, которая разрешает протокол OSPF на интерфейсах, соответствующих комбинации адрес/шаблон, а также задает область OSPF
`ip ospf cost` *`цена_интерфейса`*	Подкоманда интерфейса, задающая связанную с интерфейсом стоимость OSPF
`bandwidth` *`ширина_полосы_пропускания`*	Подкоманда интерфейса, непосредственно устанавливающая ширину полосы пропускания интерфейса (Кбит/с)
`auto-cost reference-bandwidth` *`значение`*	Команда режима конфигурирования протокола маршрутизации, задающая исходную полосу пропускания, используемую для расчетов стоимости интерфейсов в протоколе OSPF
`router-id` *`идентификатор`*	Команда OSPF, статически устанавливающая идентификатор маршрутизатора
`interface loopback` *`номер`*	Глобальная команда, создающая петлевой интерфейс и переводящая в режим конфигурации интерфейса для данного интерфейса
`maximum-paths` *`количество_путей`*	Подкоманда маршрутизатора, определяющая максимальное количество маршрутов с равной стоимостью, которые могут быть добавлены в таблицу маршрутизации
`passive-interface` *`тип номер`*	Подкоманда маршрутизатора, делающая интерфейс пассивным интерфейсом OSPF, а значит, процесс OSPF не будет формировать соседские отношения с соседними маршрутизаторами, доступными на данном интерфейсе

Окончание табл. 8.9

Команда	Описание
`passive-interface default`	Подкоманда OSPF, изменяющая стандартное значение OSPF для интерфейсов с пассивного на активный
`no passive-interface` *тип номер*	Подкоманда OSPF, переводящая интерфейс или субинтерфейс в активное состояние OSPF

Таблица 8.10. Команды EXEC главы 8

Команда	Описание
`show ip ospf`	Выводит информацию о выполняющемся на маршрутизаторе процессе OSPF, включая идентификатор маршрутизатора OSPF, области, к которым подключен маршрутизатор, и количество интерфейсов в каждой области
`show ip ospf interface brief`	Выводит интерфейсы, на которых разрешен протокол OSPF (на основании команды `network`), включая пассивные интерфейсы
`show ip ospf interface` *тип номер*	Выводит длинный список параметров, состояние и счетчики для операции OSPF на всех интерфейсах или на заданном интерфейсе, включая таймеры Hello и Dead
`show ip protocols`	Отображает параметры протокола маршрутизации и текущие значения таймеров
`show ip ospf neighbor` [*тип номер*]	Выводит краткий список соседей (по одной строке на каждого), идентифицированных по идентификатору соседнего маршрутизатора, включая их текущее состояние; вывод можно ограничить соседями на выбранном интерфейсе
`show ip ospf neighbor` *идентификатор_соседа*	Вывод такой же, как у команды `show ip ospf neighbor detail`, но только для заданного соседнего маршрутизатора (по идентификатору соседа)
`show ip ospf database`	Выводит отчет об анонсах LSA в базе данных (по одной строке на анонс LSA). Вывод организован по типам LSA (сначала тип 1, затем тип 2 и т.д.)
`show ip route`	Выводит все маршруты IPv4
`show ip route ospf`	Выводит маршруты в таблице маршрутизации, изученные по протоколу OSPF
`show ip route` *IP-адрес маска*	Выводит подробное описание маршрута для выбранной подсети/маски
`clear ip ospf process`	Возвращает процесс OSPF в исходное состояние, удаляя все соседские отношения, а также вынуждая процесс выбирать RID OSPF

Ответы на контрольные вопросы:

1 В. 2 В. 3 Б. 4 В. 5 Б. 6 Г.

Глава 9

Концепции протокола EIGRP

В настоящей главе подробно рассматривается вторая возможность протокола маршрутизации IPv4 — *расширенный протокол маршрутизации внутреннего шлюза* (Enhanced Interior Gateway Routing Protocol — EIGRP). Этот собственный протокол маршрутизации компании Cisco использует команды конфигурации, очень похожие на открытый протокол поиска первого кратчайшего маршрута (OSPF), но с серьезным отличием, а именно: конфигурация протокола EIGRP не полагается на области. Однако протокол EIGRP не использует логику *состояния канала* (Link-State — LS), вместо нее используется немного улучшенная *дистанционно-векторная* логика (Distance Vector — DV). Таким образом, в этой главе обсуждается довольно немного подробностей о работе протоколов маршрутизации до перехода к конфигурации EIGRP.

Данная глава имеет два главных раздела. В первом рассматриваются подробности работы дистанционно-векторной логики протоколов маршрутизации по сравнению с базовыми характеристиками протокола RIP, а также дополнительные возможности протокола EIGRP. Во втором разделе рассматриваются специфические особенности протокола EIGRP, включая соседские отношения, обмен информацией о маршрутизации и вычисление оптимальных в настоящее время маршрутов к каждой возможной подсети.

В этой главе рассматриваются следующие экзаменационные темы
Технологии маршрутизации IP
Настройка и проверка EIGRP (одиночная область)
Приемлемое расстояние / Возможные преемники / Административное расстояние
Условие применимости
Композиция метрик
Идентификатор маршрутизатора
Автоматический отчет
Выбор пути
Баланс нагрузки
Равномерный
Неравномерный
Пассивный интерфейс
Различия методов маршрутизации и протоколов маршрутизации
Разделение диапазона
Метрика
Следующий транзитный узел

Основные темы

EIGRP и дистанционно-векторные протоколы маршрутизации

За долгую историю протокола IPv4 было разработано множество разных *протоколов маршрутизации внутреннего шлюза* (Interior Gateway Protocol — IGP). Каждый из них чем-то отличался, в основном базовым алгоритмом протокола маршрутизации: по состоянию канала или вектору расстояния. В данном разделе будет показано, что протокол EIGRP до некоторой степени работает как дистанционно-векторный протокол маршрутизации, хотя он и не соответствует полностью ни одной из категорий.

В частности, сначала в этом разделе протокол EIGRP сравнивается с другими протоколами маршрутизации IPv4. Затем рассматриваются базовые концепции дистанционно-векторной логики (DV) на примере протокола RIP. Использование простого протокола RIP для изучения основ позволит сосредоточиться исключительно на концепциях дистанционно-векторной логики. И в завершение будет показано, что протокол EIGRP использует средства дистанционно-векторной логики эффективней, чем протокол RIP.

Введение в протокол EIGRP

Исторически первые протоколы маршрутизации IPv4 использовали дистанционно-векторную логику (DV). Протокол RIP версии 1 (RIP-1) был первым популярным протоколом маршрутизации IP, а собственный *протокол маршрутизации внутреннего шлюза* (Interior Gateway Routing Protocol — IGRP) Cisco появился немного позже (рис. 9.1).

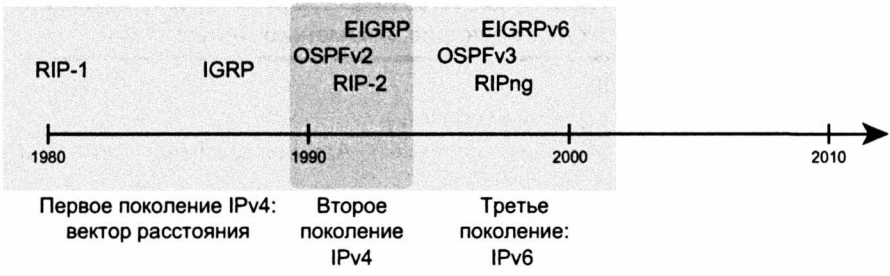


Рис. 9.1. Эволюция протоколов IP IGP

В 1990-х годах коммерческие и технические факторы породили второе поколение лучших протоколов маршрутизации. Первые протоколы, RIP-1 и IGRP, имели ряд технических ограничений, хоть и обладали великолепными возможностями для технологии уровня 1980-х годов. Серьезная мотивация для создания лучших протоколов маршрутизации стала огромным движением протокола TCP/IP в 90-х годах. Многие предприятия перешли с устаревших сетей частных производителей на сети с использованием маршрутизаторов, локальных сетей и протокола TCP/IP. Эти компании нуждались в протоколах маршрутизации лучшей производительности, включая лучшие метрики и лучшую конвергенцию. Все эти факторы привели к появлению следу-

ющего поколения внутренних протоколов маршрутизации IPv4: протокола RIP версии 2 (RIP-2), протокола OSPF версии 2 (OSPFv2) и протокола EIGRP.

ВНИМАНИЕ!

Кстати, в большинстве документов протокол EIGRP упоминается для протокола IPv4 как просто EIGRP, а протокол EIGRP для протокола IPv6 — как EIGRPv6. В данной книге используется то же соглашение. В запросах на комментарии OSPF применяются и иные версии: протокол OSPF версии 2 (OSPFv2) для маршрутов IPv4 и протокол OSPF версии 3 (OSPFv3) для маршрутов IPv6.

В настоящее время протоколы EIGRP и OSPFv2 остаются двумя главными конкурирующими протоколами маршрутизации IPv4, используемыми в современной корпоративной объединенной сети IPv4. Протокол RIP-2 как серьезный конкурент отпал, частично из-за его менее надежной метрики счетчика количества транзитных переходов, а частично из-за более медленной конвергенции. Даже сегодня во многих корпоративных сетях можно найти использующийся протокол маршрутизации EIGRP или OSPFv2.

Таким образом, как сетевому инженеру при столь широком многообразии протоколов маршрутизации IPv4 выбрать используемый протокол маршрутизации? Он должен учесть два ключевых момента о протоколе EIGRP.

Сравнение ключевых моментов протокола EIGRP с другими протоколами маршрутизации

Ключевая тема

- Протокол EIGRP использует надежную метрику на основании ширины полосы пропускания канала связи и задержки канала связи, поэтому маршрутизаторы способны правильно выбрать наилучший маршрут для использования (рис. 9.2).
- Конвергенция протокола EIGRP очень быстра, а значит, при изменении в объединенной сети протокол EIGRP быстро найдет наилучший в настоящее время маршрут.

Например, протокол RIP использует простую метрику — счетчик переходов, означающий количество маршрутизаторов между подсетью получателя и локальным маршрутизатором. Эта метрика позволяет протоколу RIP выбрать кратчайший маршрут (наименьшее количество транзитных участков), даже если более короткий маршрут проходит по медленным каналам связи, что явно не способствует созданию действительно оптимального маршрута. Вычисление метрики EIGRP использует математическую формулу, позволяющую избегать маршрутов с медленными каналами связи, создавая для них более высокие (худшие) метрики. Пример приведен на рис. 9.2.

Традиционно, с момента выпуска протокола EIGRP в 1990-х годах и до 2013 года, наибольшим его недостатком было то, что он оставался собственным протоколом компании Cisco. Поэтому для применения протокола EIGRP Cisco пользователи вынуждены были покупать маршрутизаторы Cisco. Ныне компания Cisco опубликовала протокол EIGRP как документ RFC, поэтому теперь и другие производители могут реализовать его также. В прошлом многие компании использовали протокол OSPF, а не EIGRP, чтобы иметь в дальнейшем возможность покупать и использовать маршру-

тизаторы от других производителей. В будущем можно будет использовать часть маршрутизаторов от Cisco, а часть от других производителей, и все они смогут применять протокол EIGRP.

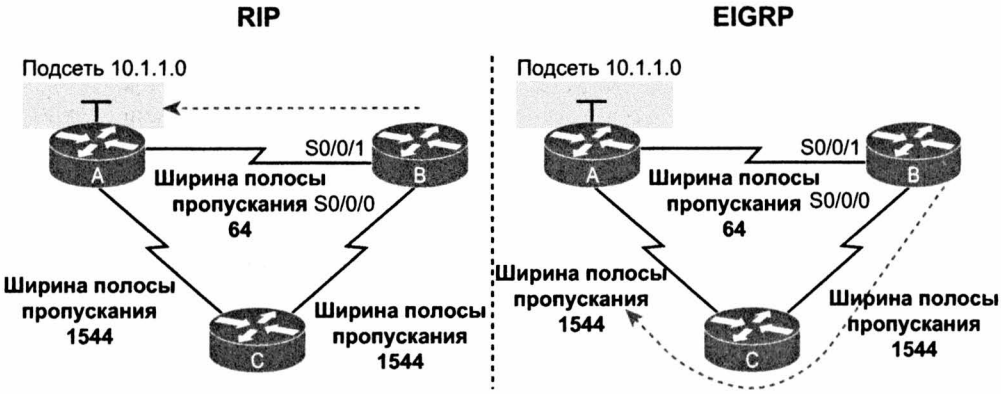


Рис. 9.2. Протокол EIGRP выбирает более длинный, но лучший маршрут к подсети 10.1.1.0

В настоящий момент протоколы EIGRP и OSPFv2 остаются наилучшим выбором для внутренних протоколов маршрутизации IPv4. Оба имеют быструю конвергенцию. Оба используют хорошие метрики, учитывающие скорости канала при выборе маршрута. Реализовать протокол EIGRP довольно просто. Большинство ответственных сетевых инженеров сравнили эти протоколы годы назад, одни из них предпочли протокол OSPFv2, а другие выбрали протокол EIGRP.

В табл. 9.1 для справки и изучения приведено несколько возможностей протоколов OSPFv2, EIGRP и RIP-2. (Обратите внимание: таблица затрагивает еще не обсуждавшиеся темы, например автоматическое суммирование.)

Ключевая тема

Таблица 9.1. Сравнение внутренних протоколов маршрутизации IP

Возможность	RIP-2	EIGRP	OSPF
Бесклассовый, поддерживает маски VLSM	Да	Да	Да
Дистанционно-векторный (DV) или состояния канала (LS)	DV	DV[1]	LS
Первоначально собственный протокол Cisco	Нет	Да	Нет
Стандартная метрика учитывает, по крайней мере частично, ширину полосы пропускания канала связи	Нет	Да	Да
Конвергенция	Медленно	Быстро	Быстро
Требует использования областей	Нет	Нет	Да
Поддерживает суммирование маршрутов вручную	Да	Да	Да
Анонсы маршрутизации передаются на многоадресатный IP-адрес	Да	Да	Да

[1]Протокол EIGRP зачастую относят к протоколам маршрутизации сбалансированного гибридного класса, а не к дистанционно-векторным или состояния канала. В некоторых документах протокол EIGRP упоминается как улучшенный дистанционно-векторный.

Базовые средства дистанционно-векторного протокола маршрутизации

Протокол EIGRP не относится исключительно к категории дистанционно-векторных (DV) протоколов маршрутизации или протоколов маршрутизации с учетом состояния канала (LS), скорее он ближе к дистанционно-векторным протоколам. Далее рассматриваются основы дистанционно-векторных протоколов маршрутизации, к которым относится протокол RIP, и их работа. В частности, в следующих примерах показаны маршруты, выбранные по простой метрике счетчика переходов протокола RIP. Хоть эта возможность и не наилучшая в современных реальных сетях, в учебных целях она намного проще протокола EIGRP.

Концепции дистанции и вектора

Термин *дистанционно-векторный* (distance vector) описывает именно то, что известно маршрутизатору о каждом маршруте. В конце процесса, когда маршрутизатор изучит маршрут к подсети, все маршрутизаторы знают ту же дистанцию (метрику), следующий транзитный маршрутизатор и исходящий интерфейс, используемый для этого маршрута (вектор или направление).

На рис. 9.3 показано представление вектора и дистанции на примере протокола RIP. Здесь представлен поток сообщений RIP, позволяющий маршрутизатору R1 изучить три маршрута IPv4 к подсети X, а именно:

- маршрут с четырьмя транзитными участками через маршрутизатор R2;
- маршрут с тремя транзитными участками через маршрутизатор R5;
- маршрут с двумя транзитными участками через маршрутизатор R7.

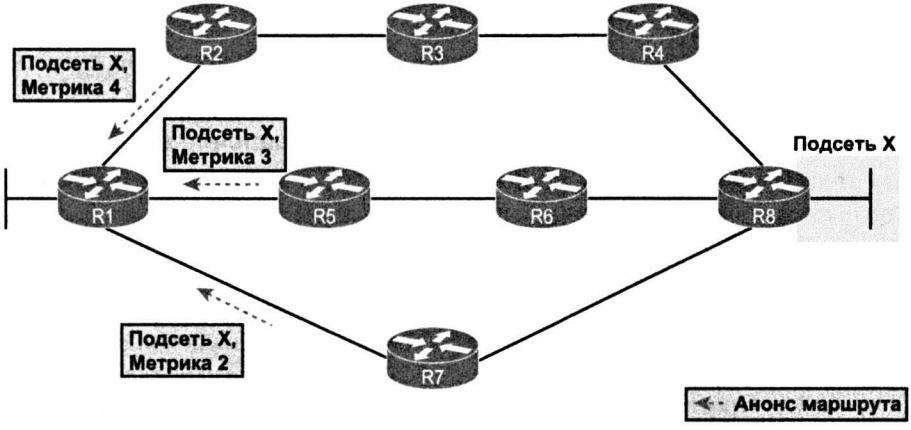


Рис. 9.3. Информация, изученная по дистанционно-векторному протоколу

Дистанционно-векторные протоколы изучают две части информации о возможном маршруте к подсети: дистанцию (метрику) и вектор (маршрутизатор следующего транзитного узла). В данном случае маршрутизатор R1 изучает три маршрута к подсети X. Когда к подсети есть только один маршрут, маршрутизатор выбирает его. Однако при трех возможных маршрутах, как в данном случае, маршрутизатор R1 выбирает маршрут из двух транзитных участков через следующий транзитный маршрутизатор R7, поскольку у этого маршрута самая низкая метрика RIP.

На рис. 9.3 показано, что маршрутизатор R1 изучает маршруты с использованием анонсов RIP, а рис. 9.4 лучше демонстрирует дистанционно-векторную логику маршрутизатора R1. Маршрутизатору R1 известно три маршрута.

Ключевая тема **Составляющие термина дистанционно-векторный**

Дистанция (distance). Метрика возможного маршрута.

Вектор (vector). Направление возможного маршрута на базе следующего транзитного маршрутизатора.

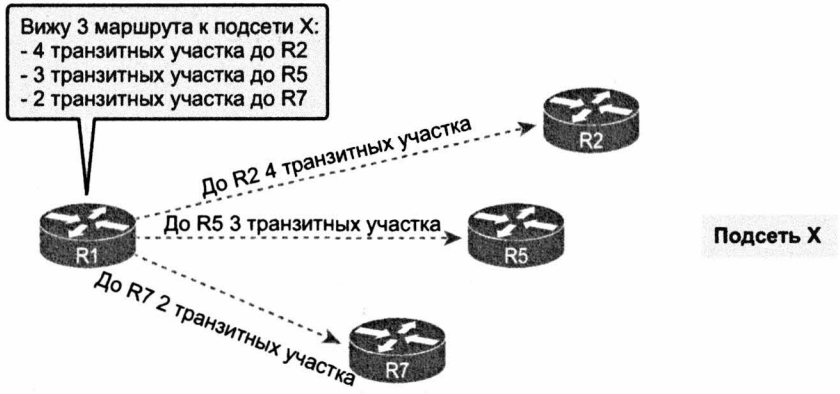


Рис. 9.4. Графическое представление дистанционно-векторной концепции

Обратите внимание, что маршрутизатору R1 неизвестно никакой другой топологической информации об объединенной сети. В отличие от протоколов с учетом состояния канала (LS), дистанционно-векторная (DV) логика протокола RIP понятия не имеет об общей топологии, ей известно только о следующих транзитных маршрутизаторах и метриках.

Сообщения полного обновления маршрутов и разделение диапазона

У дистанционно-векторных протоколов маршрутизации есть несколько функций, требующих обмена сообщениями между соседними маршрутизаторами.

В первую очередь маршрутизаторы должны передавать в сообщении информацию о маршрутизации, чтобы отправляющий маршрутизатор мог анонсировать информацию о маршрутизации соседним маршрутизаторам. Например, на рис. 9.3 маршрутизатор R1 получил маршруты в сообщении RIP. Как упоминалось в главе 8, протокол OSPF называет их сообщениями *обновления состояния канала* (Link-State Update — LSU). Протоколы RIP и EIGRP зачастую называют их *сообщениями об обновлении* (update message).

Кроме того, маршрутизаторы должны контролировать работоспособность каждого соседнего маршрутизатора (работает или нет), и для этого они регулярно обмениваются сообщениями с соседями. Чем быстрей маршрутизатор узнает об отказе соседа, тем быстрее происходит конвергенция и обнаруживаются еще доступные маршруты.

Все протоколы маршрутизации используют некий механизм для контроля состояния соседних маршрутизаторов. Протокол OSPF использует сообщения Hello с относительно коротким интервалом передачи (стандартно через 10 секунд). Протокол

EIGRP использует сообщения Hello и специальный процесс. Но такие простые дистанционно-векторные протоколы, как RIP, не используют специальных сообщений типа Hello, вместо них они используют те же сообщения об обновлении, причем как для анонсирования информации о маршрутизации, так и для выяснения состояния соседнего маршрутизатора. Другими словами, функция анонсирования информации о маршрутизации и функция мониторинга состояния соседа осуществляются теми же сообщениями об обновлении.

Простые дистанционно-векторные протоколы маршрутизации, такие как RIP, периодически (причем относительно часто) передают полный анонс маршрутизации. *Полное обновление маршрутов* (full update) означает, что маршрутизатор анонсирует все свои маршруты, используя одно или несколько сообщений об обновлении RIP, причем независимо от того, изменился маршрут или нет. *Периодически* (periodic) означает, что маршрутизатор посылает сообщения на основании установленного периода времени (у протокола RIP через 30 секунд).

На рис. 9.5 эта концепция представлена на примере объединенной сети с двумя маршрутизаторами, тремя подсетями LAN и одной подсетью WAN. На рисунке показаны полные таблицы маршрутизации обоих маршрутизаторов, а также периодические полные обновления маршрутов, передаваемые каждым маршрутизатором.

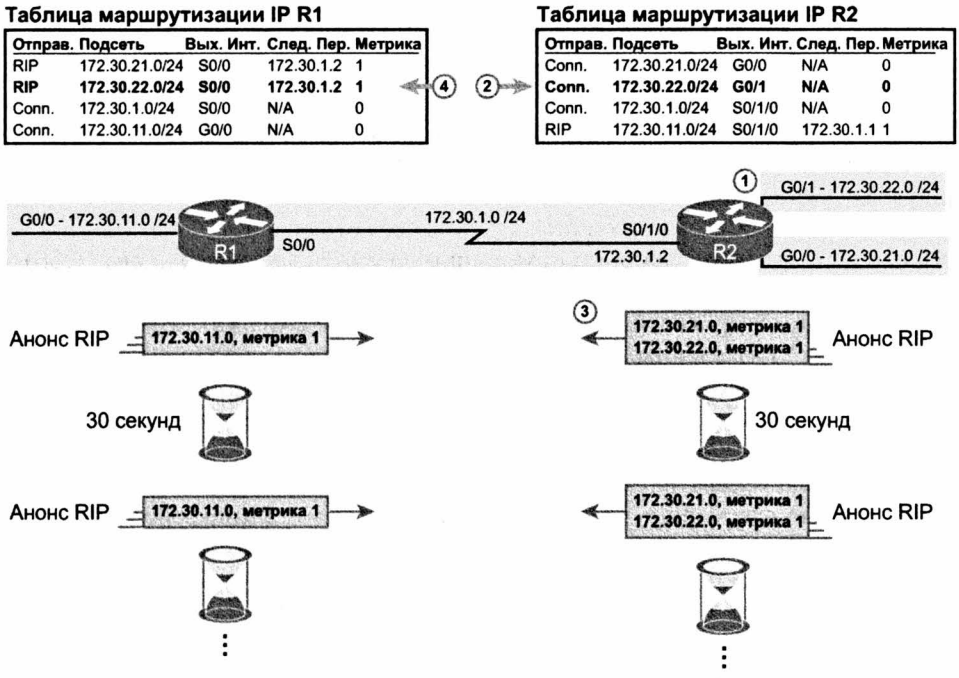


Рис. 9.5. Работа протокола RIP в нормальных условиях: полное обновление маршрутов с разделенным диапазоном

На рисунке представлено много информации, поэтому уделите время подробностям. Рассмотрите, например, как маршрутизатор R1 изучает маршрут к подсети 172.30.22.0/24, подключенной к интерфейсу G0/1 маршрутизатора R2.

1. У интерфейса G0/1 маршрутизатора R2 есть IP-адрес, находящийся в состоянии `up/up`.
2. Маршрутизатор R2 добавляет в свою таблицу маршрутизации подключенный маршрут к подсети 172.30.22.0/24 на интерфейсе G0/1.
3. Маршрутизатор R2 анонсирует маршрутизатору R1 свой маршрут к подсети 172.30.22.0/24 с метрикой 1. Это значит, что для доступа к этой подсети маршрутизатор R1 будет использовать метрику 1 (количество транзитных переходов равно 1).
4. Маршрутизатор R1 добавляет маршрут к подсети 172.30.22.0/24, пометив его как изученный по протоколу RIP с метрикой 1.

Уделим также минуту изученному на этапе 4 маршруту (он выделен полужирным в таблице маршрутизации маршрутизатора R1). Это маршрут к подсети 172.30.22.0/24, полученный от маршрутизатора R2. В нем локальный интерфейс S0/0 маршрутизатора R1 указан как исходящий интерфейс, поскольку маршрутизатор R1 получает обновления на этом интерфейсе. В нем также указан IP-адрес 172.30.1.2 последовательного интерфейса R2 как следующий транзитный переход, поскольку от этого IP-адреса маршрутизатор R1 получил маршрут.

Далее, в нижней части рисунка, представлены сообщения об обновлении RIP, используемые для контроля состояния соседей. Маршрутизаторы повторяют те же сообщения об обновлении через каждые 30 секунд. Обратите внимание, что даже если в этой объединенной сети ничего не меняется годами, то использующие протокол RIP маршрутизаторы все равно будут каждые 30 секунд повторять друг другу ту же информацию о маршрутизации. Почему? Если на протяжении определенного периода времени маршрутизатор не будет получать сообщения об обновлении от соседнего маршрутизатора, то он поймет, что сосед отключен.

И наконец, рисунок демонстрируют пример *разделенного диапазона*. Обратите внимание, что оба маршрутизатора перечисляют в своих таблицах маршрутизации IP все четыре подсети, а сообщения об обновлении RIP содержат не все четыре подсети. Причина? Разделенный диапазон. *Разделение диапазона* (split horizon) — это функция дистанционно-векторных протоколов маршрутизации, позволяющая не анонсировать в передаваемых интерфейсом обновлениях некоторые маршруты, а именно маршруты, использующие данный интерфейс как исходящий.

К не анонсируемым на интерфейсе маршрутам обычно относятся маршруты, изученные в анонсах маршрутизации, полученных на этом интерфейсе.

Концепцию разделения диапазона трудно понять на словах и намного проще на примере. На рис. 9.6 продолжается тот же пример, что и на рис. 9.5, но с большим акцентом на анонсах RIP, передаваемых с интерфейса S0/0 маршрутизатора R1 на маршрутизатор R2. На рисунке приведена таблица маршрутизации маршрутизатора R1 с тремя маршрутами более светлого цвета. Для всех этих маршрутов указан выходящий интерфейс S0/0. При создании анонса RIP, передаваемого через интерфейс S0/0, правила разделенного диапазона указывают маршрутизатору R1 игнорировать эти маршруты более светлого цвета. Только выделенный полужирным маршрут, выходной интерфейс которого отличается от S0/0, может быть включен в передаваемый с интерфейса S0/0 анонс RIP.

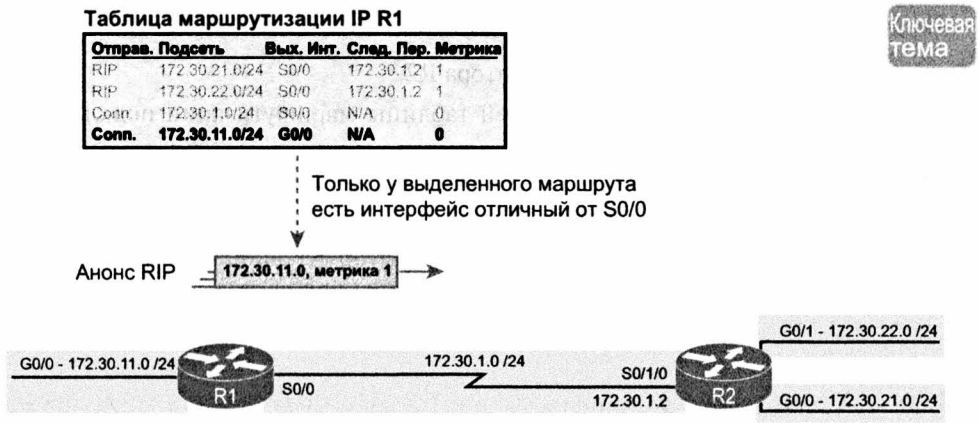


Рис. 9.6. В связи с разделением диапазона маршрутизатор R1 не анонсирует три маршрута

Вытеснение маршрута

Дистанционно-векторные протоколы позволяют предотвратить образование петлевых маршрутов, гарантируя, что каждый маршрутизатор как можно быстрее узнает об отказе маршрута по всем возможным средствам. Одним из этих средств является *вытеснение маршрута* (route poisoning), позволяющее всем маршрутизаторам наверняка узнать об отказе маршрута.

Вытеснение маршрута подразумевает анонсирование отказавшего маршрута со специальным значением метрики — *бесконечностью*. Маршрутизаторы считают маршруты с бесконечной метрикой отказавшими.

Вытеснение маршрута происходит подобно ситуации в реальной жизни, когда у двух человек есть конфликт. Они могут проигнорировать конфликт и не говорить о нем. Но будет полезней, если они открыто обсудят проблему, даже если процесс окажется немного неудобен, и смогут найти разумное решение. Вытеснение маршрута позволяет двум маршрутизаторам открыто переговорить о конкретном типе проблемы: отказавшем маршруте.

На рис. 9.7 приведен пример вытеснения маршрута RIP при отказе интерфейса G0/1 маршрутизатора R2, приведшего к потере маршрута к сети 172.30.22.0/24 через маршрутизатор R2. Протокол RIP определяет бесконечность как значение 16.

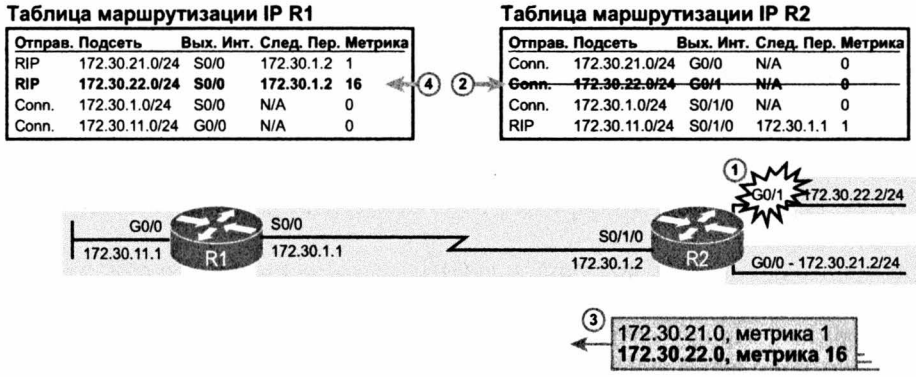


Рис. 9.7. Вытеснение маршрута

На рис. 9.7 представлен следующий процесс.

1. Отказ интерфейса G0/1 маршрутизатора R2.
2. Маршрутизатор R2 удаляет из своей таблицы маршрутизации подключенный маршрут к подсети 172.30.22.0/24.
3. Маршрутизатор R2 анонсирует маршрут к подсети 172.30.22.0 с бесконечной метрикой (для протокола RIP это значение 6).
4. В зависимости от обстоятельств маршрутизатор R1 либо немедленно удаляет маршрут к подсети 172.30.22.0 из своей таблицы маршрутизации, либо отмечает его на несколько минут как непригодный (с бесконечной метрикой), прежде чем удалить.

К концу этого процесса маршрутизатор R1 знает наверняка, что его прежний маршрут к подсети 172.30.22.0/24 отказал. Это поможет маршрутизатору R1 не создавать петлевых маршрутов IP.

У каждого протокола маршрутизации собственное определение бесконечной метрики. Протокол RIP использует значение 16, как показано на рисунке, значение 15 является метрикой вполне допустимого для использования маршрута. У протокола EIGRP бесконечности соответствует значение $2^{32} - 1$ (немногим больше 4 миллиардов), а некоторые новые версии операционной системы IOS используют значение $2^{56} - 1$. Протокол OSPFv2 использует для обозначения бесконечности значение $2^{24} - 1$.

Протокол EIGRP как расширенный дистанционно-векторный протокол

Протокол EIGRP частично действует как дистанционно-векторный протокол, а частично как совершенно уникальный протокол маршрутизации. Откровенно говоря, за долгие годы в различных документах Cisco и разных книгах (включая книги автора) протокол EIGRP относили либо к собственной категории (протоколов маршрутизации сбалансированного гибридного класса), либо к расширенным дистанционно-векторным протоколам.

Независимо от категории, протокол EIGRP использует набор средств, работающих либо как простой дистанционно-векторный протокол, такой как RIP, либо подобным образом. Далее рассматриваются некоторые из этих средств, а также различия между протоколами RIP и EIGRP.

Передача сообщений частичного обновления маршрутов осуществляется по необходимости

Протокол EIGRP не использует частую периодическую передачу полных обновлений со всеми маршрутами, как протокол RIP. Вместо этого протокол EIGRP передает информацию о каждом маршруте только однажды, когда маршрутизатор изучает ее. Впоследствии маршрутизатор посылает только частичные обновления маршрутов.

Частичные обновления маршрутов EIGRP — это сообщения об обновлении, содержащие любую новую или измененную информацию о маршруте. Например, отказ интерфейса маршрутизатора влияет на некоторые маршруты. Маршрутизатор немедленно посылает сообщение частичного обновления маршрутов, содержащее

новую информацию, любому соседнему маршрутизатору EIGRP. Когда маршрутизатору становятся доступны новые маршруты, он посылает частичные обновления только о них. Это не полные обновления маршрутов, поскольку они содержат только измененную или новую информацию.

Концепция немного похожа на лавинную рассылку анонсов LSA в области у протокола OSPF. Но создающий анонсы LSA OSPF маршрутизатор рассылает их каждые 30 минут. Протокол EIGRP даже не потрудится разослать информацию о маршрутизации повторно. Например, если информация о маршруте не изменяется на протяжении года, то протокол EIGRP будет молчать о нем весь год, однажды отправив его анонс.

Для контроля состояния соседей используются сообщения Hello

Протокол EIGRP не посылает сообщениям полного или частичного обновления маршрутов периодически, поэтому он не может полагаться на сообщения об обновлении для контроля состояния соседей. Он использует ту же фундаментальную идею, что и протокол OSPF, — сообщение Hello. Протокол EIGRP определяет, что каждый маршрутизатор должен периодически посылать сообщение Hello на каждом интерфейсе, чтобы все маршрутизаторы EIGRP знали о его работоспособности (рис. 9.8).

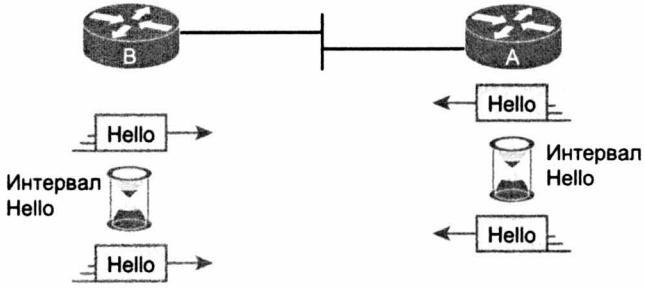


Рис. 9.8. Пакеты Hello протокола EIGRP

Маршрутизаторы используют собственный независимый *интервал Hello* (Hello Interval), определяющий период времени между отправкой каждого сообщения Hello протокола EIGRP. Например, маршрутизаторы R1 и R2 не обязаны посылать свои сообщения Hello одновременно. Кроме того, маршрутизаторы ожидают получения от соседа сообщения Hello на протяжении *интервала задержки* или *интервала Hold* (Hold Interval), стандартно соответствующему трем интервалам Hello.

Предположим, например, что маршрутизаторы R1 и R2 используют стандартные значения (5 и 15) интервалов Hello и Hold. При обычных условиях маршрутизатор R1 получает сообщения Hello от маршрутизатора R2 каждые 5 секунд, вполне в пределах интервала Hold маршрутизатора R1 (15 секунд), по истечении которого маршрутизатор R1 посчитает маршрутизатор R2 отказавшим. Если маршрутизатор R2 откажет, он больше не будет передавать сообщения Hello. Маршрутизатор R1 заметит, что на протяжении 15 секунд не получил от маршрутизатора R2 сообщений Hello и следует выбрать новый маршрут, не использующий маршрутизатор R2 как следующий транзитный маршрутизатор.

Протокол EIGRP не требует, чтобы два соседних маршрутизатора использовали одинаковые таймеры Hello и Hold, но здравый смысл подсказывает поступать именно так. К сожалению, возможная гибкость использования различных параметров на соседних маршрутизаторах позволяет установить таймеры Hello и Hold так, чтобы затруднить правильную работу соседей. Например, если маршрутизатор R2 изменит свои интервалы Hello/Hold на 30/60 соответственно, а маршрутизатор R1 сохранит прежние значения 5/15 секунд, то маршрутизатор R1 будет вполне резонно полагать, что маршрутизатор R2 отказал. Маршрутизатор R2 посылает сообщения Hello только каждые 30 секунд, а маршрутизатор R1 ожидает их получения всего 15 секунд (интервал Hold).

Резюме по внутренним средствам протоколов маршрутизации

Табл. 9.2 резюмирует обсуждаемые в этой главе средства протоколов RIP-2, EIGRP и OSPFv2. В следующем разделе этой главы специфика и особенности работы протокола EIGRP рассматриваются подробней.

Ключевая тема

Таблица 9.2. Сравнение внутренних протоколов маршрутизации IP

Средство	RIP-2	EIGRP	OSPFv2
Метрика на основании:	Счетчика переходов	Ширины полосы пропускания и задержки	Стоимость
Периодически передает полные обновления маршрутов	Да	Нет	Нет
Периодически передает сообщения Hello	Нет	Да	Да
Для отказавших маршрутов используется вытеснение	Да	Да	Да
Для ограничения рассылки обновлений о рабочих маршрутах используется разделение диапазона	Да	Да	Нет
Адрес, на который передаются сообщения	224.0.0.9	224.0.0.10	224.0.0.5, 224.0.0.6
Значение метрики, считающееся бесконечным	16	$2^{32} - 1$ или $2^{56} - 1$	$2^{24} - 1$

Концепции и принцип работы протокола EIGRP

Протокол EIGRP отличается от протокола OSPF вполне очевидно, хотя до некоторой степени они подобны. Фактически протокол EIGRP использует модель с тремя этапами, подобно протоколу OSPF, когда маршрутизатор впервые подключается к сети. Каждый из этих этапов связан со списком или с таблицей: таблицей соседних устройств, таблицей топологии и таблицей маршрутизации. Все эти процессы и таблицы ведут к созданию маршрутов IPv4 в таблице маршрутизации следующим образом.

1. **Обнаружение соседних устройств.** Маршрутизаторы EIGRP рассылают сообщения Hello, чтобы обнаружить соседние маршрутизаторы и проверить их основные конфигурационные параметры. Соседи, передавшие все параметры, отмечаются и добавляются в таблицу соседних устройств EIGRP.

2. **Обмен топологической информацией.** Соседние устройства (иногда называемые *смежными*) обмениваются полной информацией о топологии сети при включении, а впоследствии пересылают друг другу только частичные обновления маршрутов, содержащие информацию об изменениях в сетевой топологии. Полученные в этих обновлениях данные добавляются в таблицу топологии маршрутизатора EIGRP.
3. **Выбор оптимальных маршрутов.** Каждый маршрутизатор EIGRP анализирует топологическую таблицу и выбирает из нее маршруты с наименьшей метрикой к каждой подсети. Протокол EIGRP помещает маршрут с наилучшей метрикой для каждого получателя в таблицу маршрутизации IPv4.

В данном разделе обсуждаются подробности создания протоколом EIGRP своих таблиц маршрутизации согласно этим трем этапам. Хотя в общем трехэтапный процесс выглядит как у протокола OSPF, в подробностях есть существенные отличия, особенно в том, что для обработки топологических данных протокол OSPF использует логику состояния канала (LS), а протокол EIGRP не использует. Кроме этих трех этапов, в настоящем разделе рассматривается уникальная логика, используемая протоколом EIGRP при конвергенции и реакции на изменения в объединенной сети.

Соседи EIGRP

Соседи EIGRP — это маршрутизаторы, на которых запущен процесс маршрутизации EIGRP и которые подключены к той же подсети. В протоколе EIGRP используются специальные тестовые сообщения, называемые сообщениями Hello, для динамического обнаружения соседей. Такие сообщения рассылаются по зарезервированному многоадресатному адресу — 224.0.0.10.

Маршрутизатор выполняет некоторые базовые проверки параметров соседнего маршрутизатора перед тем, как включить его в свою таблицу соседей. Устройство считается потенциальным соседом EIGRP в том случае, если от него получено сообщение Hello. Получив сообщение, маршрутизатор проверяет следующие параметры.

Список причин, по которым устройство в протоколе EIGRP может не стать соседним



- Устройство должно пройти аутентификацию (пароль должен совпасть).
- Должен быть использован тот же номер автономной системы (AS number).
- IP-адрес устройства-отправителя сообщения Hello должен находиться в той же подсети.

ВНИМАНИЕ!

Значения коэффициентов для расчета метрики (так называемые коэффициенты K) должны совпадать у двух соседних устройств. Обсуждение этих коэффициентов выходит за рамки данной книги.

Протокол EIGRP использует относительно простую проверку соседей. Во-первых, если применяется аутентификация, оба маршрутизатора должны использовать одинаковый тип аутентификации и одинаковый ключ (пароль). Во-вторых,

конфигурация протокола EIGRP включает такой параметр, как *номер автономной системы* (Autonomous System Number — ASN), или ASN, который должен совпадать на обоих соседних маршрутизаторах. И наконец, IP-адреса, используемые для передачи сообщений Hello протокола EIGRP (соответствующие IP-адресам интерфейсов маршрутизаторов), должны находиться в диапазоне адресов подключенной подсети других маршрутизаторов.

Протокол EIGRP упрощает соседские отношения существенно больше, чем протокол OSPF. Принимая во внимание, что у соседей OSPF есть несколько промежуточных и несколько стабильных состояний, протокол EIGRP переходит в рабочее состояние сразу, как только соседи пройдут простые проверки. После этого оба маршрутизатора могут начать обмениваться информацией о топологии, используя сообщения об обновлении EIGRP.

Обмен топологической информацией в протоколе EIGRP

В протоколе EIGRP используются так называемые *обновления маршрутов* (update messages) для обмена топологической информацией. Такие сообщения рассылаются по многоадресатному IP-адресу 224.0.0.10, если устройство передает информацию маршрутизаторам в той же подсети; если же обновление маршрутов передается устройству в другой подсети, то оно пересылается на одноадресатный (unicast) IP-адрес конкретного маршрутизатора. Сообщения Hello всегда пересылаются по адресу 224.0.0.10. В отличие от протокола OSPF, в рассматриваемом протоколе маршрутизации нет такого понятия, как выделенный маршрутизатор (DR) или резервный выделенный маршрутизатор (BDR), тем не менее многоадресатный механизм рассылки сообщений позволяет маршрутизаторам EIGRP эффективно обмениваться маршрутной информацией.

Протокол EIGRP рассылает сообщения об обновлении без участия протокола UDP или TCP, и для этого он использует *надежный транспортный протокол* (Reliable Transport Protocol — RTP). Протокол RTP обеспечивает механизм рассылки любых сообщений EIGRP, не получаемых соседом. Использование протокола RTP облегчает избежание петель, поскольку маршрутизатор знает наверняка, что соседний маршрутизатор получил всю обновленную информацию о маршрутизации. (Применение протокола RTP — это только еще один пример отличий протокола EIGRP от таких простых дистанционно-векторных протоколов, как RIP, у которых нет никакого способа узнать, получили ли соседи сообщения об обновлении.)

ВНИМАНИЕ!

Аббревиатурой RTP обозначают также другой протокол, *транспортный протокол реального времени* (Real-time Transport Protocol), используемый для передачи пакетов IP с голосовыми и видеоданными.

Маршрутизаторы EIGRP пересылают друг другу как полные, так и частичные обновления маршрутной информации (см. рис. 9.9). В полном обновлении пересылается информация обо всех известных устройству маршрутах, а в частичных — только информация об изменении топологии, т.е. об изменении состояния какого-либо маршрута. Полные обновления обычно пересылаются устройством, когда маршрутизатор загружается или обнаруживает соседнее устройство. Обменявшись

такими обновлениями, маршрутизаторы пересылают друг другу частичные обновления при изменении какой-либо маршрутной информации.

На рис. 9.9 представлено большинство деталей, обсуждавшихся в этом разделе. Сначала устройства обмениваются сообщениями Hello, затем пересылают полные обновления, а впоследствии периодически обмениваются сообщениями Hello и частичными обновлениями маршрутной информации.

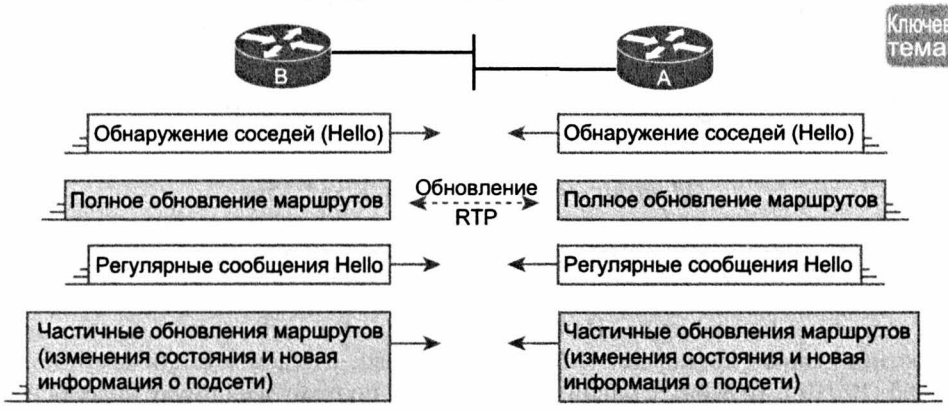


Рис. 9.9. Полные и частичные обновления EIGRP

Обратите внимание, что протокол EIGRP считает передаваемую в обновлениях информацию топологической информацией. Информация почти столь же подробна, как и топологические данные протокола OSPF, но она не пытается описать каждый маршрутизатор и канал связи в сети. Она описывает больше, чем только дистанцию (метрику) и вектор (следующий транзитный маршрутизатор) относительно локального маршрутизатора, последний изучает также метрику, используемую следующим транзитным маршрутизатором. Эта дополнительная информация используется для ускорения конвергенции EIGRP во избежание петель, как обсуждается в следующем разделе.

Расчет оптимальных маршрутов для таблицы маршрутизации

Протокол EIGRP вычисляет метрику для маршрутов совсем не так, как любой другой протокол маршрутизации. Например, при любой схеме сети и знании заданных стоимостей интерфейсов протокол OSPF способен вычислить точную метрику OSPF (стоимость) для каждого маршрута. Протокол EIGRP использует математическое уравнение и составную метрику, затрудняя точное предсказание значения метрики.

Вычисление метрики EIGRP

Составная метрика означает, что в уравнении протокол EIGRP использует несколько источников данных (компонентов метрики). Стандартно протокол EIGRP использует при вычислении два компонента метрики: ширину полосы пропускания и задержку. (Протокол EIGRP позволяет также использовать при вычислении метрики значения загруженности интерфейса и его надежности, хотя компания Cisco не рекомендует их использовать.) Протокол EIGRP анонсирует также максимальный блок передачи данных (MTU) маршрута, т.е. самый длинный пакет IP, разрешенный на маршруте, но при вычислении метрики он не используется.

ВНИМАНИЕ!

Раньше в документации зачастую было указано, что в протоколе маршрутизации EIGRP и его предшественнике, IGRP, в качестве компонента метрики также можно было использовать значение MTU. Размер блока данных, MTU, нельзя использовать в метрике, и он никогда не использовался в ее расчетах.

Формула вычисления метрики EIGRP позволяет описать некоторые из ключевых элементов составной метрики. (В реальной жизни редко кому приходится садиться и вычислять то, что маршрутизатор сам вычисляет по этой формуле.)

Формула расчета метрики протокола EIGRP выглядит следующим образом:

$$Метрика = \left(\left(\frac{10^7}{МПП} \right) + КЗ \right) * 256$$

где МПП — это минимальная полоса пропускания, т.е. минимальная полоса самого медленного канала на маршруте (в килобитах в секунду); КЗ — задержка с фиксацией состояния на маршруте. Например, если полоса пропускания самого низкоскоростного канала составляет 12 Мбит/с, то первое слагаемое в скобках будет равно 1000 ($10^7/10^4$). 10 Мбит/с равно 10 000 Кбит/с, поэтому в формулу подставляется значение 10^4.

Задержка с фиксацией состояния представляет собой сумму задержек всех каналов на маршруте и измеряется в десятках микросекунд.

Использование этих двух значений позволяет протоколу EIGRP выбрать немного лучше сбалансированный наилучший маршрут, чем протокол OSPF. Учет ширины полосы пропускания позволяет протоколу EIGRP избегать маршрутов с самыми медленными каналами связи, обычно создающими наибольшие перегрузки. В то же время применение в уравнении задержки позволяет учесть задержку каждого канала связи, чтобы маршруты с бо́льшим количеством каналов связи были относительно менее желательны, чем маршруты с меньшим количеством каналов связи.

Полосу пропускания и задержку для каждого из каналов можно указать с помощью команд `bandwidth` и `delay` соответственно в режиме конфигурации интерфейса.

ВНИМАНИЕ!

Многие команды `show`, в том числе `show ip eigrp topology` и `show interfaces`, показывают задержку в микросекундах. Тем не менее следует помнить, что в формуле расчета метрики используются десятки микросекунд.

Пример вычисляемых метрик EIGRP

Теперь, когда вы имеете представление о работе математик маршрутизатора EIGRP, рассмотрим пример, объединяющий то, что маршрутизатор изучает в сообщении об обновлении EIGRP, локальные параметры конфигурации и вычисление метрики для одного маршрута.

Локальный маршрутизатор должен учесть информацию, полученную от соседнего маршрутизатора и параметров его локальных интерфейсов. В сообщении об обновлении EIGRP передается номер подсети и маска, а также все компоненты мет-

рики: кумулятивная задержка, минимальная ширина полосы пропускания и другие обычно неиспользуемые компоненты метрики. Затем локальный маршрутизатор рассматривает параметры ширины полосы пропускания и задержки на том интерфейсе, на котором было получено обновление, и вычисляет новую метрику.

Например, на рис. 9.10 представлен маршрутизатор R1, получающий маршрут к подсети 10.1.3.0/24 от маршрутизатора R2. Сообщение об обновлении EIGRP от маршрутизатора R2 содержит минимальную ширину полосы пропускания 100000 Кбит/с и кумулятивную задержку 100 микросекунд. На интерфейсе S0/1 маршрутизатора R1 установлена ширина полосы пропускания 1544 Кбит/с (стандартная ширина полосы пропускания на последовательном канале) и задержка 20000 микросекунд.

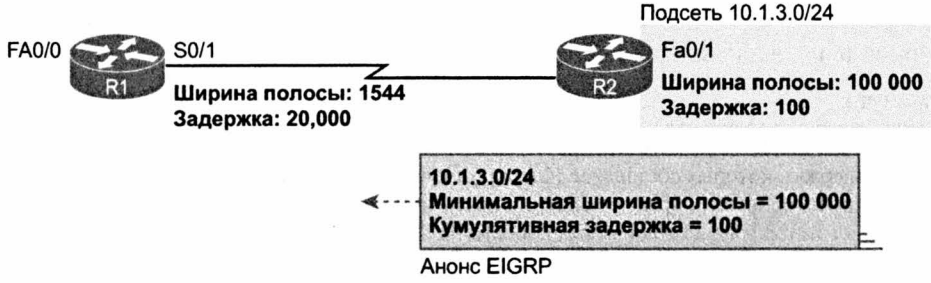


Рис. 9.10. Как маршрутизатор R1 вычисляет свою метрику EIGRP для маршрута 10.1.3.0/24

Теперь рассмотрим, как маршрутизатор R1 учитывает ширину полосы пропускания в вычислениях. Маршрутизатор R1 обнаруживает, что ширина полосы пропускания интерфейса S0/1 (1544 Кбит/с, или 1,544 Мбит/с) меньше анонсируемой минимальной ширины полосы пропускания 100 000 Кбит/с, или 100 Мбит/с. Маршрутизатор R1 должен использовать в вычислении метрики эту новую, более медленную полосу пропускания. (Если бы у интерфейса S0/1 маршрутизатора R1 была ширина полосы пропускания 100 000 Кбит/с или более, то маршрутизатор R1 использовал бы вместо нее минимальную ширину полосы пропускания, указанную в обновлении EIGRP, полученном от маршрутизатора R2.)

Что касается задержки интерфейса, то маршрутизатор всегда добавляет свою задержку интерфейса к задержке, полученной в обновлении EIGRP. Однако единица измерения задержки может создать проблемы. При этом используются следующие единицы.

Микросекунды. Используются в выводе таких команд `show`, как `show interfaces` и `show ip eigrp topology`, а также в сообщениях об обновлении EIGRP.

Десятки микросекунд. Используются командами конфигурации интерфейса (`delay`) для установки задержки и при вычислении метрики EIGRP.

Из-за этого различия в единицах измерения при просмотре задержки убедитесь, что помните о единицах измерения. В данном конкретном примере маршрутизатор R1 получил обновление, содержащее задержку 100 (микросекунд), которую он преобразует в эквивалентные 10 десятков микросекунд, прежде чем использовать это значение в формуле. Маршрутизатор R1 видит, что на его интерфейсе S0/1 установлена задержка 2000 десятков микросекунд, поэтому при вычислении он добавляет 10 десятков микросекунд и получает полную задержку в 2010 десятков микросекунд.

В результате будет получена такая метрика:

$$Метрика = \left(\left(\frac{10^7}{1544} \right) + (10 + 2000) \right) * 256 = 2172\ 416$$

ВНИМАНИЕ!

Для тех, кто хочет повторить эти вычисления: операционная система IOS округляет результат деления в формуле до ближайшего целого числа в меньшую сторону, прежде чем приступить к остальным вычислениям. В данном случае 10^7 / 1544 округляется в меньшую сторону до 6476, затем добавляется 2010, а затем умножается на 256.

Если бы к подсети 10.1.3.0/24 вело несколько маршрутов, то маршрутизатор R1 также рассчитал бы для них метрики, выбрал бы маршрут с наилучшей (меньшей) метрикой и добавил бы его в таблицу маршрутизации.

ВНИМАНИЕ!

Примеры этой главы используют маршрутизаторы с гигабитовыми интерфейсами, стандартное значение задержки которых составляет 10 микросекунд. Но операционная система IOS корректирует задержку на основании фактической скорости интерфейса LAN. В примерах в этой и следующей глав все интерфейсы LAN имеют скорость 100 Мбит/с и задержку 100 микросекунд.

Проблемы с полосой пропускания последовательных каналов

Композитная метрика протокола маршрутизации EIGRP позволяет выбирать и устанавливать в таблицу маршрутизации маршруты, в которых больше транзитных узлов, но при более высокоскоростных каналах. Чтобы быть уверенным в том, что протокол маршрутизации выбирает правильные маршруты, сетевой инженер должен указать соответствующие действительности значения полосы пропускания на интерфейсах. В частности, следует помнить, что для последовательных интерфейсов операционная система использует значение полосы пропускания (bandwidth), равное 1544, и значение задержки 20 000 микросекунд (например, как показано на рис. 9.10). Операционная система Cisco IOS не может автоматически подстраивать значение полосы пропускания на основе скорости канала на уровне 1. Следовательно, если в интерфейсе используются стандартные настройки, то такой интерфейс может вызвать проблемы в сети и в маршрутизации.

На рис. 9.11 показаны проблема, вызванная стандартными значениями полосы пропускания, и как протокол маршрутизации EIGRP будет выбирать правильный маршрут в том случае, если установлено актуальное значение полосы пропускания для интерфейса. В данном примере рассматривается маршрут от маршрутизатора B к подсети 10.1.1.0/24. В верхней части схемы сети на всех интерфейсах устройств используются стандартные настройки, следовательно, полоса пропускания неправильно будет распознаваться для интерфейса со скоростью 64 Кбит/с. В нижней части схеме показано, как протокол маршрутизации будет выбирать маршрут, если для интерфейсов правильно указана полоса пропускания командой `bandwidth`.

Хорошая стратегия метрик для использующих протокол EIGRP сетей подразумевает установку ширины полосы пропускания WAN в соответствии с фактической скоростью уровня 1 и стандартных значений для интерфейсов LAN, в результате протокол EIGRP, как правило, будет выбирать наилучшие маршруты.

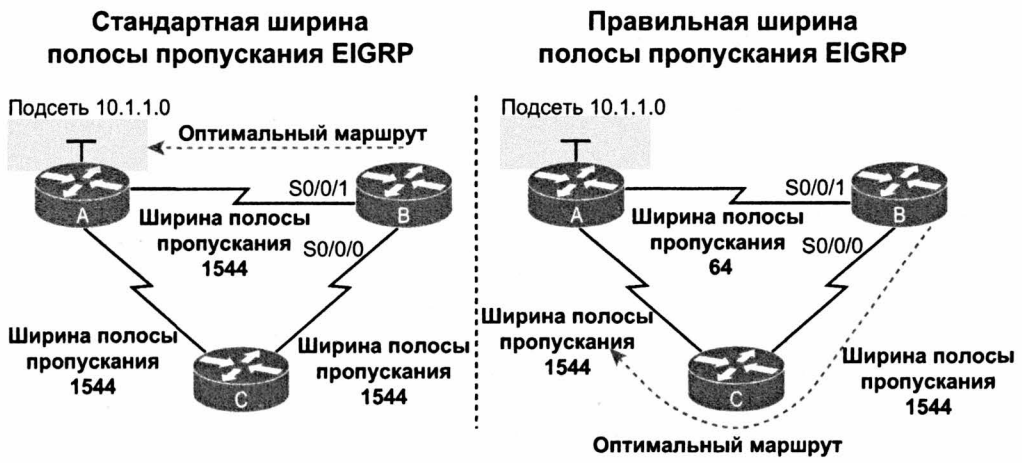


Рис. 9.11. Влияние ширины полосы пропускания на вычисление метрики EIGRP

Конвергенция протокола EIGRP

Теперь, изучив подробности формирования соседских отношений EIGRP, обмена информацией о маршрутизации и вычисления наилучшего маршрута, рассмотрим самую интересную часть протокола EIGRP: конвергенцию, т.е. переход на новый маршрут без петель.

Самая сложная проблема в любом протоколе динамической маршрутизации — кольцевые маршруты. В дистанционно-векторных протоколах маршрутизации она решается за счет использования множества разнообразных механизмов, время работы которых, а следовательно, и время конвергенции сети, может составлять несколько минут после отказа какого-либо канала. В протоколах с учетом состояния каналов проблема кольцевых маршрутов решается за счет того, что каждый маршрутизатор хранит у себя полную топологическую базу сети, а также использует сложные математические алгоритмы для ее обработки.

Протокол EIGRP позволяет избежать петель за счет хранения небольшого количества базовой топологической информации, намного меньшего по сравнению с такими протоколами состояния канала (LS), как OSPF. Протокол EIGRP учитывает каждый возможный следующий транзитный маршрутизатор на резервных маршрутах, а также некоторые подробности о метриках на этих маршрутах, но не учитывает никакой информации о топологии вне следующих транзитных маршрутизаторов. Эта менее подробная информация о топологии не требует сложного алгоритма поиска *первого кратчайшего маршрута* (Shortest Path First — SPF), но обеспечивает быструю конвергенцию маршрутов без петель.

Оптимальное и анонсируемое расстояния

Прежде чем переходить к детальному рассмотрению конвергенции EIGRP, имеет смысл узнать несколько новых терминов EIGRP. В протоколе EIGRP локальный маршрутизатор должен учитывать собственную вычисляемую метрику для каждого маршрута, но в то же время он учитывает вычисляемую метрику следующего транзитного маршрутизатора для той же подсети назначения. Для этих метрик у протокола EIGRP есть специальные термины.

Ключевая тема

Определения оптимального и анонсируемого расстояний

Оптимальное расстояние (Feasible Distance — FD). Метрика локального маршрутизатора для наилучшего маршрута к подсети, вычисляемая на локальном маршрутизаторе.

Анонсируемое расстояние (Reported Distance — RD). Лучшая метрика следующего транзитного маршрутизатора для той же подсети.

Как обычно, рассмотрим определение на примере. Используя тот же анонс, что и на рис. 9.10, на рис. 9.12 показаны оба эти вычисления на маршрутизаторе R1. Сначала маршрутизатор R1 вычисляет собственную метрику FD (оптимальное расстояние) для собственного маршрута к подсети 10.1.3.0/24 (см. рис. 9.10). Компоненты метрики используются также в обновлении, полученном от маршрутизатора R2, применяемом для вычисления метрики доступа к той же подсети. Второе вычисление маршрутизатора R1 основывается на информации от маршрутизатора R2 (самая медленная полоса пропускания составляет 100 000 Кбит/с, а кумулятивная задержка — 100 микросекунд), оно дает анонсируемое расстояние для этого маршрута на маршрутизаторе R1.

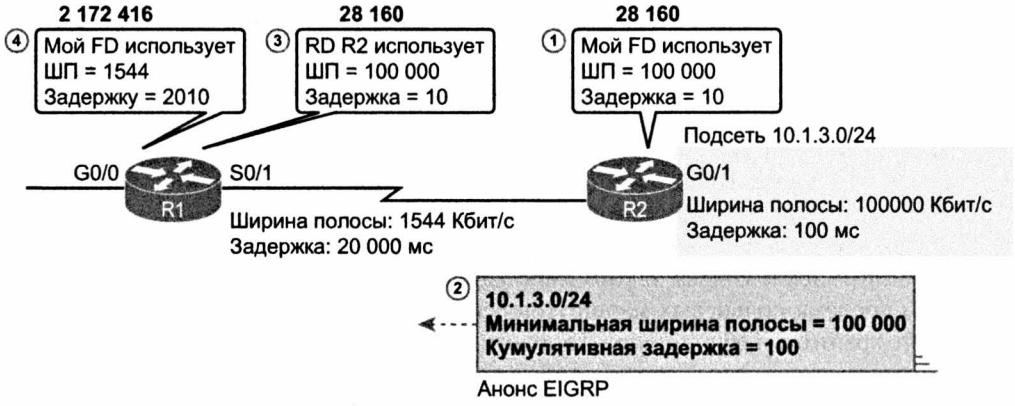


Рис. 9.12. Как маршрутизатор R1 вычисляет анонсируемое (RD) и оптимальное (FD) расстояния для подсети 10.1.3.0/24

Рассмотрим этапы, показанные на рисунке.

1. Маршрутизатор R2 вычисляет собственную метрику FD (свое оптимальное расстояние) для маршрута к подсети 10.1.3.0/24 на основании ширины полосы пропускания 100 000 Кбит/с и задержки 100 микросекунд.
2. Маршрутизатор R2 передает анонс EIGRP для подсети 10.1.3.0/24 с теми же компонентами метрики.
3. Маршрутизатор R1 вычисляет анонсируемое расстояние (RD) для этого маршрута, используя ту же формулу, что и маршрутизатор R2 на этапе 1, со значениями, полученными в анонсе на этапе 2.
4. Маршрутизатор R1 вычисляет свою метрику (с точки зрения маршрутизатора R1), учитывая ширину полосы пропускания и задержку интерфейса S0/1 маршрутизатора R1 (см. рис. 9.10).

Фактически на основании представленной на рис. 9.12 информации можно легко вычислить оптимальное расстояние маршрутизатора R2 для доступа к подсети 10.1.3.0/24, совпадающее с анонсируемым расстоянием маршрутизатора R1 для доступа к подсети 10.1.3.0/24:

$$\left(\left(\frac{10^7}{100\,000}\right)+(10)\right)*256=28160$$

Процесс конвергенции EIGRP использует одну из двух ветвей этой логики, в зависимости от того, имеет ли отказавший маршрут *резервный маршрут* (feasible successor) или нет. Решение о наличии у маршрутизатора резервного маршрута зависит от значений FD и RD параллельных маршрутов для доступа к данной подсети. В следующем разделе определяется концепция резервного маршрута и обсуждается то, что происходит в этом случае.

Оптимальный и резервный маршруты в протоколе EIGRP

Как и любой другой протокол маршрутизации, EIGRP рассчитывает метрики для всех маршрутов ко всем подсетям. Маршрут с наилучшей (минимальной) метрикой до какой-либо подсети называется *оптимальным* (successor), устройство устанавливает такой маршрут в таблицу маршрутизации. Как уже было сказано ранее, метрику такого маршрута называют *оптимальным расстоянием* (feasible distance — FD).

К той же самой подсети может вести несколько маршрутов с метрикой, которая больше, чем FD; из таких маршрутов протокол EIGRP пытается выбрать некоторый резервный маршрут, который можно использовать мгновенно для передачи данных после пропадания основного. Для расчетов протокол EIGRP использует некоторый простой алгоритм, с помощью которого помечает резервные маршруты в топологической таблице, на которые будет происходить мгновенное переключение в случае отказа оптимального пути, а также гарантирует отсутствие кольцевых маршрутов среди них. Такие альтернативные маршруты, готовые к использованию, называют *резервными*. Может ли маршрут использоваться в качестве резервного, определяется следующим правилом.

Ключевая тема

Условие резервного маршрута

Если расстояние RD для неоптимального маршрута строго меньше, чем FD, то такой маршрут будет резервным.

Рассмотрим пример. На рис. 9.13 маршрутизатор E выбирает свой оптимальный маршрут к подсети 1. Маршрутизатор E изучает три маршрута к подсети 1, от маршрутизаторов B, C и D. На рисунке приведены метрики, вычисленные на маршрутизаторе E, показанные в таблице топологии EIGRP маршрутизатора E. Маршрутизатор E находит, что у маршрута через маршрутизатор D самая низкая метрика, делающая этот маршрут оптимальным маршрутом к подсети 1. Маршрутизатор E добавляет этот маршрут в свою таблицу маршрутизации, как показано на рисунке. Метрика FD (оптимальное расстояние), вычисленная для этого маршрута, имеет в данном случае значение 14 000.

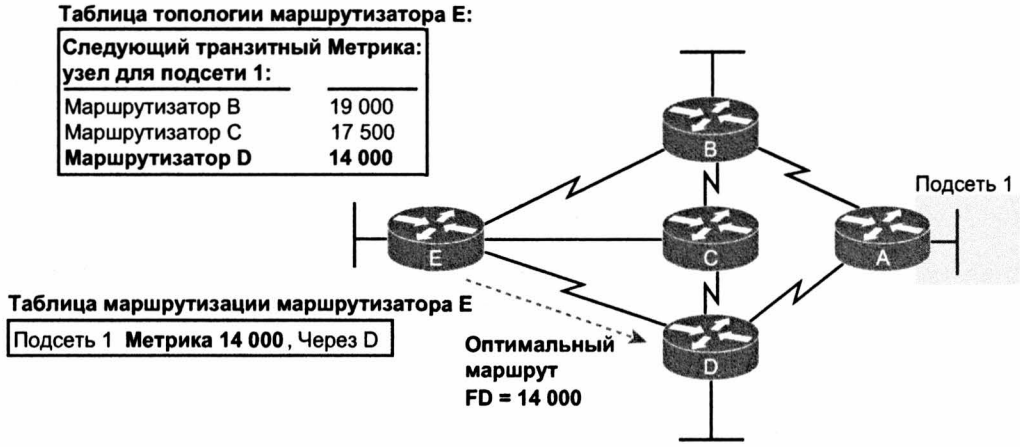


Рис. 9.13. Маршрут через маршрутизатор D является оптимальным маршрутом к подсети 1

В то же время протокол EIGRP на маршрутизаторе E решает, применять ли любой из двух других маршрутов к подсети 1 немедленно, если маршрут через маршрутизатор D откажет по любой причине. Немедленно применяется только резервный маршрут. Чтобы удовлетворять условию резервного маршрута, анонсируемое расстояние (RD) запасного маршрута должно быть меньше, чем оптимальное расстояние (FD) оптимального маршрута. Рис. 9.14 представляет собой обновленную версию рис. 9.13. Маршрутизатор E использует следующую логику, принимая решение о том, что маршрут через маршрутизатор B не является резервным маршрутом, в отличие от маршрута через маршрутизатор C:

- Маршрутизатор E сравнивает FD (14 000) с RD (15 000) маршрута через маршрутизатор B. Поскольку RD больше (хуже), чем FD, маршрут не признается резервным.
- Маршрутизатор E сравнивает FD (14 000) с RD (13 000) маршрута через маршрутизатор C. Поскольку RD лучше, чем FD, этот маршрут признается резервным.

Ключевая тема

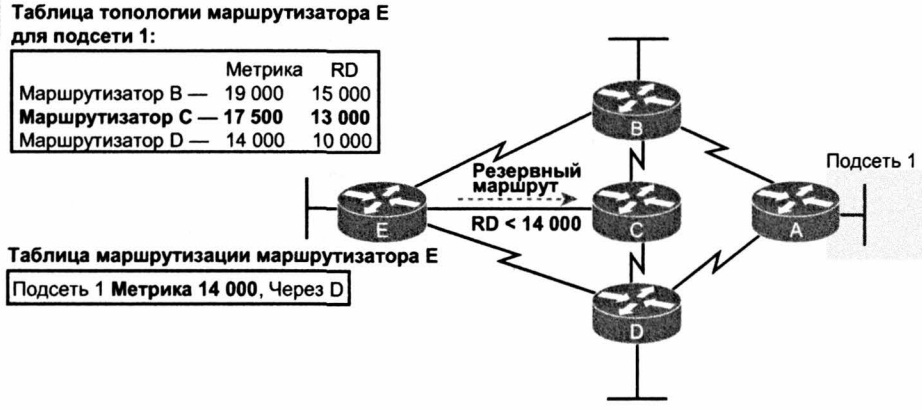


Рис. 9.14. Маршрут через маршрутизатор C является резервным

Если маршрут к подсети 1 через маршрутизатор D откажет, маршрутизатор E сможет немедленно поместить маршрут через маршрутизатор C в таблицу маршрутизации, не опасаясь создания петлевого маршрута. В данном случае конвергенция происходит почти немедленно.

Процесс запросов и ответов

Если к какой-либо подсети пропадает маршрут и для него нет резервного, то в протоколе EIGRP запускается специализированный алгоритм, называемый *алгоритмом распределенных обновлений* (Diffusing Update Algorithm — DUAL). Задача такого алгоритма — разослать запросы соседним устройствам, чтобы обнаружить маршрут к подсети и гарантировать отсутствие петель в маршрутизации. Когда такой маршрут обнаружен, алгоритм DUAL добавляет его в таблицу маршрутизации.

Процесс DUAL протокола EIGRP использует сообщения просто для подтверждения существования маршрута без петель, прежде чем принять решение о замене отказавшего маршрута альтернативным. Предположим, например, что оба маршрутизатора, C и D, на рис. 9.14 откажут. У маршрутизатора E не останется никакого резервного маршрута к подсети 1, но есть очевидный физически доступный путь через маршрутизатор B. Чтобы использовать этот маршрут, маршрутизатор E посылает сообщения *запроса EIGRP* своим работающим соседям (в данном случае маршрутизатору B). Маршрут маршрутизатора B к подсети 1 все еще работает, поэтому маршрутизатор B отвечает маршрутизатору E *ответным сообщением EIGRP*, просто сообщая подробности рабочего маршрута к подсети 1 и подтверждая, что он все еще работоспособен. Затем маршрутизатор E может добавить новый маршрут к подсети 1 в свою таблицу маршрутизации, не опасаясь создания петли.

Процесс DUAL использует специальный механизм обмена сообщениями, чтобы установить, существует ли альтернативный маршрут, убедиться в том, что такой маршрут не будет создавать маршрутных петель, и заменить нерабочий маршрут в таблице маршрутизации новым. Обратимся к рассматривавшейся на рис. 9.14 схеме сети и представим себе, что два маршрутизатора, C и D, отказали. У маршрутизатора E в таком случае не будет резервного маршрута к подсети 1, но зато в сети есть вполне очевидный путь через маршрутизатор B. Чтобы использовать этот маршрут, устройство E сначала должно послать *запрос* (query) всем соседним устройствам (в данном случае маршрутизатору B). Маршрут устройства B к подсети 1 является корректным, поэтому маршрутизатор B ответит специализированным *ответом* (reply), содержащим информацию о маршруте и подтверждающим его работоспособность. Маршрутизатор E после этого добавит новый маршрут к подсети 1 в свою таблицу маршрутизации.

Замена отказавшего маршрута резервным происходит очень быстро и обычно длится 1-2 секунды. Когда же используется механизм запросов и ответов, конвергенция сети может продолжаться дольше; в большинстве сетей время конвергенции обычно составляет порядка 10 секунд.

Обзор

Резюме

- Протокол EIGRP использует надежную метрику на основании ширины полосы пропускания канала связи и задержки канала связи.
- Конвергенция протокола EIGRP очень быстра, а значит, при некотором изменении в объединенной сети протокол EIGRP быстро найдет наилучший в настоящее время маршрут.
- Когда маршрутизатор изучит маршрут к подсети, все маршрутизаторы знают ту же дистанцию (метрику), следующий транзитный маршрутизатор и исходящий интерфейс, используемый для этого маршрута (вектор или направление).
- Разделение диапазона — это функция дистанционно-векторных протоколов маршрутизации, позволяющая не анонсировать маршруты, использующие данный интерфейс как исходящий. Дистанционно-векторные протоколы позволяют предотвратить образование петлевых маршрутов и гарантируют при этом, что каждый маршрутизатор как можно быстрее узнает об отказе маршрута по всем возможным средствам.
- Вытеснение маршрута подразумевает анонсирование отказавшего маршрута со специальным значением метрики — бесконечностью.
- Протокол EIGRP передает информацию о каждом маршруте только однажды, когда маршрутизатор изучает ее.
- Протокол EIGRP не требует, чтобы два соседних маршрутизатора использовали одинаковые таймеры Hello и Hold, но здравый смысл подсказывает поступать именно так.
- Сосед EIGRP — это другой маршрутизатор EIGRP, соединенный с общей подсетью, с которой маршрутизатор желает обмениваться топологической информацией EIGRP.
- Когда маршрутизатор находит нового соседа, он обменивается с ним полными обновлениями маршрутов, как обычные протоколы состояния канала или дистанционно-векторные протоколы.
- После первоначального обмена маршрутами протокол EIGRP посылает только частичные обновления маршрутов, когда изменяется состояние канала связи или добавляется новая подсеть.
- Протокол EIGRP позволяет избежать петель за счет хранении небольшого количества базовой топологической информации, намного меньшего, по сравнению с такими протоколами состояния канала.
- Протокол EIGRP вычисляет метрику для каждого маршрута к подсети, и самая низкая метрика определяет оптимальное расстояние.
- Если к какой-либо подсети пропадает маршрут и для него нет резервного, то протокол EIGRP запускает алгоритм распределенных обновлений, облегчающий обнаружение маршрута к подсети.

Контрольные вопросы

Ответьте на эти вопросы. Ответы можно найти на последней странице главы. Полное объяснение ответов приведено в приложении B на веб-сайте

1. Какое из следующих средств дистанционно-векторных протоколов предотвращает петлевые маршруты, вынуждая протокол маршрутизации анонсировать в нормальном стабильном состоянии только часть известных маршрутов, а не всю таблицу маршрутизации?

   А) Вытеснение маршрута.

   Б) Обратное вытеснение маршрута.

   В) Алгоритм DUAL.

   Г) Разделение диапазона.

2. Какое из следующих средств дистанционно-векторных протоколов предотвращает петлевые маршруты за счет анонсирования маршрута с бесконечной метрикой при отказе маршрута?

   А) Алгоритм SPF Дейкстры.

   Б) Алгоритм DUAL.

   В) Разделение диапазона.

   Г) Вытеснение маршрута.

3. Маршрутизаторы A и B используют протокол EIGRP. Как маршрутизатор A отслеживает состояние маршрутизатора B, чтобы отреагировать на его отказ?

   А) Используя сообщения EIGRP Hello, периодически получаемые маршрутизатором A от маршрутизатора B и подтверждающие его работоспособность.

   Б) Использование сообщений об обновлении EIGRP, периодически получаемые маршрутизатором A от маршрутизатора B и подтверждающие его работоспособность.

   В) Используя периодические пакеты ping с IP-адреса маршрутизатора B, на основании таймера EIGRP соседа.

   Г) Все ответы неверные.

4. Что из перечисленного ниже используется в расчетах метрики протокола EIGRP при стандартных настройках? (Выберите два ответа.)

   А) Полоса пропускания (bandwidth).

   Б) Задержка (delay).

   В) Загрузка (load).

   Г) Надежность (reliability).

   Д) Размер блока MTU.

   Е) Количество транзитных узлов (hop count).

5. Что из перечисленного ниже верно об оптимальном расстоянии протокола EIGRP?

   А) Оптимальное расстояние является характеристикой резервного маршрута (feasible successor).

Б) Оптимальное расстояние является характеристикой оптимального маршрута (successor).

В) Оптимальное расстояние описывает маршрут к подсети от соседнего маршрутизатора.

Г) Оптимальное расстояние представляет собой метрику протокола EIGRP для всех маршрутов к какой-либо подсети.

6. Что из перечисленного ниже верно об анонсируемом расстоянии протокола EIGRP?

А) Оптимальное расстояние является характеристикой резервного маршрута (feasible successor).

Б) Оптимальное расстояние является характеристикой оптимального маршрута (successor).

В) Оптимальное расстояние описывает маршрут к подсети от соседнего маршрутизатора.

Г) Оптимальное расстояние представляет собой метрику протокола EIGRP для всех маршрутов к какой-либо подсети.

Ключевые темы

Повторите все ключевые темы данной главы, отмеченные пиктограммой "Ключевая тема". Ключевые темы и соответствующие им страницы перечислены в табл. 9.3.

Таблица 9.3. Ключевые темы главы 9

Элемент	Описание	Страница
Список	Сравнение ключевых моментов протокола EIGRP с другими протоколами маршрутизации	317
Табл. 9.1	Сравнение внутренних протоколов маршрутизации IP	318
Список	Составляющие термина дистанционно-векторный	320
Рис. 9.6	В связи с разделением диапазона маршрутизатор R1 не анонсирует три маршрута	323
Табл. 9.2	Сравнение внутренних протоколов маршрутизации IP	326
Список	Список причин, по которым устройство в протоколе EIGRP может не стать соседним	327
Рис. 9.9	Полные и частичные обновления EIGRP	329
Список	Определения оптимального и анонсируемого расстояний	334
Определение	Условие резервного маршрута	335
Рис. 9.14	Маршрут через маршрутизатор C является резервным	336

Заполните таблицы и списки по памяти

Распечатайте приложение Г с веб-сайта или его раздел, относящийся к этой главе, и заполните таблицы и списки по памяти. В приложении Д приведены заполненные таблицы и списки для самоконтроля.

Ключевые термины

После первого прочтения главы попытайтесь дать определения следующим ключевым терминам. Но не расстраивайтесь, если не все получится сразу, в главе 22 описано, как использовать эти термины на завершающем этапе подготовки к экзамену.

конвергенция (convergence), дистанционно-векторный (distance vector), протокол маршрутизации внутреннего шлюза (Interior Gateway Protocol — IGP), частичное обновление маршрутов (partial update), периодическое обновление маршрутов (periodic update), откорректированный маршрут (poisoned route), разделение диапазона (split horizon), мгновенное обновление (triggered update), условие резервирования (feasibility condition), оптимальное расстояние (Feasible Distance — FD), резервный маршрут (feasible successor), полное обновление маршрутов (full update), анонсируемое расстояние (reported distance), оптимальный маршрут (successor)

Ответы на контрольные вопросы:

1 Г. 2 Г. 3 А. 4 А и Б. 5 Б. 6 В.

Глава 10

Реализация протокола EIGRP для IPv4

В главе 9 рассматривалась исключительно концепция *расширенного протокола маршрутизации внутреннего шлюза* (Enhanced Interior Gateway Routing Protocol — EIGRP), а в этой главе речь пойдет о том, как заставить его работать на маршрутизаторе Cisco.

В данной главе будет рассмотрено множество параметров настройки протокола EIGRP. Она начинается с описания наиболее фундаментальных параметров настройки протокола EIGRP, а затем более частных задач конфигурации (например, как настроить балансировку нагрузки неравной метрики), а также функции автоматического суммирования, которая имеет громкое название, но является, главным образом, областью потенциальных проблем.

Здесь мы будем регулярно обращаться к командам конфигурации и соответствующим командам, позволяющим проверить полученную настройку и работоспособность средства. В частности, мы затронем тему поиска оптимального расстояния, анонсируемого расстояния, резервного маршрута и оптимального маршрута.

В этой главе рассматриваются следующие экзаменационные темы

Технологии маршрутизации IP

Настройка и проверка EIGRP (одиночная область)

- Приемлемое расстояние / Возможные преемники / Административное расстояние
- Условие применимости
- Композиция метрик
- Идентификатор маршрутизатора
- Автоматический отчет
- Выбор пути
- Баланс нагрузки
  - Равномерный
  - Неравномерный
- Пассивный интерфейс

Различия методов маршрутизации и протоколов маршрутизации

- Административное расстояние
- Разделение диапазона
- Метрика
- Следующий транзитный узел

Основные темы

Настройка и проверка протокола EIGRP

Данный раздел начинается с обсуждения наиболее популярных элементов конфигурации протокола EIGRP. Как принято в этой книге, раздел начинается с тем по настройке и продолжается темами по проверке.

Настройка протокола EIGRP

Настройка протокола EIGRP очень похожа на настройку протокола OSPF. Команда `router eigrp` разрешает его применение и переводит пользователя в режим конфигурации EIGRP, где настраивается одна или несколько команд `network`. Для каждого соответствующего команде `network` интерфейса протокол EIGRP пытается обнаруживать соседей и анонсировать подсеть, подключенную к данному интерфейсу.

Ниже перечислены основные этапы настройки маршрутизатора.

Последовательность настройки протокола EIGRP



Этап 1 Перейдите в режим конфигурации EIGRP и задайте номер автономной системы EIGRP (номер ASN) при помощи глобальной команды `router eigrp` *`номер_автономной_системы`*

Этап 2 Укажите одну или несколько команд `network` *`IP-адрес`* [*`шаблон_маски`*] в режиме конфигурирования маршрутизатора. Эти команды включают протокол EIGRP на интерфейсах, адреса которых попадают в указанный ими диапазон, и добавляют соответствующие сети в обновления маршрутной информации

Этап 3 (Необязательный.) Подкомандой маршрутизатора `eigrp router-id` *`значение`* явно задайте идентификатор маршрутизатора EIGRP (RID)

Этап 4 (Необязательный.) Можно изменить таймеры Hello и Hold с помощью команд `ip interval hello eigrp` *`номер_автономной_системы таймер`* и `ip hold-time eigrp` *`номер_автономной_системы таймер`* в режиме конфигурирования интерфейса

Этап 5 (Необязательный.) Можно повлиять на выбор маршрута протоколом маршрутизации вручную, указав на интерфейсах полосу пропускания с помощью команд `bandwidth` *`значение`* и `delay` *`значение`*

Этап 6 (Необязательный.) Можно указать, сколько маршрутов с одинаковой метрикой будет одновременно использоваться для балансировки нагрузки с помощью команды `maximum-paths` *`значение`*, и включить балансировку нагрузки по каналам с разными метриками с помощью команды `variance` *`множитель`*

Этап 7 (Необязательный.) Разрешите автоматическое суммирование маршрутов в границах классовых сетей IPv4, используя подкоманду маршрутизатора `auto-summary`

С примера 10.1 начинается обсуждение самой простой из возможных конфигураций протокола EIGRP. В этой конфигурации используется максимум стандартных значений, но она действительно разрешает протокол EIGRP на каждом интерфейсе всех маршрутизаторов, представленных на рис. 10.1. Все три маршрутизатора могут использовать одинаковую конфигурацию только при двух обязательных командах на каждом маршрутизаторе.

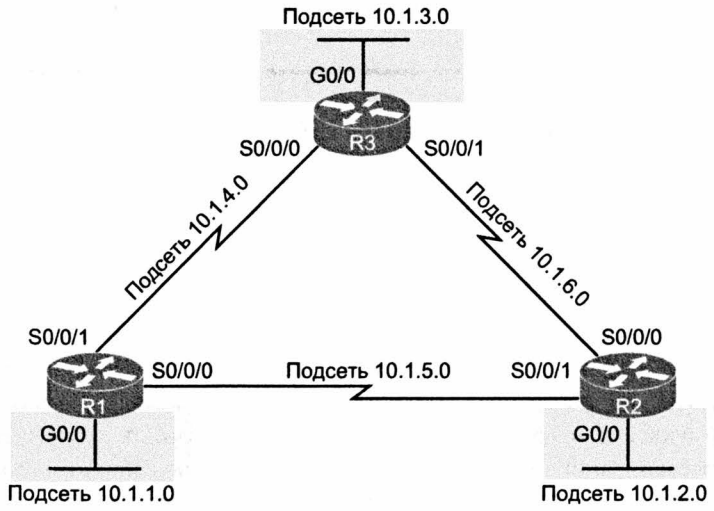


Рис. 10.1. Схема сети для примеров настройки протокола EIGRP

Пример 10.1. Настройка конфигурации EIGRP на всех трех маршрутизаторах рис. 10.1

```
router eigrp 1
  network 10.0.0.0
```

В этой простой конфигурации используется только два параметра, выбираемых сетевым инженером: номер автономной системы и номер классовый сети в команде `network`.

Фактический номер ASN не имеет значения, но все маршрутизаторы должны использовать в команде `router eigrp` одинаковое значение номера ASN. В данном примере все они используют команду `router eigrp 1`. (Маршрутизаторы, использующие разные номера ASN, не станут соседями EIGRP.) Диапазон допустимых номеров ASN, от 1 до 65 535, совпадает с диапазоном допустимых идентификаторов процесса в команде `router ospf`.

Команды EIGRP `network` допускают две разновидности синтаксиса: один с шаблоном маски в конце и один без него, как показано в примере 10.1 (команда `network 10.0.0.0`). Без шаблона маски эта команда должна вывести классовую сеть (номер сети класса A, B или C). Будучи веденной, эта команда указывает маршрутизатору сделать следующее:

- найти собственные интерфейсы с адресами в этой классовой сети;
- разрешить протокол EIGRP на этих интерфейсах.

Будучи разрешенным, протокол EIGRP начинает анонсировать подсети, подключенные к интерфейсам, рассылать сообщения Hello и прослушивать их, пытаясь установить соседские отношения с другими маршрутизаторами EIGRP.

ВНИМАНИЕ!

Интересно, но на реальных маршрутизаторах можно ввести команду EIGRP `network` *номер* и использовать разделяемое точками десятичное число, не являющееся номером классовой сети. В этом случае операционная система IOS не выдаст сообщения об ошибке, однако изменит введенный номер так, чтобы он стал номером используемой классовой сети. Например, операционная система IOS изменит команду `network 10.1.1.1` на `network 10.0.0.0`.

Настройка протокола EIGRP с использованием шаблона маски

Команда EIGRP `network` без шаблона маски, как показано в примере 10.1, может делать именно то, что хочет инженер, но этого может оказаться недостаточно. Например, инженер хочет разрешить протокол EIGRP на интерфейсе G0/0, но не на интерфейсе G0/1. IP-адреса обоих интерфейсов принадлежат сети класса A 10.0.0.0, а подкоманда EIGRP `network 10.0.0.0` распространилась бы на оба интерфейса, а не только на интерфейс G0/0.

Операционная система IOS предоставляет вторую версию команды EIGRP `network`, позволяющую использовать шаблон маски, чтобы инженер мог точно установить правильное значение IP-адреса интерфейса. В данном случае команда `network` должна использовать не номер классовой сети, а IP-адрес и шаблон маски, как в списке управления доступом (ACL). Логика та же, что и у адреса с шаблоном маски в списке ACL или у адреса и маски в команде OSPF `network`, обсуждаемой в главе 8.

Вернемся к рис. 10.1. У маршрутизатора R3 есть IP-адреса в трех подсетях: 10.1.3.0/24, 10.1.4.0/24 и 10.1.6.0/24. Пример 10.2 демонстрирует дополнительную конфигурацию EIGRP для маршрутизатора R3, использующую команду `network` для диапазона адресов в каждой из трех подключенных к нему подсетей. При маске подсети /24 каждая из команд `network` использует шаблон маски 0.0.0.255 с параметром адреса идентификатора подсети одного из интерфейсов маршрутизатора R3.

Пример 10.2. Использование шаблона маски в конфигурации EIGRP

```
R3(config)# router eigrp 1
R3(config-router)# network 10.1.3.0 0.0.0.255
R3(config-router)# network 10.1.4.0 0.0.0.255
R3(config-router)# network 10.1.6.0 0.0.0.255
```

В качестве альтернативы маршрутизатор R3 мог бы снабдить каждый интерфейс командами, использующими шаблон маски 0.0.0.0 и конкретный IP-адрес каждого интерфейса. Например, команда `network 10.1.3.3 0.0.0.0` соответствовала бы адресу 10.1.3.3 интерфейса LAN маршрутизатора R3, разрешая протокол EIGRP на этом одном интерфейсе.

Проверка основных средств протокола EIGRP

Подобно протоколу OSPF, протокол EIGRP использует три таблицы, соответствующие трем его главным логическим блокам: *таблицу соседних устройств* (neighbor table), *таблицу топологии* (topology table) и *таблицу маршрутизации IPv4* (IPv4 routing table). Однако прежде, чем протокол EIGRP даже попытается постро-

ить эти таблицы, операционная система IOS должна соединить логику конфигурации с локальными интерфейсами. Когда протокол разрешен на интерфейсе, маршрутизатор может начать создавать свои три таблицы.

Далее рассматриваются этапы проверки рабочей объединенной сети, использующей протокол EIGRP. На рис. 10.2, *слева*, представлен набор концепций (сверху вниз) со ссылками на различные команды `show` справа. Дальнейшие темы следуют той же последовательности.

ВНИМАНИЕ!

Все последующие примеры проверки содержат вывод, полученный на маршрутизаторах рис. 10.1. На этом рисунке маршрутизаторы R1 и R2 используют конфигурацию EIGRP из примера 10.1, а маршрутизатор R3 использует конфигурацию, представленную в примере 10.2. Кроме того, обратите внимание, что все маршрутизаторы используют гигабитовые интерфейсы LAN, работающие на скорости 100 Мбит/с, поскольку они соединены с коммутаторами; этот факт влияет на метрики в немалой степени.

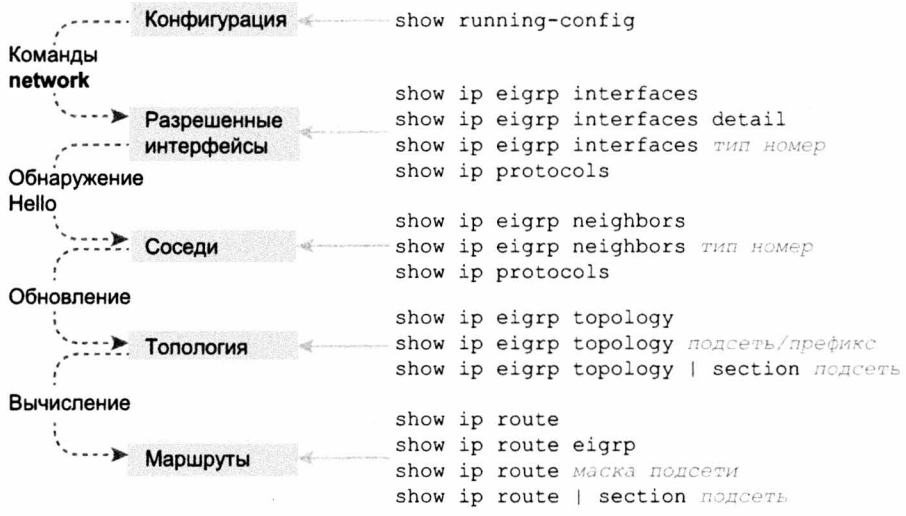


Рис. 10.2. Путеводитель по темам (слева) и командам проверки (справа)

Поиск интерфейсов с разрешенным протоколом EIGRP

В первую очередь каждый маршрутизатор должен разрешить протокол EIGRP на соответствующих интерфейсах. Пример 10.3 начинает процесс проверки конфигурации с интерфейсов маршрутизатора, на которых разрешен протокол EIGRP. Операционная система IOS предоставляет три способа составления списка таких интерфейсов.

- Команда `show running-config` позволяет просмотреть конфигурацию протокола EIGRP и интерфейсов. Она применяют ту же логику для создания списка интерфейсов, на которых должен быть разрешен протокол EIGRP.

- Команда `show ip protocols` выводит краткую версию информации о конфигурации протокола EIGRP, для создания списка интерфейсов применяется та же логика.
- Команда `show ip eigrp interfaces` выводит интерфейсы маршрутизатора, на которых фактически разрешен протокол EIGRP.

Из этих трех возможностей только команда `show ip eigrp interfaces` позволяет создать истинный список интерфейсов, фактически выбранных маршрутизатором. Две другие команды демонстрируют конфигурацию и позволяют сделать обоснованное предположение. (Обе важны!)

Команда `show ip eigrp interfaces` выводит поддерживающие протокол EIGRP интерфейсы непосредственно и кратко, по одной строке на интерфейс. Списки команды `show ip eigrp interfaces detail`, напротив, очень подробны, информация об интерфейсе включает интервалы Hello и Hold, а также разрешено ли разделение диапазона. Пример 10.3 демонстрирует вывод обеих команд на маршрутизаторе R1.

Пример 10.3. Поиск интерфейсов с разрешенным протоколом EIGRP на маршрутизаторе R1

```
R1# show ip eigrp interfaces
EIGRP-IPv4 Interfaces for AS(1)
              Xmit Queue   PeerQ        Mean   Pacing Time  Multicast   Pending
Interfac Peers Un/Reliable Un/Reliable SRTT   Un/Reliable  Flow Timer  Routes
Gi0/0    0     0/0         0/0         0      0/0          0           0
Se0/0/0  1     0/0         0/0         2      0/16         50          0
Se0/0/1  1     0/0         0/0         1      0/15         50          0

R1# show ip eigrp interfaces detail S0/0/0
EIGRP-IPv4 Interfaces for AS(1)
              Xmit Queue   PeerQ        Mean   Pacing Time  Multicast   Pending
Interfac Peers Un/Reliable Un/Reliable SRTT   Un/Reliable  Flow Timer  Routes
Se0/0/0  1     0/0         0/0         2      0/16         50   0
  Hello-interval is 5, Hold-time is 15
  Split-horizon is enabled
! Строки опущены для краткости
```

Обратите внимание, что первая команда, `show ip eigrp interfaces`, выводит все интерфейсы с разрешенным протоколом EIGRP, на которые маршрутизатор в настоящее время посылает сообщения Hello, пытаясь найти новых соседей EIGRP. Маршрутизатор R1 с одной подкомандой EIGRP `network 10.0.0.0` разрешает протокол EIGRP на всех трех своих интерфейсах (согласно рис. 10.1). Вторая команда выводит больше подробностей об интерфейсе, включая параметры интервала Hello локального маршрутизатора, времени задержки и разделения горизонта.

Обратите также внимание на отсутствие информации об интерфейсах, на которых не разрешен протокол EIGRP. Например, если протокол EIGRP не разрешен на интерфейсе S0/0/0, команда `show ip eigrp interfaces detail S0/0/0` просто не выведет о нем информации под строкой заголовков. Короче говоря, вывод команды `show ip eigrp interface` опускает интерфейсы, на которых не разрешен протокол EIGRP.

Кроме того, обратите внимание, что команда `show ip eigrp interfaces ...` не выводит информацию для пассивных интерфейсов. Как и открытый протокол поиска первого кратчайшего маршрута (OSPF), протокол EIGRP поддерживает подкоманду `passive-interface type number`. Эта команда указывает протоколу EIGRP не обнаруживать и не формировать соседские отношения на указанном интерфейсе. Но протокол EIGRP все еще анонсирует подсети, подключенные к интерфейсу.

Таким образом, команда `show ip eigrp interfaces` выводит информацию об интерфейсах с разрешенным протоколом EIGRP, но не о пассивных интерфейсах EIGRP.

Два других метода поиска интерфейсов с разрешенным протоколом EIGRP требуют исследования конфигурации и размышления о правилах EIGRP. В реальной жизни начинают с команды `show ip eigrp interfaces`, но на экзамене может быть дана только конфигурация, или даже она не дана. В качестве альтернативы команда `show ip protocols` выводит много подробностей о протоколе EIGRP, включая краткое повторение команд конфигурации EIGRP `network`. Пример 10.4 демонстрирует вывод этих команд на маршрутизаторе R1.

Пример 10.4. Использование команды `show ip protocols` для получения списка интерфейсов с разрешенным протоколом EIGRP на маршрутизаторе R1

```
R1# show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "eigrp 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP-IPv4 Protocol for AS(1)
    Metric weight K1=1, K2=0, K3=1, K4=0, K5=0
    NSF-aware route hold timer is 240
    Router-ID: 10.1.5.1
      Topology : 0 (base)
        Active Timer: 3 min
       Distance: internal 90 external 170
       Maximum path: 4
       Maximum hopcount 100
       Maximum metric variance 1
  Automatic Summarization: disabled
  Maximum path: 4
  Routing for Networks:
    10.0.0.0
  Routing Information Sources:
    Gateway         Distance      Last Update
    10.1.4.3        90            00:22:32
    10.1.5.2        90            00:22:32
  Distance: internal 90 external 170
```

Для просмотра краткого повторения конфигурации EIGRP обратитесь к концу примера, ниже заголовка `Routing for Networks`. В данном случае следующая строка указывает адрес 10.0.0.0 — это прямая ссылка на команду конфигурации `network 10.0.0.0`, представленную в примере 10.1. Для конфигураций, использующих пара-

метр шаблона маски, формат немного иной, чем показано в примере 10.5, где демонстрируется отрывок вывода команды `show ip protocols` на маршрутизаторе R3. Маршрутизатор R3 использует три команды `network`, приведенные в примере 10.2.

Пример 10.5. Просмотр заданных команд `network` при помощи команды `show ip protocols`




```
R3# show ip protocols
! Строки опущены для краткости

  Automatic Summarization: disabled
  Maximum path: 4
  Routing for Networks:
    10.1.3.0/24
    10.1.4.0/24
    10.1.6.0/24
! Строки опущены для краткости
```

Для интерпретации значения выделенных строк вывода команды `show ip protocols` следует выполнить несколько математических вычислений. Числа в выводе имеют формат /*x* (в данном случае /24). Это шаблон маски с *x* двоичных 0, или в данном случае — 0.0.0.255.

Завершая рассмотрение команды `show ip protocols`, уделим еще минуту некоторым деталям вывода этой команды в примере 10.4. Например, она выводит идентификатор маршрутизатора EIGRP (RID), которым у маршрутизатора R1 является 10.1.5.1. Протокол EIGRP резервирует свой RID точно так же, как и протокол OSPF, на основании следующего.

Правила выбора протоколом EIGRP идентификатора маршрутизатора



1. Значение, заданное подкомандой EIGRP `eigrp router-id` *номер*.
2. Наибольший IP-адрес работающего петлевого интерфейса на момент начала процесса EIGRP.
3. Наибольший IP-адрес не петлевого интерфейса на момент начала процесса EIGRP.

Единственное различие по сравнению с протоколом OSPF в том, что идентификатор RID EIGRP задается подкомандой маршрутизатора `eigrp router-id` *значение*, тогда как протокол OSPF использует подкоманду `router-id` *значение*.

Отображение состояния соседей EIGRP

Как только маршрутизатор разрешает протокол EIGRP на интерфейсе, он пытается обнаруживать соседние маршрутизаторы, прослушивая сообщения EIGRP Hello. Если два соседних маршрутизатора слышат сообщения Hells друг от друга и соответствуют обязательным параметрам, они становятся соседями.

Наилучшая и наиболее очевидная команда вывода соседей EIGRP — это `show ip eigrp neighbors`. Она выводит список соседей на основании IP-адресов интерфейсов (а не идентификаторов их маршрутизаторов, как в соглашении OSPF). Вывод указывает также интерфейс локального маршрутизатора, доступного соседу.

Пример 10.6 демонстрирует соседей маршрутизатора R1, выводя их по IP-адресу 10.1.4.3 (R3). Он доступен маршрутизатору R1 через интерфейс S0/0/1, согласно первой выделенной строке в примере.

Пример 10.6. Отображение соседей EIGRP для маршрутизатора R1

```
R1# show ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(1)
H   Address     Interface   Hold Uptime   SRTT   RTO  Q    Seq
                            (sec)         (ms)       Cnt  Num
1   10.1.4.3    Se0/0/1      13 00:05:49  2      100  0    29
0   10.1.5.2    Se0/0/0      12 00:05:49  2      100  0    39
```

Правая часть вывода также содержит немного интересной статистики. Четыре столбца справа имеют отношение к протоколу RTP, обсуждавшемуся в главе 9. Столбец `Uptime` отображает время, прошедшее с момента установления соседских отношений. И наконец, в столбце `Hold` указан обратный отсчет текущего времени задержки от 15 секунд, в данном случае до 0. В данном случае при интервале Hello 5 и интервале Hold 15 этот счетчик изменится от 15 до 10, а затем сбрасывается в 15, когда поступает следующее сообщение Hello.

Другой, менее очевидный способ создания списка соседей EIGRP подразумевает использование команды `show ip protocols`. Вернемся в примере 10.4 к концу вывода команды `show ip protocols` на маршрутизаторе R1. В списке ниже заголовка `Routing Information Sources` перечислены IP-адреса тех же двух соседних маршрутизаторов, что и в выводе команды `show ip eigrp neighbors` в примере 10.6.

Отображение таблиц маршрутизации IPv4

Как только маршрутизаторы EIGRP становятся соседями, они начинают обмениваться информацией о маршрутизации и сохранять ее в свих таблицах топологии. Затем они вычисляют свои наилучшие маршруты IPv4. В этом разделе пропускается множество этапов проверки для занесения в таблицы топологии EIGRP — автор оставил эту тему для второго раздела данной главы. Тем не менее на настоящий момент этапы проверки таблиц маршрутизации IP должны быть вам уже знакомы в общих чертах. В примере 10.7 приведено несколько моментов для маршрутизатора R1 на рис. 10.1: сначала показана вся таблица маршрутизации IPv4, а затем, в выводе команды `show ip route eigrp`, только маршруты, изученные по протоколу EIGRP.

Пример 10.7. Таблица маршрутизации IP на маршрутизаторе R1 (согласно рис. 10.1)

```
R1# show ip route
Codes: L - local, 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, H - NHRP, l - LISP
       + - replicated route, % - next hop override
```

```
Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 9 subnets, 2 masks
C       10.1.1.0/24 is directly connected, GigabitEthernet0/0
L       10.1.1.1/32 is directly connected, GigabitEthernet0/0
D       10.1.2.0/24 [90/2172416] via 10.1.5.2, 00:06:39, Serial0/0/0
D       10.1.3.0/24 [90/2172416] via 10.1.4.3, 00:00:06, Serial0/0/1
C       10.1.4.0/24 is directly connected, Serial0/0/1
L       10.1.4.1/32 is directly connected, Serial0/0/1
C       10.1.5.0/24 is directly connected, Serial0/0/0
L       10.1.5.1/32 is directly connected, Serial0/0/0
D       10.1.6.0/24 [90/2681856] via 10.1.5.2, 00:12:20, Serial0/0/0
                    [90/2681856] via 10.1.4.3, 00:12:20, Serial0/0/1

R1# show ip route eigrp
! Легенда, опущена для краткости

      10.0.0.0/8 is variably subnetted, 9 subnets, 2 masks
D       10.1.2.0/24 [90/2172416] via 10.1.5.2, 00:06:43, Serial0/0/0
D       10.1.3.0/24 [90/2172416] via 10.1.4.3, 00:00:10, Serial0/0/1
D       10.1.6.0/24 [90/2681856] via 10.1.5.2, 00:12:24, Serial0/0/0
                    [90/2681856] via 10.1.4.3, 00:12:24, Serial0/0/1
```

Обе команды, `show ip route` и `show ip route eigrp`, выводят перед изученными по протоколу EIGRP маршрутами символ `D`. Компания Cisco решила использовать для обозначения протокола EIGRP символ `D`, поскольку, когда он был создан, символ `E` уже использовался для ныне устаревшего *протокола маршрутизации внешнего шлюза* (Exterior Gateway Protocol — EGP). Поэтому для обозначения маршрутов, изученных по протоколу EIGRP, компания Cisco выбрала следующий ближайший неиспользованный символ — D.

Теперь уделите минуту обдумыванию маршрутов EIGRP, полученных маршрутизатором R1 по подключенным к нему маршрутам. В проекте на рис. 10.1 шесть подсетей: три в локальных сетях и три в глобальных. Первая команда примера выводит три из этих подсетей как подключенные маршруты (10.1.1.0/24, 10.1.4.0/24 и 10.1.5.0/24). Другие три подсети выглядят как изученные маршруты EIGRP.

И наконец, обратите внимание, что два числа в скобках для каждого маршрута представляют собой административное расстояние и составную метрику соответственно. Операционная система IOS использует административное расстояние для выбора наилучшего маршрута, когда она изучает несколько маршрутов к той же подсети, но из двух разных источников информации о маршрутизации. Более подробную информацию об административном расстоянии см. в главе 8.

Метрики EIGRP, оптимальные и резервные маршруты

Протоколы OSPF и EIGRP используют в основном подобные идеи: разрешение протокола на интерфейсах маршрутизаторов, формирование соседских отношений, создание таблиц топологии и добавление маршрутов IPv4 в таблицу маршрутизации. Эти протоколы маршрутизации отличаются главным образом по топологическим данным, которые они создают и используют. Подобно протоколу состояния канала, протокол OSPF создает и сохраняет много топологических данных, достаточно много, чтобы смоделировать всю топологию сети в области. Протокол EIGRP

сохраняет разные виды данных с меньшим количеством подробностей и использует совершенно иной алгоритм анализа данных.

Во втором разделе этой главы основное внимание уделено топологической базе данных EIGRP и, в частности, ключевым идеям хранения в базе данных. Как упоминалось в главе 9, *оптимальный маршрут* (successor) EIGRP — это оптимальный маршрут маршрутизатора для доступа к подсети. Любой из других возможных маршрутов без петель, применимый при отказе оптимального маршрута, называется *резервным маршрутом* (Feasible Successor — FS). Вся информация, необходимая для определения, какой маршрут является оптимальным, какой резервным (или если он не является ни тем ни другим), приведена в таблице топологии EIGRP.

В этом разделе продемонстрировано использование команды `show` для идентификации оптимального и резервного маршрутов согласно таблице топологии EIGRP. Чтобы обсуждение было более интересным, в примерах этого раздела используется расширенная топология сети (рис. 10.3).

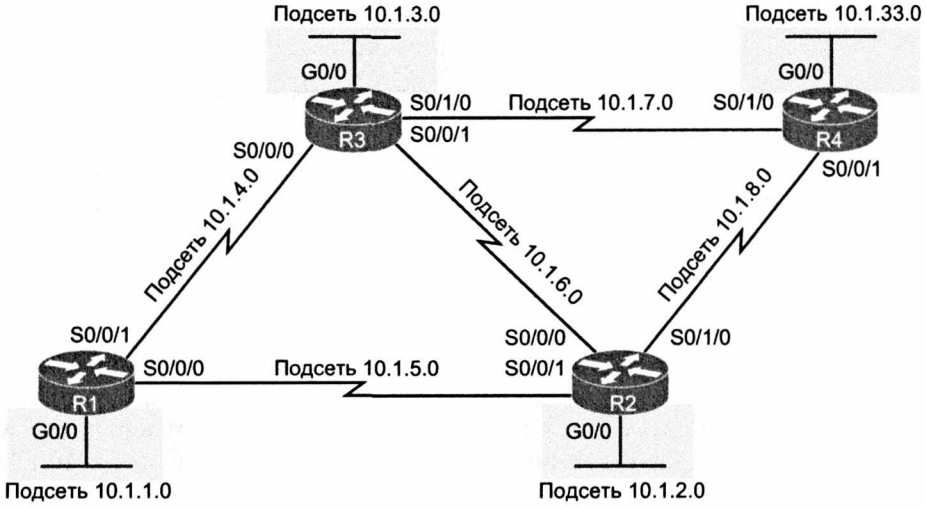


Рис. 10.3. Расширенная объединенная сеть

Просмотр таблицы топологии EIGRP

Для начала рассмотрим таблицу топологии EIGRP на маршрутизаторе R1 для расширенной сети, показанной на рис. 10.3. У новой сети пять сетей WAN и четыре подсети LAN, с несколькими маршрутами для доступа к каждой подсети. Все каналы связи используют стандартные параметры ширины полосы пропускания и задержки. (Обратите внимание, что, как и в предыдущих примерах, все гигабитовые интерфейсы маршрутизаторов применяют автопереговоры для использования скорости 100 Мбит/с, что изменяет параметры задержки интерфейса, а следовательно, и вычисление метрик EIGRP.)

Пример 10.8 начинается с обсуждения вывода команды `show ip eigrp topology` на маршрутизаторе R1. Эта команда выводит несколько строк информации о каждой известной маршрутизатору R1 подсети в таблице топологии EIGRP.

Пример 10.8. Таблица топологии EIGRP на маршрутизаторе R1

```
R1# show ip eigrp topology
EIGRP-IPv4 Topology Table for AS(1)/ID(10.1.5.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

P 10.1.5.0/24,  1 successors, FD is 2169856
        via Connected, Serial0/0/0
P 10.1.7.0/24,  1 successors, FD is 2681856
        via 10.1.4.3 (2681856/2169856), Serial0/0/1
P 10.1.3.0/24,  1 successors, FD is 2172416
        via 10.1.4.3 (2172416/28160), Serial0/0/1
P 10.1.2.0/24,  1 successors, FD is 2172416
        via 10.1.5.2 (2172416/28160), Serial0/0/0
P 10.1.6.0/24, 2 successors, FD is 2681856
        via 10.1.4.3 (2681856/2169856), Serial0/0/1
        via 10.1.5.2 (2681856/2169856), Serial0/0/0
P 10.1.4.0/24,  1 successors, FD is 2169856
        via Connected, Serial0/0/1
P 10.1.33.0/24,  2 successors, FD is 2684416
        via 10.1.4.3 (2684416/2172416), Serial0/0/1
        via 10.1.5.2 (2684416/2172416), Serial0/0/0
P 10.1.1.0/24,  1 successors, FD is 28160
        via Connected, GigabitEthernet0/0
P 10.1.8.0/24,  1 successors, FD is 2681856
        via 10.1.5.2 (2681856/2169856), Serial0/0/0
```

Сначала просмотрите весь вывод и подсчитайте подсети на каналах в левой части примера. Обратите внимание на то, что маршрутизатор R1 выводит группу сообщений для всех девяти подсетей, включая подключенные подсети от маршрутизатора R1. Протокол EIGRP хранит свою топологическую информацию обо всех подсетях, включая подключенные подсети.

Теперь внимательно рассмотрите первую выделенную строку для подсети 10.1.3.0/24 от интерфейса LAN маршрутизатора R3. В первой строке для данной подсети выводится идентификатор подсети и маска, а также количество оптимальных маршрутов и оптимальное расстояние (FD). (Напомним, FD — это метрика оптимального маршрута, являющегося наилучшим маршрутом для доступа к определенной подсети.)

Чтобы вам было понятно, элементы на рис. 10.4 приведены с теми же подробностями о подсети 10.1.3.0/24 в таблице топологии EIGRP маршрутизатора R1.

Уделим подсети 10.1.3.0/24 еще несколько минут. Вывод содержит по одной строке на подсеть получателя и по одной строке ниже для маршрута, начиная со слова *via*. На рис. 10.4 в первой строке (как обычно) выводятся подсеть, префиксная маска, количество оптимальных маршрутов и FD. Во второй строке (с отступом) выводится информация о маршруте, включая следующий транзитный маршрутизатор (после слова *via*) и исходящий интерфейс. Если бы маршрутизатор поместил данный конкретный маршрут в таблицу маршрутизации IP, то в этом маршруте IP использовался бы данный IP-адрес следующей транзитной точки перехода и локальный исходящий интерфейс. Обратите внимание: если протокол EIGRP выводит несколько таких строк, начинающихся со слова *via*, то есть несколько возможных маршрутов к данной подсети.

Ключевая тема

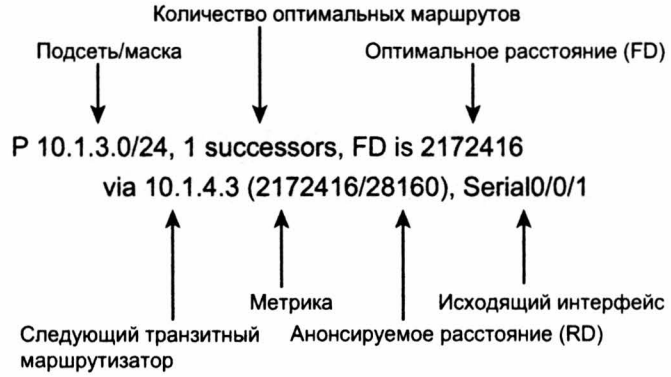


Рис. 10.4. Поля в выводе команды `show ip eigrp topology`

И наконец, обратите внимание, что команда `show ip eigrp topology` также выводит в круглых скобках две вычисляемые метрики EIGRP. Первая метрика вычисляется локальным маршрутизатором для данного маршрута. Вторая — это анонсируемое расстояние (RD): метрика, вычисляемая с точки зрения следующего транзитного маршрутизатора. В представленном на рис. 10.4 примере RD 28160 является анонсируемым расстоянием маршрутизатора R1 для этого маршрута, что будет метрикой на следующем транзитном маршрутизаторе 10.1.4.3 (R3).

Поиск оптимального маршрута

К сожалению, команда `show ip eigrp topology` не свидетельствует со всей очевидностью, какие маршруты являются оптимальными (другими словами, лучше всего), а какие резервными (т.е. быстро используемыми для замены). Ниже показано, как в выводе этой команды найти резервные и оптимальные маршруты.

В первую очередь обратите внимание, что вывод в примере 10.8 отображает только оптимальные маршруты, без резервных маршрутов. Со всеми стандартными параметрами ширины полосы пропускания и задержки ни один из маршрутов в этой сети не указывается как резервный. В примере 10.11 часть параметров изменена так, что некоторые маршруты стали резервными, а пока обратите внимание на то, что все выведенные в примере 10.8 маршруты являются оптимальными.

Проще всего распознать оптимальный маршрут по тому, что у него одинаковые значения метрики и FD. Первая строка вывода топологии для подсети отображает FD (т.е. наилучшую метрику из всех маршрутов для доступа к подсети). У оптимального маршрута по определению наилучшая метрика, поэтому она должна равняться FD (оптимальному расстоянию). Как показано на рис. 10.5, достаточно найти FD в первой строке, а затем найти среди маршрутов тот, у которого та же метрика (первое число в круглых скобках).

Когда протокол EIGRP вычисляет метрики для всех возможных маршрутов, победитель иногда очевиден, поэтому протокол EIGRP выбирает один оптимальный маршрут (см. рис. 10.5). Но в других случаях метрики для параллельных маршрутов к той же подсети равнозначны. В этом случае, при стандартных параметрах конфигурации, протокол EIGRP предоставляет такое средство, как *распределение нагрузки с учетом равной стоимости* (equal-cost load balancing), позволяющее рассматривать все эти маршруты как оптимальные.

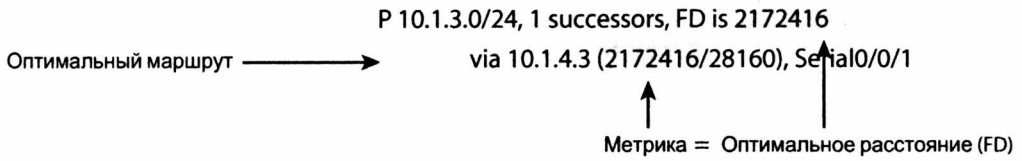


Рис. 10.5. Идентификация оптимального маршрута: FD (первая строка) равняется метрике (вторая строка)

В примере 10.9 демонстрируются два оптимальных маршрута. Это отрывок таблицы топологии EIGRP для маршрута R1 к подсети 10.1.33.0/24, доступной на интерфейсе LAN маршрутизатора R4. В данном случае маршрутизатор R1 имеет два разных маршрута через два разных интерфейса к двум разным соседним следующим транзитным маршрутизаторам. Оба маршрута имеют одинаковую метрику, равную FD (2684416), поэтому они являются оптимальными.

Пример 10.9. Отображение двух оптимальных маршрутов на маршрутизаторе R1 для подсети 10.1.33.0/24

```
R1# show ip eigrp topology | section 10.1.33.0
P 10.1.33.0/24,  2 successors, FD is 2684416
        via 10.1.4.3 (2684416/2172416), Serial0/0/1
        via 10.1.5.2 (2684416/2172416), Serial0/0/0
```

В данном случае, при стандартных настройках, маршрутизатор R1 добавил бы оба маршрута в свою таблицу маршрутизации IP. Далее в главе логика работы маршрутизатора с несколькими маршрутами равной стоимости к той же подсети обсуждается немного подробней, а также обсуждаются возможности балансировки нагрузки на маршрутах равной стоимости.

ВНИМАНИЕ!

В примере 10.9 команда `show ip eigrp topology` связана с командой `section`. Она требует у операционной системы IOS найти раздел или группу сообщений с выводимым текстом (в данном случае `10.1.33.0`) и представить только эту группу сообщений. Это способ получения только желаемой части, а не всего вывода команды.

Поиск резервного маршрута

В соответствии с соглашением, команда `show ip eigrp topology` выводит и оптимальный, и резервный маршруты, если они есть. До сих пор в этой главе использовались стандартные параметры ширины полосы пропускания и задержки, что предотвращало образование резервных маршрутов. Теперь изменим конфигурацию так, чтобы создать резервные маршруты и продемонстрировать их распознавание в топологической базе данных.

Сначала рассмотрим пример 10.9, выводящий топологические данные маршрутизатора R1 для подсети 10.1.33.0/24 — подсети LAN на маршрутизаторе R4. С точки зрения маршрутизатора R1 при всех стандартных параметрах ширины полосы пропускания и задержки оба маршрута идентичны. Маршрут от маршрутизатора R1 до маршрутизатора R3 использует два последовательных канала со стандартными настройками ширины полосы пропускания в 1544 Кбит/с и задержкой в 20000 микро-

секунд на всех последовательных каналах. Маршрут от маршрутизатора R1 до маршрутизатора R2 также использует два последовательных канала, также со стандартной шириной полосы пропускания и задержкой. В результате у маршрутизатора R1 есть два маршрута равной стоимости для подсети 10.1.33.0/24, как показано на рис. 10.6, *слева*.

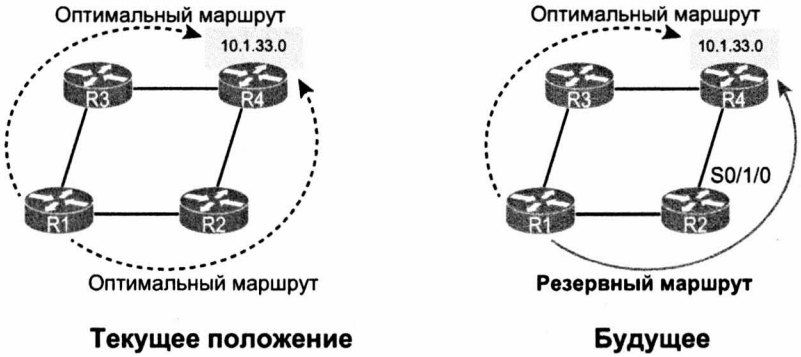


Рис. 10.6. Сравнение двух оптимальных маршрутов для получения одного оптимального и одного резервного маршрутов

В следующем примере маршрут через маршрутизатор R2 сделан хуже, чем маршрут через маршрутизатор R3, у него теперь ниже ширина полосы пропускания на последовательном канале маршрутизатора R2, соединенного с маршрутизатором R4. В настоящее время путь R1-R2-R4 имеет с точки зрения маршрутизатора R1 ширину полосы пропускания меньше 1544 Кбит/с. При снижении ширины полосы пропускания до значения ниже 1544 Кбит/с метрики этих двух маршрутов больше не будут совпадать. В результате верхний маршрут, R1-R3-R4, останется единственным оптимальным маршрутом, а маршрут R1-R2-R4 станет резервным.

Для начала, чтобы изменить конфигурацию, ухудшив ширину полосы пропускания, в примере 10.10 показана команда `bandwidth 1400` для интерфейса S0/1/0 маршрутизатора R2.

Пример 10.10. Изменение ширины полосы пропускания интерфейса при настройке маршрутов EIGRP

```
R2# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)# interface s0/1/0
R2(config-if)# bandwidth 1400
```

Как только маршрутизатор R2 изменяет свою ширину полосы пропускания, он посылает частичное обновление EIGRP (см. главу 9). Другие маршрутизаторы получают новую информацию и повторно вычисляют свои метрики и значения анонсируемого расстояния (RD). Для демонстрации различий в примере 10.11 повторяется команда `show ip eigrp topology | section 10.1.33.0` на маршрутизаторе R1, как в предыдущем примере 10.9. В примере 10.9 эта команда показала на маршрутизаторе R1 два оптимальных маршрута к этой подсети. Теперь, в примере 10.11,

у маршрутизатора R1 есть только один оптимальный маршрут, но резервный маршрут (FS) в выводе фактически скрыт, а причина объясняется после примера.

Пример 10.11. Просмотр резервного маршрута на маршрутизаторе R1 к подсети 10.1.33.0/24

```
R1# show ip eigrp topology | section 10.1.33.0
P 10.1.33.0/24, 1 successors, FD is 2684416
        via 10.1.4.3 (2684416/2172416), Serial0/0/1
        via 10.1.5.2 (2854912/2342912), Serial0/0/0
```

Чтобы увидеть резервный маршрут и выяснить, почему он резервный, рассмотрим числа в выводе примера 10.11. Или рассмотрим тот же вывод, повторенный на рис. 10.7 с комментариями. В любом случае логика следующая.

- Согласно первой строке, существует один оптимальный маршрут.
- Оптимальное расстояние (FD) составляет 2684416.
- В двух строках, начинающихся на via (два возможных маршрута), метрика первого маршрута составляет 2684416 и равняется оптимальному расстоянию (FD). В результате первая строка выводит подробности одного оптимального маршрута.
- Вторая начинающаяся на via строка имеет метрику (первое число в круглых скобках) 2854912, что отличается от значения FD 2684416. В результате этот маршрут не является оптимальным.
- Во второй, начинающейся на via строке указано анонсируемое расстояние (RD, второе число) 2342912, которое меньше оптимального расстояния (FD) 2684416. Таким образом, второй маршрут соответствует условию резервного, что и делает его резервным маршрутом.

Ключевая тема

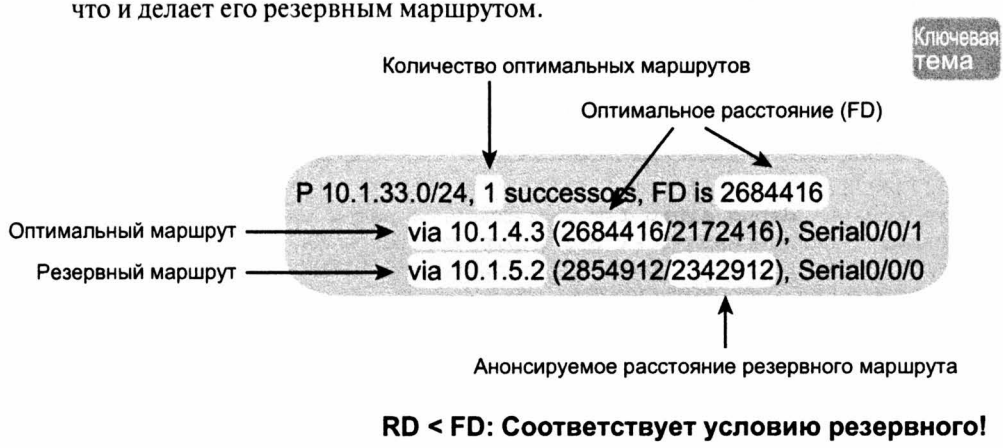


Рис. 10.7. Идентификация резервного маршрута

ВНИМАНИЕ!

Команда `show ip eigrp topology` выводит только оптимальные и резервные маршруты. Для просмотра других маршрутов используйте команду `show ip eigrp topology all-links`, выводящую все маршруты, даже не являющиеся ни оптимальными, ни резервными.

Конвергенция с использованием резервного маршрута

Протокол EIGRP нуждается в концепции резервного маршрута для помощи в скорейшей конвергенции при отказе оптимального маршрута, так как резервный маршрут применяется немедленно. Следующий пример демонстрирует процесс конвергенции на маршрутизаторе R1, когда он теряет свой текущий оптимальный маршрут к подсети 10.1.33.0/24 через маршрутизатор R3 и заменяет его резервным маршрутом через маршрутизатор R2 (рис. 10.8).



Рис. 10.8. Схема события конвергенции описывается в следующем примере

В примере 10.12 показаны не только главные результаты отказоустойчивой архитектуры и конвергенции, но и процесс использования некоторых отладочных сообщений. Как известно, некоторые из отладочных сообщений не имеют особого смысла. Часть из них в примере удалена, а наиболее полезные сообщения выделены в выводе, чтобы подчеркнуть происходящее в отказоустойчивой архитектуре.

В данном примере канал связи между маршрутизаторами R3 и R4 отключен (командой `shutdown`). Отладочные сообщения на маршрутизаторе R1 демонстрируют влияние логики EIGRP при изменении маршрута. Обратите особое внимание на временные метки в отладочных сообщениях, — как ни удивительно, но все происходит в пределах той же миллисекунды.

Пример 10.12. Отладочные сообщения во время конвергенции на резервный маршрут к подсети 10.1.33.0/24

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
! Ниже команда debug eigrp fsm разрешает, а затем маршрутизатор R3
! блокирует канал связи S0/1/0 с маршрутизатором R4, но это не
! представлено в тексте примера. НЕКОТОРЫЕ СООБЩЕНИЯ ОТЛАДКИ пропущены
! для повышения удобочитаемости.
R1# debug eigrp fsm
EIGRP FSM Events/Actions debugging is on
R1#
*Nov 13 23:50:41.099: EIGRP-IPv4(1): Find FS for dest 10.1.33.0/24. FD is
2684416, RD is 2684416 on tid 0
*Nov 13 23:50:41.099: EIGRP-IPv4(1): 10.1.4.3 metric
72057594037927935/720575940379279 36
*Nov 13 23:50:41.099: EIGRP-IPv4(1): 10.1.5.2 metric 2854912/2342912
found Dmin is 2854912
*Nov 13 23:50:41.099: DUAL: AS(1) RT installed 10.1.33.0/24 via 10.1.5.2
!
! Далее маршрутизатор R1 использует новый оптимальный маршрут
! к подсети 10.1.5.2: R2.
```

```
R1# show ip eigrp topology | section 10.1.33.0
P 10.1.33.0/24, 1 successors, FD is 2854912
        via 10.1.5.2 (2854912/2342912), Serial0/0/0
R1# show ip route | section 10.1.33.0
D     10.1.33.0/24 [90/2854912] via 10.1.5.2, 00:16:50, Serial0/0/0
```

И наконец, удостоверьтесь, что обратили внимание на конечное состояние конвергенции в конце примера. Пример демонстрирует обновленные записи топологической базы данных R1 для подсети 10.1.33.0/24 с новым оптимальным маршрутом, новым оптимальным расстоянием (FD) (2854912 вместо прежних 2684416, как в примере 10.10) и новым следующим транзитным маршрутизатором (R2, 10.1.5.2). Последняя команда выводит новый маршрут IPv4 с новым оптимальным расстоянием, указанным как метрика в скобках, и новым следующим транзитным маршрутизатором R2 (10.1.5.2).

Исследование компонентов метрики

До сих пор обсуждение метрик в этой главе сосредоточивалось в основном на составной метрике EIGRP. Но протокол EIGRP анонсирует разные компоненты метрики и затем использует некоторые из этих компонентов для вычисления составной метрики. Прежде чем завершить обсуждение выбора оптимального маршрута (с наилучшей метрикой) и резервных маршрутов (без петель) на основании их составной метрики, в данном разделе будет показано, как просмотреть индивидуальные компоненты метрики, используемые протоколом EIGRP.

При использовании стандартных значений (рекомендуемых Cisco) протокол EIGRP базирует свою составную метрику на минимальной ширине полосы пропускания канала связи на маршруте и полной задержке всех каналов связи на маршруте. Однако маршрутизаторы EIGRP анонсируют все компоненты метрики, включая надежность канала связи и его загрузку. В примере 10.13 показан вывод команды `show ip eigrp topology 10.1.3.0/24` на маршрутизаторе R1. Команда выводит подробности топологических данных EIGRP для маршрутов к этой подсети. Выделенные строки в примере отображают составную метрику, а также индивидуальные компоненты метрики.

Пример 10.13. Компоненты метрики EIGRP в топологической базе данных

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
R1# show ip eigrp topology 10.1.3.0/24
EIGRP-IPv4 Topology Entry for AS(1)/ID(10.1.13.1) for 10.1.3.0/24
  State is Passive, Query origin flag is 1, 1 Successor(s), FD is 2172416
  Descriptor Blocks:
  10.1.4.3 (Serial0/0/1), from 10.1.4.3, Send flag is 0x0
    Composite metric is (2172416/28160), route is Internal
    Vector metric:
      Minimum bandwidth is 1544 Kbit
      Total delay is 20100 microseconds
      Reliability is 255/255
      Load is 1/255
      Minimum MTU is 1500
      Hop count is 1
      Originating router is 3.3.3.3
10.1.5.2 (Serial0/0/0), from 10.1.5.2, Send flag is 0x0
```

```
Composite metric is (2684416/2172416), route is Internal
Vector metric:
    Minimum bandwidth is 1544 Kbit
    Total delay is 40100 microseconds
    Reliability is 255/255
    Load is 1/255
    Minimum MTU is 1500
    Hop count is 2
```

Другие параметры конфигурации EIGRP

До сих пор в этой главе мы рассматривали базовые функции протокола EIGRP. Подробности конфигурации были относительно общими, только в связи с природой протокола EIGRP. Тем не менее мы уделили немало времени на демонстрацию результатов разрешения протокола EIGRP на маршрутизаторах в сети, разрешения его работы на интерфейсах, формирования соседских отношений, изучения топологической информации и в конечном счете добавления маршрутов в таблицу маршрутизации IP.

Настоящий раздел посвящен уже не базовым средствам, а затронутые в нем темы либо совершенно необязательны, либо стандартны и не обсуждались до сих пор. Здесь также затрагивается небольшой ряд других тем EIGRP, включая балансировку нагрузки, настройку метрик EIGRP и автоматическое суммирование.

Балансировка нагрузки между несколькими маршрутами EIGRP

Подобно протоколу OSPF, протокол EIGRP позволяет поместить в таблицу маршрутизации IPv4 несколько маршрутов с равными метрикам. Как и протокол OSPF, стандартно протокол EIGRP поддерживает четыре таких маршрута для каждой подсети, но подкоманда EIGRP `maximum-paths` *`количество`* позволяет задать и другое значение. (Обратите внимание: максимальное количество путей равной стоимости зависит от версии операционной системы IOS и платформы маршрутизатора.)

Фактически в примере 10.9 продемонстрирован подобный случай с маршрутом к подсети 10.1.33.0/24 на маршрутизаторе R1. Пример 10.14 возвращается к тому же случаю, но на сей раз с отображением таблиц топологии и маршрутизации IP. Благодаря стандартным параметрам конфигурации EIGRP, `maximum-paths 4`, маршрутизатор R1 помещает оба оптимальных маршрута в таблицу маршрутизации IP.

Пример 10.14. Таблица маршрутизации маршрутизатора R1 с несколькими маршрутами EIGRP равной стоимости

```
R1# show ip eigrp topology | section 10.1.33.0
P 10.1.33.0/24, 2 successors, FD is 2684416
        via 10.1.4.3 (2684416/2172416), Serial0/0/1
        via 10.1.5.2 (2684416/2172416), Serial0/0/0

R1# show ip route | section 10.1.33.0
D     10.1.33.0/24 [90/2684416] via 10.1.5.2, 00:02:23, Serial0/0/0
                   [90/2684416] via 10.1.4.3, 00:02:23, Serial0/0/1
```

Хотя возможность добавить несколько маршрутов с одинаковыми метриками может быть полезна, протокол EIGRP зачастую вычисляет подобные значения метрик, которые близки, но все же не равны. Значения метрик EIGRP зачастую исчисляются миллионами, поэтому точное совпадение маловероятно.

Для решения этой проблемы операционная система IOS применяет концепцию *балансировки нагрузки с неодинаковыми стоимостями* (unequal-cost load balancing), использующую такой параметр EIGRP, как *вариация* (variance). Вариация позволяет считать равными маршруты с относительно близкими значениями метрики, а следовательно, добавлять в таблицу маршрутизации несколько маршрутов неравной метрики к той же подсети.

В режиме конфигурирования протокола маршрутизации EIGRP с помощью команды `variance` *множитель* можно указать целое число в диапазоне 1–128 (параметр вариации метрики). Маршрутизатор после введения этой команды умножает метрику FD (т.е. метрику оптимального маршрута) на это число и получает диапазон метрики маршрутов, которые могут быть добавлены в таблицу маршрутизации. Строго говоря, любой резервный маршрут, метрика RD которого меньше, чем полученное число, будет считаться маршрутом с равной метрикой FD и может быть установлен в таблицу маршрутизации. Сколько таких маршрутов попадет в таблицу маршрутизации протокола EIGRP, опять же зависит от настройки, заданной командой `maximum-paths`.

В предыдущем подразделе действительно резюмируются правила для вариации и балансировки нагрузки с неодинаковыми стоимостями, но понять концепцию на примере много проще. Чтобы сделать числа более очевидными, в табл. 10.1 приведены небольшие значения метрики. В таблице перечислены метрики трех маршрутов к той же подсети, рассчитанные маршрутизатором R4. В таблице также перечислены метрики RD для соседних маршрутизаторов и указано, какое именно решение по каждому маршруту примут устройства на основе параметра вариации.

Таблица 10.1. Пример работы параметра вариации метрики

Следующий транзитный узел	Метрика	RD	Добавляется в таблицу маршрутизации при вариации, равной 1	Добавляется в таблицу маршрутизации при вариации, равной 2	Добавляется в таблицу маршрутизации при вариации, равной 3
R1	50	30	Да	Да	Да
R2	90	40	Нет	Да	Да
R3	120	60	Нет	Нет	Нет

Прежде чем описывать параметр вариации, следует обратить внимание на то, что маршрут через маршрутизатор R1 является оптимальным, поскольку у него минимальная метрика. Следовательно, метрика этого маршрута, 50, является оптимальным расстоянием (FD). Маршрут через маршрутизатор R2 является резервным, поскольку его метрика (анонсируемое расстояние RD) 40 меньше, чем расстояние FD, равное 50. Маршрут через маршрутизатор R3 резервным не является, так как его значение RD, равное 60, больше, чем FD.

Стандартное значение вариации метрики равно 1, поэтому метрики должны быть равны друг другу точно, чтобы они считались совпадающими. В таком случае только один маршрут будет добавлен в таблицу маршрутизации.

При наличии команды `variance 2` значение FD (50) умножается на вариацию (2), что дает 100. Маршрут через маршрутизатор R2 с метрикой 90 хоть и меньше, чем результат уравнения вариация*FD = 100, но маршрутизатор R4 также добавляет маршрут через маршрутизатор R2 в таблицу маршрутизации. Теперь маршрутизатор может направить трафик через оба эти маршрута, сбалансировав нагрузку. Метрика третьего маршрута, 120, больше, чем вариация*FD = 100, поэтому он не добавляется в таблицу маршрутизации.

При наличии команды `variance 3` произведение FD (50) на 3 дает 150, а вычисляемые метрики всех трех маршрутов меньше 150. Однако маршрут через маршрутизатор R3 не является резервным (FS), поэтому он не может быть добавлен в таблицу маршрутизации во избежание образования петлевого маршрута.

Ниже перечислены ключевые моменты, связанные с параметром вариации метрики.



Вариация метрики в протоколе EIGRP

- Текущее значение метрики FD маршрута к подсети (т.е. оптимального) умножается на параметр вариации метрики.
- Резервные маршруты, метрика которых меньше или равна произведению FD на вариацию, добавляются в таблицу маршрутизации с учетом значения, указанного в команде `maximum-paths`.
- Маршруты, не являющиеся оптимальными или резервными, не могут быть добавлены в таблицу маршрутизации, независимо от значения, указанного в настройках вариации, поскольку это может создать петлевые маршруты.

После того как маршруты были установлены в таблицу маршрутизации, устройство может балансировать нагрузку по ним с помощью разных методов. Маршрутизатор может балансировать нагрузку по каналам пропорционально метрикам каналов, а это означает, что в канал с меньшей метрикой будет отправляться большее количество пакетов. Маршрутизатор может пересылать весь трафик через канал с наименьшей метрикой, а остальные маршруты будут присутствовать в таблице маршрутизации только для ускорения конвергенции протокола маршрутизации при исчезновении оптимального маршрута к подсети. Детали различных механизмов балансировки нагрузки требуют более тщательного исследования внутренних механизмов пересылки пакетов операционной системы IOS, а эти темы выходят за рамки рассмотрения данной книги.

Настройка алгоритма расчета метрики в протоколе EIGRP

Стандартно протокол EIGRP вычисляет целочисленную метрику на основании ширины полосы пропускания и задержки интерфейса. Используя подкоманды интерфейса `bandwidth` *значение* и `delay` *значение*, можно изменить эти параметры на любом интерфейсе, что в свою очередь повлияет на выбор маршрутизаторами маршрутов.

Компания Cisco рекомендует устанавливать совершенно точное значение ширины полосы пропускания каждого интерфейса, а не подбирать его с целью подпра-

вить значение вычисляемой метрики EIGRP. Последовательные каналы маршрутизатора следует настраивать командой `bandwidth` *скорость*, со значением скорости в Кбит/с, подбирая фактическую скорость интерфейса. Интерфейсы Ethernet маршрутизатор может использовать со стандартными настройками; операционная система IOS изменит параметр ширины полосы пропускания интерфейса Ethernet так, чтобы он соответствовал фактической физической скорости передачи.

Поскольку на параметр задержки интерфейса полагается и несколько других средств операционной системы IOS, компания Cisco рекомендует изменять параметр задержки интерфейса, если необходимо настроить метрику EIGRP. Для изменения параметра задержки интерфейса используйте команду `delay` *значение*, где *значение* — это параметр задержки с необычной единицей измерения в десятки микросекунд. Интересно, но формула метрики EIGRP также использует десятки микросекунд; однако команды `show` выводят значение задержки в микросекундах, как демонстрирует пример 10.15, включая следующие подробности.

1. Интерфейс Fa0/0 маршрутизатора имеет стандартный параметр задержки в 100 микросекунд (мс), т.е. фактически он работает на скорости 100 Мбит/с.
2. Команда `delay 123` устанавливает на интерфейсе задержку в 123 десятка микросекунд.
3. Команда `show interfaces fa0/0` выводят задержку в 1230 микросекунд.

Пример 10.15. Настройка задержки интерфейса

```
Yosemite# show interfaces fa0/0
FastEthernet0/0 is up, line protocol is up
  Hardware is Gt96k FE, address is 0013.197b.5026 (bia 0013.197b.5026)
  Internet address is 10.1.2.252/24
MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
! Строки опущены для краткости
Yosemite# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Yosemite(config)# interface fa0/0
Yosemite(config-if)# delay 123
Yosemite(config-if)# ^Z

Yosemite# show interfaces fa0/0
FastEthernet0/0 is up, line protocol is up
  Hardware is Gt96k FE, address is 0013.197b.5026 (bia 0013.197b.5026)
  Internet address is 10.1.2.252/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 1230 usec,
! Строки опущены для краткости
```

Автоматическое суммирование и несмежные классовые сети

Прежние протоколы маршрутизации, а именно RIP 1 и IGRP, были *классовыми протоколами маршрутизации*. Данный термин происходит из того факта, что эти протоколы маршрутизации должны были уделить больше внимания деталям сети классе A, B и C, частично из-за простоты самого протокола маршрутизации.

Эти устаревшие классовые протоколы маршрутизации требовали также больше внимания и осторожности при проектировании подсетей, чтобы избежать проблем,

связанных с несмежной классовой сетью. Когда классовая сеть становилась несмежной, упрощенные протоколы маршрутизации отказывали из-за необходимости применения *автоматического суммирования* (autosummarization).

В настоящее время большинство предприятий используют протоколы OSPF, или EIGRP, или в редких случаях протокол RIP 2. Все эти протоколы маршрутизации бесклассовые. В результате эти более новые протоколы маршрутизации можно настроить так, чтобы старая проблема с несмежными классовыми сетями не возникала вообще.

Хотя современные версии операционной системы IOS используют стандартные настройки, позволяющие игнорировать эту проблему, протокол EIGRP обладает средством автоматического суммирования, требует от сетевого инженера знаний о старой проблеме несмежной сети. Просто на всякий случай, на нескольких следующих страницах обсуждаются автоматическое суммирование и проблемы маршрутизации, которые могут случиться в результате.

ВНИМАНИЕ!

В реальных сетях использования автоматического суммирования, как правило, стараются избегать.

Автоматическое суммирование по границе классовой сети

Протокол маршрутизации, использующий автоматическое суммирование, автоматически создает суммарный маршрут при определенных условиях. В частности, когда маршрутизатор находится на границе между классовыми сетями (т.е. с одними интерфейсами в одной сети класса A, B или C и другими интерфейсами в другой сети класса A, B или C), он суммирует маршруты. В итоге все маршруты к хостам в одной классовой сети объединяются в единый маршрут ко всей сети класса A, B или C. Или более формально:

Ключевая тема

Определение автоматического суммирования

Когда связанные с подсетями в сети X маршруты анонсирует интерфейс, IP-адрес которого не принадлежит сети X, все эти маршруты анонсируются как один маршрут ко всей сети X класса A, B или C.

Как обычно, пример сделает концепцию намного понятней. Рассмотрим рис. 10.9, на котором представлены две рабочие сети: 10.0.0.0 и 172.16.0.0. У маршрутизатора R3 есть четыре (подключенных) маршрута к подсетям сети 10.0.0.0 справа и один интерфейс слева, подключенный к другой классовой сети — сети 172.16.0.0 класса B. В результате маршрутизатор R3 с разрешенным автоматическим суммированием будет суммировать маршрут для всей сети 10.0.0.0 класса A.

Рассмотрим этапы, приведенные на рисунке.

1. Подкоманда EIGRP `auto-summary` разрешила на маршрутизаторе R3 автоматическое суммирование.
2. Поскольку канал связи с маршрутизатором R2 подключается к другой сети (172.16.0.0), маршрутизатор R3 анонсирует маршрут для всей сети 10.0.0.0 класса A вместо набора маршрутов для каждой подсети в сети 10.0.0.0.

3. Маршрутизатор R2 изучает один маршрут, т.е. маршрут к сети 10.0.0.0/8, представляющий всю сеть 10.0.0.0, при следующем транзитном маршрутизаторе R3.

Пример 10.16 демонстрирует вывод команды `show ip route` на маршрутизаторе R2, подтверждая результат наличия параметра `auto-summary` на маршрутизаторе R3.

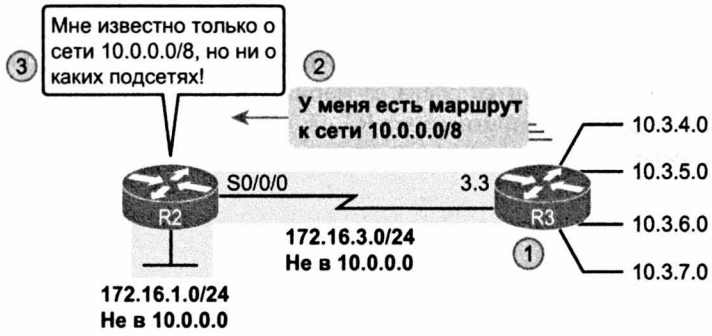


Рис. 10.9. Автоматическое суммирование

Пример 10.16. Маршрутизатор R2 с единым маршрутом ко всей сети 10.0.0.0

```
R2# show ip route eigrp
! Строки опущены для краткости

D      10.0.0.0/8 [90/2297856] via 172.16.3.3, 00:12:59, Serial0/0/0
```

Обратите внимание, что сам по себе параметр `auto-summary` проблем не вызывает. В проекте на рис. 10.9 и в выводе команды в примере 10.16 никаких проблем нет. Маршрутизатор R2 способен перенаправить пакеты ко всем подсетям в сети 10.0.0.0, используя выделенный суммарный маршрут, а маршрутизатор R3 перенаправит их далее к подсетям.

Несмежные классовые сети

Автоматическое суммирование не создает проблем, пока полученная в итоге сеть является смежной (непрерывной), а не несмежной. Жители Соединенных Штатов могут оценить концепцию несмежной сети по аналогии с термином *смежные 48* (contiguous 48), обозначающем 48 американских штатов кроме Аляски и Гавайев. Чтобы добраться до Аляски из любого другого из 48 штатов, придется проехать по другой стране (Канаде), поэтому Аляска не смежна с 48 штатами. Другими словами, она является несмежной.

Чтобы лучше понять смысл терминов *смежный* (contiguous) и *несмежный* (discontiguous) в контексте сетей, обратимся к двум следующим формальным определениям смежной и несмежной классовой сети.

Определение смежных и несмежных сетей

Ключевая тема

- *Смежная сеть* (contiguous network). Классовая сеть, в которой передаваемые между любыми парами подсетей пакеты способны следовать только через

подсети той же классовой сети без необходимости проходить через подсети любой другой классовой сети.

- *Несмежная сеть* (discontiguous network). Классовая сеть, в которой пакеты, передаваемые между по крайней мере одной парой подсетей, вынуждены проходить через подсети другой классовой сети.

На рис. 10.10 представлена расширенная версия объединенной сети, показанной на рис. 10.9, чтобы получился пример несмежной сети 10.0.0.0. В этом проекте часть подсетей сети 10.0.0.0 находится слева от маршрутизатора R1, тогда как другие все еще остаются справа от маршрутизатора R3. Пакеты, передаваемые из подсетей слева подсетям справа, должны пройти через подсети сети 172.16.0.0 класса B.

Ключевая тема

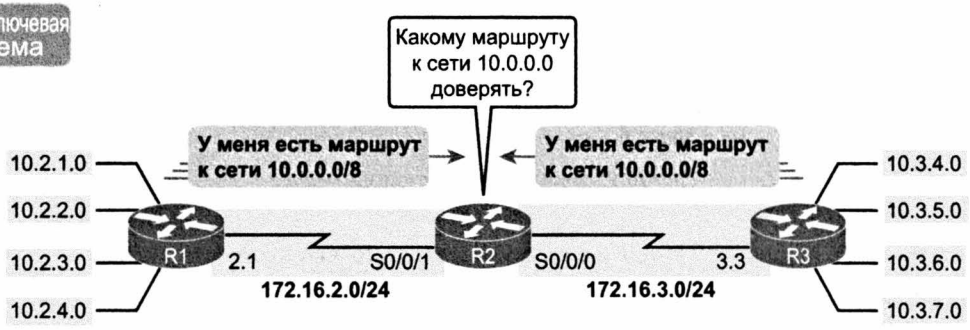


Рис. 10.10. Несмежная сеть 10.0.0.0

Автоматическое суммирование создает проблемы на таких маршрутизаторах, как R2, находящихся полностью вне несмежной сети, ведь они не будут знать, куда именно перенаправлять пакеты к несмежной сети. Идея анонсирования маршрутизатору R2 (в середине сети) маршрута к сети 10.0.0.0/8 маршрутизаторами R1 и R3 представлена на рис. 10.10. Пример 10.17 демонстрирует результирующие маршруты на маршрутизаторе R2.

Пример 10.17. Таблица маршрутизации: автоматическое суммирование привело к проблеме маршрутизации с несмежной сетью 10.0.0.0

```
R2# show ip route | section 10.0.0.0
D      10.0.0.0/8 [90/2297856] via 172.16.3.3, 00:00:15, Serial0/0/0
                  [90/2297856] via 172.16.2.1, 00:00:15, Serial0/0/1
```

Как показано в примере 10.17, у маршрутизатора R2 теперь есть два маршрута к сети 10.0.0.0/8: один указывает влево на маршрутизатор R1, другой — вправо на маршрутизатор R3. Маршрутизатор R2 использует свою обычную логику балансировки нагрузки, ведь с его точки зрения эти два маршрута — просто маршруты равной стоимости к тому же получателю: всей сети 10.0.0.0. Иногда маршрутизатор R2 перенаправляет пакет правильному получателю, а иногда нет.

У этой проблемы есть два решения. Старомодное решение подразумевает создание плана IP-адресации без несмежных классовых сетей. Другое решение — отказаться от использования автоматического суммирования, либо используя изначальные параметры протокола EIGRP, либо отключив его подкомандой EIGRP `no`

`auto-summary`. В примере 10.18 показана полученная таблица маршрутизации на маршрутизаторе R2 для маршрутов к сети 10.0.0.0 после применения команды `no auto-summary` на маршрутизаторах R1 и R3.

Пример 10.18. Бесклассовый протокол маршрутизации без автоматического суммирования допускает несмежные сети

```
R2# show ip route 10.0.0.0
Routing entry for 10.0.0.0/24, 8 known subnets
  Redistributing via eigrp 1
D     10.2.1.0 [90/2297856] via 172.16.2.1, 00:00:12, Serial0/0/1
D     10.2.2.0 [90/2297856] via 172.16.2.1, 00:00:12, Serial0/0/1
D     10.2.3.0 [90/2297856] via 172.16.2.1, 00:00:12, Serial0/0/1
D     10.2.4.0 [90/2297856] via 172.16.2.1, 00:00:12, Serial0/0/1
D     10.3.4.0 [90/2297856] via 172.16.3.3, 00:00:06, Serial0/0/0
D     10.3.5.0 [90/2297856] via 172.16.3.3, 00:00:06, Serial0/0/0
D     10.3.6.0 [90/2297856] via 172.16.3.3, 00:00:06, Serial0/0/0
D     10.3.7.0 [90/2297856] via 172.16.3.3, 00:00:06, Serial0/0/0
```

Обзор

Резюме

- Команда EIGRP `network` допускает две разновидности синтаксиса: один с шаблоном маски в конце и один без него.
- Команда `network` указывает маршрутизатору находить собственные интерфейсы с адресами в данной сети и разрешать протокол EIGRP на этих интерфейсах.
- Операционная система IOS предоставляет вторую версию команды EIGRP `network`, позволяющую использовать шаблон маски, чтобы инженер мог точно установить правильное значение IP-адреса интерфейса.
- Как только маршрутизатор разрешает протокол EIGRP на интерфейсе, он пытается обнаруживать соседние маршрутизаторы, прослушивая сообщения EIGRP Hello.
- Как только маршрутизаторы EIGRP становятся соседями, они начинают обмениваться информацией о маршрутизации, сохранять ее в свих таблицах топологии и вычислять по ней свои наилучшие маршруты IPv4.
- Резервный маршрут ускоряет конвергенцию при отказе оптимального маршрута, поскольку резервный маршрут применяется немедленно.
- Протокол EIGRP анонсирует разные компоненты метрики, а затем использует некоторые из них для вычисления составной метрики.
- Протокол EIGRP базирует свою составную метрику на минимальной ширине полосы пропускания канала связи на маршруте.
- Протокол EIGRP позволяет поместить в таблицу маршрутизации IPv4 несколько маршрутов с равными или почти равными метрикам.
- Маршруты, не являющиеся ни оптимальными, ни резервными, не добавляются в таблицу маршрутизации IP независимо от параметра вариации, поскольку это может создать петлевые маршруты.
- Протокол EIGRP обладает средством автоматического суммирования, требующим от сетевого инженера знаний о старой проблеме несмежной сети.
- Протокол маршрутизации, использующий автоматическое суммирование, автоматически создает суммарный маршрут при определенных условиях.

Контрольные вопросы

Ответьте на эти вопросы. Ответы можно найти на последней странице главы. Полное объяснение ответов приведено в приложении B на веб-сайте.

1. Какая из следующих команд `network`, после команды `router eigrp 1`, указывает маршрутизатору начать использовать протокол EIGRP на интерфейсах с IP-адресами 10.1.1.1, 10.1.100.1 и 10.1.120.1? (Выберите два ответа.)

   А) `network 10.0.0.0`.

   Б) `network 10.1.1x.0`.

В) `network 10.0.0.0 0.255.255.255.`

Г) `network 10.0.0.0 255.255.255.0.`

2. Маршрутизаторы R1 и R2 подключены к той же сети VLAN с IP-адресами 10.0.0.1 и 10.0.0.2 соответственно. На маршрутизаторе R1 введены команды `router eigrp 99` и `network 10.0.0.0`. Какая из следующих команд могла бы быть частью конфигурации EIGRP на маршрутизаторе R2, гарантирующей, что эти два маршрутизатора станут соседями и обменяются маршрутами? (Выберите два ответа.)

   А) `network 10.`

   Б) `network 10.0.0.1 0.0.0.0.`

   В) `network 10.0.0.2 0.0.0.0.`

   Г) `network 10.0.0.0.`

3. Какое значение символа в выводе команды `show ip route` означает, что маршрут был изучен по протоколу EIGRP?

   А) E.

   Б) I.

   В) G.

   Г) D.

4. Внимательно рассмотрите следующий отрывок вывода команды `show` на маршрутизаторе R1:

```
EIGRP-IPv4 Neighbors for AS(1)
H Address Interface Hold Uptime SRTT RTO Q Seq
          (sec)    (ms)   Cnt Num
1 10.1.4.3 Se0/0/1  13 00:05:49 2  100 0 29
0 10.1.5.2 Se0/0/0  12 00:05:49 2  100 0 39
```

   Какой из следующих ответов справедлив для данного маршрутизатора на основании этого вывода?

   А) Адрес 10.1.4.3 идентифицирует работающее соседнее устройство на основании текущего идентификатора маршрутизатора соседа EIGRP.

   Б) Адрес 10.1.5.2 идентифицирует маршрутизатор, способный или неспособный стать соседом EIGRP в некоторый момент после того, как оба маршрутизатора проверят все требования к соседям.

   В) Адрес 10.1.5.2 идентифицирует работающее соседнее устройство на основании IP-адреса интерфейса соседа на канале связи между маршрутизатором R1 и этим соседом.

   Г) Адрес 10.1.4.3 идентифицирует собственный IP-адрес маршрутизатора R1 на интерфейсе S0/0/1.

5. Исследуйте следующий отрывок вывода на интерфейсе CLI маршрутизатора:

```
P 10.1.1.0/24, 1 successors, FD is 2172416
  via 10.1.6.3 (2172416/28160), Serial0/1
  via 10.1.4.2 (2684416/2284156), Serial0/0
  via 10.1.5.4 (2684416/2165432), Serial1/0
```

   Что из следующего идентифицирует IP-адрес следующей транзитной точки перехода на резервном маршруте?

А) 10.1.6.3.

Б) 10.1.4.2.

В) 10.1.5.4.

Г) Вывод команды не позволяет определить его.

6. Процессу EIGRP на маршрутизаторе R1 известно о трех возможных маршрутах к подсети 1. Один из маршрутов оптимальный, один резервный. Маршрутизатор R1 не использует команду `variance` для балансировки нагрузки при неравной стоимости. Какие из следующих команд выводят информацию о резервном маршруте, включая его метрику, топологическую информацию EIGRP или маршрут IPv4?

   А) `show ip eigrp topology`.

   Б) `show ip eigrp database`.

   В) `show ip route eigrp`.

   Г) `show ip eigrp interfaces`.

7. У маршрутизатора R1 есть четыре маршрута к подсети 2. У одного маршрута, оптимального, есть метрика 100, а у резервного маршрута метрика 350. У двух других есть метрики 450 и 550. Конфигурация EIGRP маршрутизатора R1 включает команду `variance 5`. Выберите маршрут с самой высокой метрикой к подсети 2, который будет выведен командой `show ip route eigrp` на маршрутизаторе R1.

   А) Оптимальный маршрут (метрика 100).

   Б) Резервный маршрут (метрика 350).

   В) Маршрут с метрикой 450.

   Г) Маршрут с метрикой 550.

Ключевые темы

Повторите все ключевые темы данной главы, отмеченные пиктограммой "Ключевая тема". Ключевые темы и соответствующие им страницы перечислены в табл. 10.2.

Таблица 10.2. Ключевые темы главы 10

Элемент	Описание	Страница
Список	Последовательность настройки протокола EIGRP	343
Прим. 10.5	Просмотр заданных команд network при помощи команды show ip protocols	349
Список	Правила выбора протоколом EIGRP идентификатора маршрутизатора	349
Рис. 10.4	Поля в выводе команды show ip eigrp topology	354
Рис. 10.7	Идентификация резервного маршрута	357
Список	Вариация метрики в протоколе EIGRP	362
Определение	Определение автоматического суммирования	364
Список	Определение смежных и несмежных сетей	365
Рис. 10.10	Несмежная сеть 10.0.0.0	366

Заполните таблицы и списки по памяти

Распечатайте приложение Г с веб-сайта или его раздел, относящийся к этой главе, и заполните таблицы и списки по памяти. В приложении Д приведены заполненные таблицы и списки для самоконтроля.

Ключевые термины

После первого прочтения главы попытайтесь дать определения следующим ключевым терминам. Но не расстраивайтесь, если не все получится сразу, в главе 22 описано, как использовать эти термины на завершающем этапе подготовки к экзамену.

условие резервирования (feasibility condition), оптимальное расстояние (Feasible Distance — FD), резервный маршрут (feasible successor), анонсируемое расстояние (reported distance), оптимальный маршрут (successor), балансировка нагрузки с неодинаковыми стоимостями (unequal-cost load balancing), вариация (variance), автоматическое суммирование (autosummary), несмежная сеть (discontiguous network)

Таблицы команд

Хоть и не обязательно заучивать информацию из таблиц данного раздела, ниже приведен список команд конфигурации и пользовательских команды главы. Фактически команды стоит запомнить, чтобы лучше понять содержимое главы и выполнить задачи по подготовке к экзамену. Чтобы проверить, насколько хорошо вы запомнили команды, закройте левую сторону таблицы листом бумаги, читайте описания с правой стороны и пытайтесь вспомнить команду.

Таблица 10.3. Конфигурационные команды главы 10

Команда	Описание
`router eigrp` *`номер_автономной_системы`*	Глобальная команда, переводящая пользователя в режим конфигурации EIGRP для выбранного номера автономной системы (ASN)
`network` *`номер_сети`* [*`шаблон_маски`*]	Подкоманда маршрутизатора EIGRP, разрешающая протокол EIGRP на этих интерфейсах и соответствующая либо всем интерфейсам в классовой сети, либо подмножеству интерфейсов, на основании шаблона маски в стиле ACL
`maximum-paths` *`количество_путей`*	Подкоманда маршрутизатора, определяющая максимальное количество маршрутов равной стоимости, которые могут быть добавлены в таблицу маршрутизации
`variance` *`множитель`*	Подкоманда маршрутизатора, определяющая множитель EIGRP, используемый для определения, достаточно ли метрика маршрута FS близка к метрике оптимального маршрута, чтобы они считались равными
`bandwidth` *`ширина_полосы_пропускания`*	Подкоманда интерфейса, непосредственно устанавливающая ширину полосы пропускания интерфейса (Кбит/с)

Окончание табл. 10.3

Команда	Описание
`delay` *значение_задержки*	Подкоманда интерфейса для установки значения задержки интерфейса шагом в десяток микросекунд
`ip hello-interval eigrp` *номер_автономной_системы значение_таймера*	Подкоманда интерфейса, устанавливающая интервал Hello EIGRP для данного процесса EIGRP
`ip hold-time eigrp` *номер_автономной_системы значение_таймера*	Подкоманда интерфейса, устанавливающая время задержки EIGRP для данного интерфейса
`maximum-paths` *количество_путей*	Подкоманда маршрутизатора, определяющая максимальное количество маршрутов равной стоимости, которые могут быть добавлены в таблицу маршрутизации
`[no] auto-summary`	Подкоманда маршрутизатора, отключающая (при помощи параметра `no`) или включающая автоматическое суммирование маршрутов в границе классовой сети
`passive-interface` *тип номер*	Подкоманда маршрутизатора, делающая интерфейс пассивным интерфейсом OSPF, а значит, процесс OSPF не будет формировать соседские отношения с соседними маршрутизаторами, доступными на данном интерфейсе
`passive-interface default`	Подкоманда OSPF, изменяющая стандартное значение OSPF для интерфейсов с пассивного на активный
`no passive-interface` *тип номер*	Подкоманда OSPF, переводящая интерфейс или субинтерфейс в активное состояние OSPF

Таблица 10.4. Команды EXEC главы 10

Команда	Описание
`show ip eigrp interfaces`	Выводит по одной строке на каждый интерфейс, на котором разрешен протокол EIGRP, но он не сделан пассивным командой конфигурации `passive-interface`
`show ip eigrp interfaces` *тип номер*	Выводит статистику по интерфейсам, на которых разрешен протокол EIGRP, но он не сделан пассивным командой конфигурации `passive-interface`
`show ip eigrp interfaces detail` [*тип номер*]	Выводит подробности конфигурации и статистику для всех или только для выбранных интерфейсов, которые разрешены, но не пассивны
`show ip protocols`	Отображает параметры протокола маршрутизации и текущие значения таймеров
`show ip eigrp neighbors`	Выводит соседей EIGRP и их состояние
`show ip eigrp neighbors` *тип номер*	Выводит соседей EIGRP, доступных для заданного интерфейса
`show ip eigrp topology`	Выводит содержимое таблицы топологии EIGRP, включая оптимальные и резервные маршруты

Окончание табл. 10.4

Команда	Описание
`show ip eigrp topology` *подсеть/префикс*	Выводит подробную топологическую информацию о выбранной подсети
`show ip eigrp topology | section` *подсеть*	Выводит подмножество команд `show ip eigrp topology` (только раздел для выбранного идентификатора подсети)
`show ip route`	Выводит все маршруты IPv4
`show ip route eigrp`	Выводит маршруты в таблице маршрутизации IPv4, изученные по протоколу EIGRP
`show ip route` *ip-адрес маска*	Выводит подробное описание маршрута для выбранной подсети/маски
`show ip route | section` *подсеть*	Выводит подмножество команд `show ip route` (только раздел для выбранного идентификатора подсети)
`debug eigrp fsm`	Выводит изменения в оптимальных маршрутах EIGRP и маршрутах FS

Ответы на контрольные вопросы:

1 А и В. 2 В и Г. 3 Г. 4 В. 5 В. 6 А. 7 Б.

Глава 11

Поиск и устранение неисправностей протоколов маршрутизации IPv4

Процесс локализации проблемы при поиске и устранении возможной проблемы протокола маршрутизации IPv4 имеет смысл начать с интерфейсов, а затем перейти к соседям. Конфигурация протокола маршрутизации определяет интерфейсы, на которых маршрутизатор должен использовать протокол маршрутизации. После выявления этих интерфейсов сетевой инженер может просмотреть соседей, подключенных к каждому интерфейсу маршрутизатора, и найти тех из них, которые должны существовать, но не существуют.

В данной главе речь пойдет о проблемах, связанных с этими двумя логическими ветвями: на каких интерфейсах маршрутизатора должен быть разрешен протокол маршрутизации и какие соседские отношения должен формировать каждый маршрутизатор. Материал главы основан на конфигурации, обсуждаемой в главах 8–10 этой книги, и основное внимание уделено поиску ошибок конфигурации с использованием команд `show` и `debug`.

Сначала рассматриваются общие понятия, связанные с поиском и устранением проблем протокола маршрутизации. В следующем разделе рассматриваются проблемы, связанные с поиском интерфейса, на котором маршрутизатор разрешает выполнение протокола маршрутизации. Завершается глава разделом, посвященным соседским отношениям по протоколу маршрутизации. Кроме того, во всех разделах попеременно рассматриваются расширенный протокол маршрутизации внутреннего шлюза (EIGRP) и открытый протокол поиска первого кратчайшего маршрута (OSPF).

В этой главе рассматриваются следующие экзаменационные темы

Поиск и устранение неисправностей

Поиск и устранение проблем OSPF

- Соседские отношения
- Таймеры Hello и Dead
- Область OSPF
- Максимальный блок передачи данных интерфейса
- Типы сетей
- Состояние соседей
- База данных топологии OSPF

Поиск и устранение проблем EIGRP

- Соседские отношения
- Номер AS
- Балансировка нагрузки
- Разделенный диапазон

Основные темы

Методы поиска и устранения проблем в протоколах маршрутизации

Основная задача любого протокола маршрутизации — заполнить таблицу маршрутизации устройства актуальными оптимальными маршрутами, поэтому процесс поиска и устранения неисправностей обычно начинается с таблицы маршрутизации. Зная базовую информацию о структуре сети, маршрутизаторах в сети, IP-адресах и масках их интерфейсов, а также какой протокол маршрутизации используется, сетевой инженер может рассчитать адреса сетей и подсетей, которые должны присутствовать в таблицах маршрутизации устройств, и указать адреса транзитных устройств на маршрутах к таким подсетям. Например, на рис. 11.1 показана сеть, состоящая из шести подсетей. В таблице маршрутизации маршрутизатора R1 должны присутствовать все шесть подсетей, три из которых напрямую подключены к устройству, информация о двух подсетях получена от маршрутизатора R2 (172.16.4.0/24 и 172.16.5.0/24), а об одной — от маршрутизатора R3 (172.16.6.0/24).

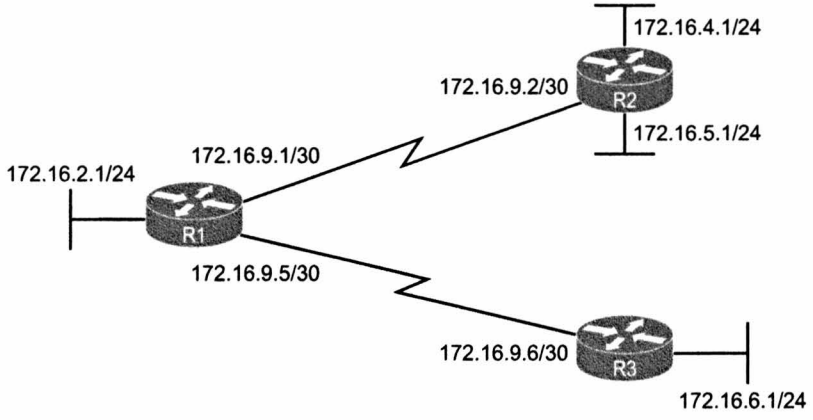


Рис. 11.1. Сеть с шестью подсетями

Итак, один из возможных алгоритмов поиска и устранения неисправностей — анализ схемы сети, анализ таблиц маршрутизации и поиск недостающих маршрутов. Если один или более маршрутов отсутствуют в таблице маршрутизации, следует проверить, получил ли маршрутизатор какую-либо информацию о них от транзитных (т.е. соседних) устройств на маршруте. Дальнейшие действия существенно отличаются в зависимости от того, какая проблема возникла: маршрутизатор не может обнаружить соседние устройства или обнаружил, но не может получить правильные маршруты.

Например, представим себе ситуацию, когда маршрутизатор R1 (см. рис. 11.1) обнаружил маршрут к подсети 172.16.4.0/24, но не обнаружил маршрут к подсети 172.16.5.0/24. Вполне очевидно, что данный маршрутизатор успешно обнаружил маршрутизатор R2. Основная причина неправильной работы в данном случае может

быть связана как с самим протоколом маршрутизации, так и с другими протоколами. Например, интерфейс локальной сети маршрутизатора R1 может быть в нерабочем состоянии. Если же у устройства R1 нет маршрутов как к сети 172.16.4.0/24, так и к сети 172.16.5.0/24, то, скорее всего, такая ситуация сигнализирует о том, что есть проблема в установлении связи с устройством R2.

Поиск и устранение неисправностей, связанных с протоколами маршрутизации в реальных сетях, могут быть неимоверно сложными, много сложнее, чем в самых трудных заданиях экзамена CCNA. Описать наиболее полные рекомендации в рамках данной книги практически невозможно, поэтому ниже представлен самый общий и достаточно поверхностный метод устранения проблем, который, тем не менее, будет полезен при сдаче экзамена.

Если экзаменационный вопрос связан с поиском ошибок в протоколе маршрутизации, то следует отметить, что наиболее общие промахи в конфигурации можно локализовать с помощью следующего процесса даже без использования команды `show running-config`. Процесс состоит из трех основных этапов, описанных ниже.

Этап 1 Изучите структуру сети, чтобы определить, на каких интерфейсах должен быть запущен протокол маршрутизации и какие соседние устройства должны быть обнаружены маршрутизатором

Этап 2 Проверьте, включен ли протокол маршрутизации на нужных интерфейсах (с использованием информации этапа 1). Если протокол не включен, исправьте эту ошибку

Этап 3 Проверьте, обнаружило ли устройство все соседние маршрутизаторы. Если нет, то исправьте эту ошибку

Например, как отмечено звездочками на рис. 11.2, каждый маршрутизатор должен разрешить протокол маршрутизации на каждом из представленных на рисунке интерфейсов. Кроме того, соседские отношения протокола маршрутизации должны быть сформированы между маршрутизаторами R1 и R2, а также R1 и R3, но не между маршрутизаторами R2 и R3.

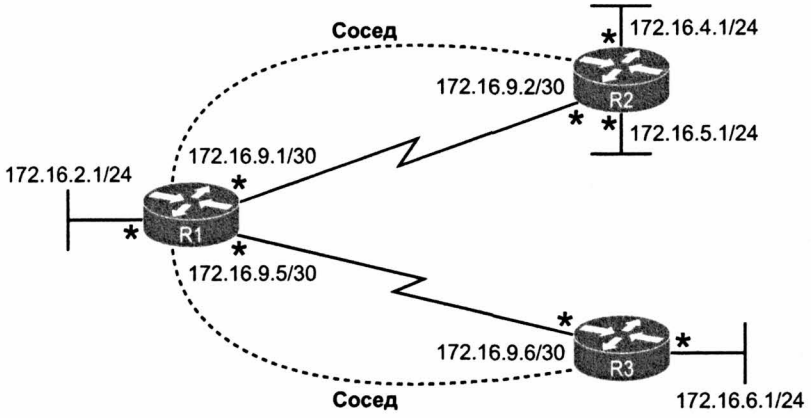


Рис. 11.2. Интерфейсы, на которых разрешен протокол маршрутизации, и соседские отношения

На настоящий момент представленные на рис. 11.2 концепции должны быть уже очевидны, а в данной главе обсуждается, как некоторые из наиболее распространенных ошибок конфигурации могут повлиять на интерфейсы, используемые протоколом маршрутизации, а также формирует ли протокол маршрутизации соседские отношения.

Интерфейсы, участвующие в маршрутизации

В этом разделе описан второй этап процесса поиска и устранения неисправностей, описанного в начале главы: проверка интерфейсов, на которых включен протокол маршрутизации. В обоих протоколах, OSPF и EIGRP, интерфейсы добавляются в процесс маршрутизации с помощью команд `network` в режиме конфигурирования протокола маршрутизации. Для любых интерфейсов, адреса которых попадают в диапазон, указанный командой `network`, устройство выполняет следующие действия.

Ключевая тема **Два действия, выполняемые протоколами маршрутизации EIGRP и OSPF при их включении на интерфейсе**

- Пытается обнаружить соседние устройства в подсети, подключенной к интерфейсу.
- Анонсирует подсеть, настроенную на интерфейсе.

Чтобы устройство не пыталось найти соседние маршрутизаторы, для интерфейса может быть указана команда `passive-interface` в режиме конфигурирования протокола маршрутизации. Тем не менее устройство все равно будет анонсировать в сообщениях протокола маршрутизации подсеть интерфейса.

С помощью команд группы `show` можно определить, какие интерфейсы участвуют в протоколах маршрутизации OSPF и EIGRP. В частности, команда `show ip eigrp interfaces` выводит информацию обо всех интерфейсах, участвующих в процессах протокола EIGRP, для которых не указана команда `passive-interface`. С помощью команды `show ip protocols`, даже без привилегированного режима, можно быстро определить, какие сети были указаны в командах `network` и какие протоколы маршрутизации запущены на маршрутизаторе, а также получить список интерфейсов, для которых указана команда `passive-interface`.

Сравнив вывод двух указанных команд, можно определить полный список интерфейсов, на которых используется протокол маршрутизации, и узнать, какие из них работают в пассивном режиме (`passive-interface`). В протоколе маршрутизации OSPF можно использовать немного отличающуюся команду, `show ip ospf interface brief`, которая также покажет список всех интерфейсов OSPF (в том числе и тех, которые работают в пассивном режиме). Используя эту команду, наряду со списком выведенных командой `show ip protocols` пассивных интерфейсов, можно снова выявить все интерфейсы с разрешенным протоколом OSPF, а также все пассивные интерфейсы.

В табл. 11.1 перечислены все описанные команды.

Таблица 11.1. Ключевые команды для поиска интерфейсов, участвующих в протоколе маршрутизации

Ключевая тема

Команда	Описание	Выводит ли пассивные интерфейсы?
`show ip eigrp interfaces`	Выводит список интерфейсов, в которых включен протокол маршрутизации EIGRP (на основании команд `network` в конфигурации), за исключением интерфейсов, работающих в пассивном режиме	Нет
`show ip ospf interface brief`	Выводит список интерфейсов, в которых включен протокол маршрутизации OSPF (на основании команд `network` в конфигурации), в том числе интерфейсы, работающие в пассивном режиме	Да
`show ip protocols`	Выводит список протоколов маршрутизации, настроенных в устройстве, список их характеристик и содержимое команд `network` для каждого протокола маршрутизации, а также интерфейсы, работающие в пассивном режиме	Да

ВНИМАНИЕ!

Все указанные в табл. 11.1 команды выводят список интерфейсов независимо от их текущего состояния, фактически отображая настройки, заданные командами `network` и `passive-interface`.

Итак, необходимый для данного этапа набор команд представлен в табл. 11.1. Теперь рассмотрим примеры их использования для протоколов EIGRP и OSPF.

Поиск и устранение неисправностей интерфейсов в протоколе EIGRP

В этом разделе приведено несколько примеров команд для сети, представленной на рис. 11.3.

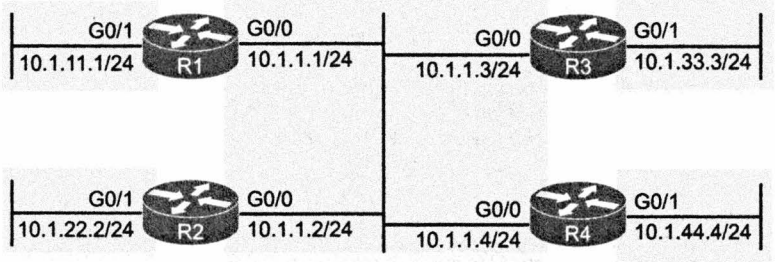


Рис. 11.3. Схема сети для иллюстрации команд процесса поиска и устранения неисправностей в протоколах EIGRP и OSPF

В этом примере показаны четыре маршрутизатора, которые настроены следующим образом.

- Для маршрутизаторов R1 и R2 на интерфейсах локальной сети указана правильная конфигурация.
- На маршрутизаторе R3 протокол EIGRP не включен для интерфейса G0/1 (по ошибке).
- На маршрутизаторе R4 сетевой инженер собирался ввести команду `passive-interface G0/1`, поскольку в сегменте локальной сети нет других маршрутизаторов кроме R4, но ошибся и ввел `passive-interface G0/0`.

Данный пример начинается с детального рассмотрения работы маршрутизаторов R1 и R2, а затем переходит к обсуждению проблем, связанных с маршрутизаторами R3 и R4.

Рассмотрение рабочих интерфейсов EIGRP

Команды `show` в примерах 11.1 и 11.2 выводят конфигурацию маршрутизаторов R1 и R2 соответственно. Команды `show ip eigrp interfaces` и `show ip protocols` выводят соответственно конфигурацию и маршруты, изученные по протоколу EIGRP на каждом маршрутизаторе.

Пример 11.1. EIGRP Проблемы интерфейсов EIGRP: команды на маршрутизаторе R1

```
R1# show running-config
! Показаны только важные для данного примера команды
router eigrp 99
  network 10.0.0.0
!
R1# show ip eigrp interfaces
EIGRP-IPv4 Interfaces for AS(99)
              Xmit Queue   PeerQ        Mean Pacing Time Multicast   Pendin
Interfac Peers Un/Reliable Un/Reliable SRTT Un/Reliable Flow Timer Routes
Gi0/0    3     0/0         0/0         2    0/0         50         0
Gi0/1    0     0/0         0/0         0    0/0         0          0

R1# show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "eigrp 99"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP-IPv4 Protocol for AS(99)
    Metric weight K1=1, K2=0, K3=1, K4=0, K5=0
    NSF-aware route hold timer is 240
    Router-ID: 1.1.1.1
    Topology : 0 (base)
      Active Timer: 3 min
      Distance: internal 90 external 170
      Maximum path: 4
      Maximum hopcount 100
      Maximum metric variance 1

Automatic Summarization: disabled
Maximum path: 4
```

```
Routing for Networks:
  10.0.0.0
Routing Information Sources:
  Gateway    Distance    Last Update
  10.1.1.2   90          09:55:51
  10.1.1.3   90          00:02:00
Distance: internal 90 external 170

R1# show ip route eigrp
! Легенда, опущена для краткости

     10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
D       10.1.22.0/24 [90/30720] via 10.1.1.2, 00:00:40, GigabitEthernet0/0
```

Пример 11.2. Проблемы интерфейсов EIGRP: команды на маршрутизаторе R2

```
R2# show running-config
! Показаны только важные для данного примера команды
router eigrp 99
  network 10.1.0.0 0.0.255.255

R2# show ip eigrp interfaces
EIGRP-IPv4 Interfaces for AS(99)
              Xmit Queue   PeerQ        Mean Pacing Time Multicast   Pendin
Interface Peers Un/Reliable Un/Reliable SRTT Un/Reliable Flow Timer Routes
Gi0/0     2     0/0         0/0         1    0/1         50         0
Gi0/1     0     0/0         0/0         0    0/0         0          0

R2# show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "eigrp 99"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Default networks flagged in outgoing updates
Default networks accepted from incoming updates
EIGRP-IPv4 Protocol for AS(99)
  Metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  NSF-aware route hold timer is 240
  Router-ID: 2.2.2.2
  Topology : 0 (base)
    Active Timer: 3 min
    Distance: internal 90 external 170
    Maximum path: 4
    Maximum hopcount 100
    Maximum metric variance 1

Automatic Summarization: disabled
Maximum path: 4
Routing for Networks:
  10.1.0.0/16
Routing Information Sources:
  Gateway    Distance    Last Update
  10.1.1.3   90          00:02:30
  10.1.1.1   90          09:56:20
Distance: internal 90 external 170
```

```
R2# show ip route eigrp
! Легенда, опущена для краткости
     10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
D       10.1.11.0/24 [90/30720] via 10.1.1.1, 00:03:25, GigabitEthernet0/0
```

В выводе команды `show ip eigrp interfaces` для маршрутизаторов R1 и R2 можно увидеть, что в них запущен протокол маршрутизации EIGRP с номером автономной системы 99, и он включен на интерфейсах G0/0 и G0/1 обоих маршрутизаторов. Эта команда позволяет определить, на каких интерфейсах включен протокол маршрутизации, за исключением тех, которые работают в пассивном режиме.

В выводе команды `show ip protocols` выделены строки, представляющие наибольший интерес. Выделенная информация позволяет определить, какие команды `network` были использованы. Команда `show ip protocols` выводит под заголовком "`Routing for Networks`" по одной строке для каждой введенной команды `network`. Вывод примера 11.1 свидетельствует о наличии на маршрутизаторе R1 команды конфигурации `network 10.0.0.0` (в начале примера), а пример для маршрутизатора R2, "10.1.0.0/16", — наличие на нем команды `network 10.1.0.0 0.0.255.255`.

Рассмотрение проблемных интерфейсов EIGRP

Далее рассматриваются проблемы конфигурации на маршрутизаторах R3 и R4.

В примере 11.2 показаны команды, позволяющие определить проблемы на маршрутизаторе R3. В конце вывода команды `show ip protocols` для маршрутизатора R2 указаны два источника маршрутной информации: 10.1.1.1 (R1) и 10.1.1.3 (R3). Тем не менее устройство R2 обнаружило только один маршрут EIGRP (10.1.11.0/24), как показано в выводе команды `show ip route eigrp`. Если бы все в сети было правильно, маршрутизатор R2 обнаружил бы два маршрута EIGRP, по одному для каждой из подсетей, показанных на рис. 11.3.

Пример 11.3 демонстрирует первопричину проблем на маршрутизаторе R3. Команда `show ip eigrp interfaces` на маршрутизаторе R3 выводит интерфейс G0/0, а не G0/1, поэтому проблема может быть связана с тем, что протокол EIGRP был настроен на интерфейсе G0/1. Конфигурация вверху примера сообщает первопричину: неправильная команда `network`, не разрешающая протокол EIGRP на интерфейсе G0/1 маршрутизатора R3.

Пример 11.3. Проблемы EIGRP на маршрутизаторе R3

```
R3# show running-config
! Строки опущены для краткости
router eigrp 99
  network 10.1.1.3 0.0.0.0
  network 10.1.13.3 0.0.0.0
  auto-summary

R3# show ip eigrp interfaces
EIGRP-IPv4 Interfaces for AS(99)
                Xmit Queue   PeerQ        Mean Pacing Time Multicast   Pendin
Interface Peers Un/Reliable Un/Reliable SRTT Un/Reliable Flow Timer
```

```
Gi0/0     2        0/0          0/0          1     0/1          50          0

R3# show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "eigrp 99"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP-IPv4 Protocol for AS(99)
    Metric weight K1=1, K2=0, K3=1, K4=0, K5=0
    NSF-aware route hold timer is 240
    Router-ID: 3.3.3.3
    Topology : 0 (base)
      Active Timer: 3 min
      Distance: internal 90 external 170
      Maximum path: 4
      Maximum hopcount 100
      Maximum metric variance 1

Automatic Summarization: disabled
Maximum path: 4
Routing for Networks:
  10.1.1.3/32
  10.1.13.3/32
Routing Information Sources:
  Gateway         Distance      Last     Update
  10.1.1.2        90            00:05:14
  10.1.1.1        90            00:05:14
Distance: internal 90 external 170
```

Основная причина проблем в маршрутизаторе R3 — команда конфигурации `network 10.1.13.3 0.0.0.0`, которая не совпадает с IP-адресом Fa0/1, т.е. 10.1.33.3. Если бы конфигурация устройства была недоступна (например, в сертификационном экзамене), то нужную информацию можно было получить с помощью команды `show ip protocols`. В данном примере в выводе этой команды для маршрутизатора R3 содержится строка "`10.1.13.3/32`", свидетельствующая о том, что параметры команды `network` были указаны неправильно, часть "`/32`" преобразуется в шаблон маски из 32 двоичных нулей, или десятичное число 0.0.0.0.

Неправильная конфигурация маршрутизатора R3 означает, что на интерфейсе G0/1 маршрутизатора R3 не происходят два действия. Маршрутизатор R3 не пытается искать соседей на своем интерфейсе G0/1, что не является грандиозным предприятием в данном случае. Но маршрутизатор R3 не анонсирует также подсеть 10.1.33.0/24, подключенную к его интерфейсу G0/1.

Что касается проблемы маршрутизатора R4, то в примере 11.4 показано, почему маршрутизаторы R1 и R2 не изучают маршрут к подсети 10.1.44.0/24 маршрутизатора R4. В данном случае инженер, возможно, правильно использовал на маршрутизаторе R4 подкоманду маршрутизатора `passive-interface Gigabitethernet0/1`, поскольку никаких других маршрутизаторов не должно существовать на интерфейсе G0/1 маршрутизатора R4. Но инженер по ошибке сделал интерфейс G0/0 маршрутизатора R4 пассивным.

Пример 11.4. Проблемы EIGRP на маршрутизаторе R4

```
R4# show running-config
! Строки опущены для краткости
router eigrp 99
  passive-interface GigabitEthernet0/0
  network 10.0.0.0
  auto-summary

R4# show ip eigrp interfaces
EIGRP-IPv4 Interfaces for AS(99)
              Xmit Queue   PeerQ        Mean Pacing Time Multicast   Pendin
Interfac Peers Un/Reliable Un/Reliable SRTT Un/Reliable Flow Timer Routes
Gi0/1    0     0/0         0/0         0    0/1         0          0

R4# show ip protocols | begin Routing for Networks
  Routing for Networks:
    10.0.0.0
  Passive Interface(s):
    GigabitEthernet0/0
  Routing Information Sources:
    Gateway Distance Last Update
  Distance: internal 90 external 170
```

ВНИМАНИЕ!

Последняя команда в примере, `show ip protocols | begin Routing for Networks`, осуществляет вывод, начинающийся с зависящей от регистра строки `Routing for Networks`. Это средство можно использовать с любым выводом команды, если вы предпочитаете просматривать лишь последние строки вывода команды.

Для поиска этой ошибки в примере 11.4 используется вывод двух команд. Команда `show ip eigrp interfaces` на маршрутизаторе R4 опускает пассивный интерфейс (G0/0). Это означает, что маршрутизатор R4 не будет пытаться искать соседей EIGRP для этого интерфейса. Кроме того, выделенная часть команды `show ip protocols` маршрутизатора R4 отображает интерфейс G0/0 как пассивный, что снова означает то, что маршрутизатор R4 даже не будет пытаться стать соседом для других устройств на его интерфейсе G0/0.

Поиск и устранение неисправностей интерфейсов в протоколе OSPF

У протокола OSPF те же основные требования к интерфейсам, что и у протокола EIGRP, но с несколькими исключениями. Во-первых, маршрутизатор EIGRP должен использовать тот же номер автономной системы (ASN), что и соседние маршрутизаторы, как задано глобальной командой конфигурации `router eigrp` *asn*. Маршрутизаторы OSPF могут использовать любой идентификатор процесса в команде `router ospf` *идентификатор_процесса*, совпадение с соседями необязательно. Во-вторых, протокол OSPF требует, чтобы интерфейсам, подключенным к той же подсети, была присвоена та же область OSPF, тогда как у протокола EIGRP нет вообще концепции областей.

Пример 11.5 демонстрирует по большей части рабочую объединенную сеть OSPF на основании рис. 11.3. Проблема в данном случае кроется в проекте области, как

показано на рис. 11.4 (пересмотренной версии рис. 11.3). Все подсети должны быть помещены в область 0. Но инженер допустил ошибку конфигурации на маршрутизаторе R2, поместив оба его интерфейса в область 1. В результате интерфейс G0/0 маршрутизатора R2 нарушает правило проекта OSPF, требующее находиться в той же подсети, что и маршрутизаторы R1, R3 и R4, но не в той же области OSPF.



Рис. 11.4. Проект предполагал использовать только область 0, а маршрутизатор R2 нарушил это требование

Пример 11.5 начинает поиск причины проблемы с изучения состояния OSPF на интерфейсах маршрутизаторов R1 и R2 при помощи команды `show ip ospf interface brief`.

Пример 11.5. Команда `show ip interface brief` на маршрутизаторах R1 и R2

```
R1> show ip ospf interface brief
Interface  PID  Area  IP Address/Mask  Cost  State  Nbrs F/C
Gi0/1      1    0     10.1.11.1/24     1     DR     0/0
Gi0/0      1    0     10.1.1.1/24      1     DROTH  2/2
! ------------------------------------------------------------------------
! Следующая команда на R2
R2> show ip ospf interface brief
Interface  PID  Area  IP Address/Mask  Cost  State  Nbrs F/C
Gi0/1      2    1     10.1.22.2/24     1     WAIT   0/0
Gi0/0      2    1     10.1.1.2/24      1     WAIT   0/0
```

С общей точки зрения, вывод команды `show ip ospf interface brief` похож на таковой у команды `show ip eigrp interface`, с одной строкой для каждого разрешенного интерфейса. Команда `show ip ospf interface` не представлена в примере — она выводит подробную информацию OSPF для каждого интерфейса.

При данной конкретной проблеме вывод в примере 11.5 демонстрирует, что на обоих маршрутизаторах, R1 и R2, протокол OSPF разрешен на обоих интерфейсах LAN. Но эта команда выводит также номер области для каждого интерфейса, у маршрутизатора R2 оба интерфейса LAN находятся в области 1. Кроме того, эти команды повторяют IP-адреса и маски интерфейсов, по ним можно заметить, что адрес 10.1.1.1/24 маршрутизатора R1 находится в той же подсети, что и адрес 10.1.1.2/24 маршрутизатора R2, что помещает эти два маршрутизатора в ту же подсеть, но в различные области OSPF.

В примере 11.6 показан другой способ поиска проблемы: при помощи команд `show ip protocols` на маршрутизаторах R1 и R2. Поскольку эти команды выводят команды `network` протокола OSPF в сокращенной форме, это может указать на возможные ошибки конфигурации, даже если конфигурация недоступна.

Пример 11.6. Поиск ошибок конфигурации OSPF на маршрутизаторах R1 и R2 при помощи команды `show ip protocols`

```
R1> show ip protocols
*** IP Routing is NSF aware ***

  Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 1.1.1.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    10.0.0.0 0.255.255.255 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    2.2.2.2         110           00:14:32
    3.3.3.3         110           00:14:32
    10.1.44.4       110           00:14:42
  Distance: (default is 110)

R1> show ip route ospf
! Легенда, опущена для краткости

     10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
O       10.1.33.0/24 [110/2] via 10.1.1.3, 00:15:32, GigabitEthernet0/0
O       10.1.44.0/24 [110/2] via 10.1.1.4, 00:15:42, GigabitEthernet0/0
! ------------------------------------------------------------------------
! Теперь переходим к маршрутизатору R2
R2> show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "ospf 2"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 2.2.2.2
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    10.0.0.0 0.255.255.255 area 1
  Routing Protocol is "ospf 2"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Router ID 2.2.2.2
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Maximum path: 4
Routing for Networks:
    10.0.0.0 0.255.255.255 area 1
  Routing Information Sources:
    Gateway         Distance      Last Update
  Distance: (default is 110)
```

```
R2>
Nov 15 12:16:39.377: %OSPF-4-ERRRCV: Received invalid packet: mismatched
area ID, from backbone area must be virtual-link but not found from
10.1.1.1, GigabitEthernet0/0
```

При более внимательном рассмотрении вывода команды `show ip protocols` маршрутизатора R2, особенно выделенной части, можно заметить ошибку конфигурации. Как обычно, раздел "`Routing for Networks:`" указывает сокращенную версию конфигурации. В данном случае выделенная фраза "`10.0.0.0 0.255.255.255 area 1`" фактически является точным синтаксисом одной из команд `network` на маршрутизаторе R2, только без слова `network` (команда `network 10.0.0.0 0.255.255.255 area 1`). Поскольку в проекте на рис. 11.4 все интерфейсы должны находиться в области 0, данную конкретную проблему можно решить командой `network 10.0.0.0 0.255.255.255 area 0`.

В конце примера также показано сообщение системного журнала, которое создается в маршрутизаторе R2, чтобы уведомить пользователя, подключенного к консоли, о том, что устройство получило сообщение Hello, содержащее номер зоны, несовпадающий с локальным.

Кроме проверки интерфейсов, можно проверить некоторые другие настройки. Обычно имеет смысл пойти дальше и проверить настройки IP-адресов на интерфейсах и их состояние с помощью команд `show interfaces` и `show ip interface brief`. В частности, следует обратить внимание на коды состояний интерфейсов и убедиться в том, что они работают (`up/up`), поскольку маршрутизатор не будет посылать пакеты (включая пакеты протоколов маршрутизации) через интерфейсы, не находящиеся в состоянии `up/up`. Более подробная информация о проверке интерфейса приведена в главе 5 и здесь не повторяется.

Соседские отношения

В этом разделе рассматривается множество фактов, свидетельствующих о том, что, прежде чем два маршрутизатора станут соседями, они должны свериться с каждым потенциальным соседом.

На самом простом уровне протоколы маршрутизации могут легко создать соседские отношения, используя протокол Hello. Сначала протокол маршрутизации следует разрешить на интерфейсе. Кроме того, интерфейс не может быть настроен как пассивный, поскольку это запрещает протоколу маршрутизации передавать сообщения Hello.

Кроме простого процесса, протоколы маршрутизации фактически проверяют и несколько других параметров, чтобы выяснить, должны ли маршрутизаторы стать соседями. И протокол OSPF, и EIGRP используют сообщения Hello, которые содержат информацию, используемую для выполнения некоторых базовых проверок. Например, как было показано в примере 11.5, маршрутизатор OSPF не должен становиться соседом другого маршрутизатора в другой области, поскольку все маршрутизаторы в общей подсети должны быть в той же области OSPF, в соответствии с проектом.

Как только маршрутизатор EIGRP или OSPF услышит сообщение Hello от нового соседа, протокол маршрутизации исследует информацию в этом сообщении и сравнивает ее с собственными параметрами локального маршрутизатора. Если соответствие есть — прекрасно. В противном случае маршрутизаторы соседями не станут. Поскольку нет формального термина для описания всех элементов, рассматриваемых протоколом маршрутизации, в данной книге они называются *требованиями к соседям* (neighbor requirements).

В табл. 11.2 перечислены требования к настройкам соседних устройств, которые должны быть выполнены, чтобы два устройства установили между собой канал связи в протоколах EIGRP и OSPF. Ниже также более подробно описаны настройки, перечисленные в таблице, для обоих протоколов маршрутизации, EIGRP и OSPF, на примере сети, показанной на рис. 11.3.

Ключевая тема

Таблица 11.2. Требования к соседям в протоколах EIGRP и OSPF

Требование	EIGRP	OSPF
Интерфейсы должны быть в рабочем состоянии (up/up)	Да	Да
Интерфейсы должны относиться к той же подсети	Да	Да
Списки (ACL) не должны фильтровать сообщения протокола маршрутизации	Да	Да
Аутентификация, если она настроена, должна пройти успешно	Да	Да
В командах конфигурации маршрутизатора должны совпадать номер автономной системы или идентификатор процесса (ASN/PID)	Да	Нет
Таймеры Hello, Hold и Dead должны совпадать	Нет	Да
Идентификаторы маршрутизаторов (Router ID) должны быть уникальными	Нет[1]	Да
Коэффициенты K (K-value) должны совпадать	Да	Не определено
Интерфейсы устройств должны быть в одной области	Не определено	Да

[1] Дублирующиеся идентификаторы маршрутизаторов в протоколе EIGRP не помешают соседним устройствам установить канал связи, но могут привести к тому, что внешние маршруты EIGRP не будут добавляться в таблицы маршрутизации.

ВНИМАНИЕ!

Хотя информацию данной таблицы важно изучить и запомнить, при первом чтении данной главы ее достаточно просто прочитать. Впоследствии, делая обзор главы или части, удостоверьтесь, что помните подробности таблицы.

В отличие от большинства требований к соседям, перечисленным в табл. 11.2, первые три требования имеют весьма косвенное отношение к самим протоколам маршрутизации. Два маршрутизатора должны быть способны передавать пакеты друг другу по соединяющей их физической сети. Для этого интерфейсы маршрутизатора должны быть в состоянии up/up и находиться в той же подсети. Кроме того,

маршрутизаторы не должны использовать списки ACL, отфильтровывающие трафик протокола маршрутизации.

Например, протокол OSPF посылает множество сообщений на известные многоадресатные IP-адреса 224.0.0.5 и 224.0.0.6, тогда как протокол EIGRP использует адрес 224.0.0.10. Такая команда ACL, как `access-list 101 deny ip any host 224.0.0.10`, в списке ACL на входящем интерфейсе маршрутизатора отфильтровала бы входящие пакеты EIGRP. Либо такая команда ACL, как `access-list 102 deny ospf any any`, может отфильтровать весь трафик OSPF. Поэтому уделяйте особое внимание спискам ACL, особенно если похоже на то, что все настройки протокола маршрутизации выглядят хорошо.

На практике, прежде чем приступать к изучению вывода различных команд и использовать сложные методы поиска и устранения неисправностей, следует убедиться, что два маршрутизатора могут обмениваться пакетами ping в своем сегменте сети. Если устройства не могут обмениваться такими пакетами, следует проверить работоспособность уровней 1, 2 и 3 маршрутизаторов с помощью методов и процессов, описанных в томе I.

Детали процесса поиска ошибок для двух протоколов почти не отличаются. Ниже сначала будет рассмотрен протокол маршрутизации EIGRP, а затем — OSPF.

ВНИМАНИЕ!

В данном разделе предполагается, что протокол маршрутизации был включен на всех интерфейсах маршрутизатора.

Последовательность проверки соседей EIGRP

Любые два маршрутизатора EIGRP, подключенные к одному и тому же каналу передачи данных, интерфейсы которых включены в протокол маршрутизации EIGRP и не работают в пассивном режиме, постараются установить между собой канал для передачи маршрутной информации. Чтобы быстро и точно определить, какие устройства прошли проверку параметров конфигурации протокола EIGRP и могут установить между собой канал связи, следует использовать команду `show ip eigrp neighbors`. В ее выводе присутствуют только соседние устройства, которые прошли все проверки своих настроек.

В примере 11.7 снова демонстрируется вывод команды `show ip eigrp neighbors` с четырьмя маршрутизаторами на рис. 11.3. В данном случае все маршрутизаторы были настроены правильно, поэтому у каждого есть соседские отношения с другими тремя маршрутизаторами в той же подсети LAN.

Пример 11.7. Вывод команды `show ip eigrp neighbors` для маршрутизатора R1 (все ошибки в конфигурации исправлены)

```
R1# show ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(99)
H  Address         Interface  Hold Uptime   SRTT   RTO  Q    Seq
                              (sec)         (ms)       Cnt  Num
1  10.1.1.3        Gi0/0       13 00:00:20  1      100  0    31
2  10.1.1.4        Gi0/0       13 00:00:43  80     480  0    10
0  10.1.1.2        Gi0/0       13 00:13:52  1      100  0    20
```

Если команда `show ip eigrp neighbors` не выводит одного или нескольких ожидаемых соседей, то первый этап локализации проблемы подразумевает проверку командой `ping` с каждого из двух маршрутизаторов IP-адресов других маршрутизаторов в той же подсети. Если все работает, обратитесь к представленному в табл. 11.3 списку требований к соседям EIGRP и проверьте их. В табл. 11.3 не только резюмируются требования к соседям EIGRP, но и предлагаются наилучшие команды для их проверки.

Ключевая тема

Таблица 11.3. Требования к соседям EIGRP и наилучшие команды `show/debug`

Требование	Наилучшие команды для изоляции проблемы
Должны находиться в той же подсети	`show interfaces, show ip interface`
В командах конфигурации `router` должен использоваться тот же номер ASN	`show ip eigrp interfaces, show ip protocols`
Аутентификация соседей EIGRP должна быть пройдена	`debug eigrp packets`
Коэффициенты K должны совпадать	`show ip protocols`

Из четырех требований, перечисленных в табл. 11.3, первые два уже обсуждались.

Для аутентификации протокол EIGRP позволяет доверять маршрутизаторам как соседям EIGRP, только если они используют тот же ключ безопасности (пароль); если эта проверка терпит неудачу, соседские отношения не формируются. Стандартно маршрутизаторы не делают попыток аутентификации EIGRP, что позволяет маршрутизаторам формировать соседские отношения EIGRP. Если один маршрутизатор использует аутентификацию, а другой — нет, то они не станут соседями. Если аутентификацию используют оба, они должны применять одинаковый ключ аутентификации, чтобы стать соседями.

Последняя запись в таблице, о коэффициентах K, относится к компонентам метрик EIGRP и их вычислениям. *Коэффициенты K* (K-value) — это переменные, в основном позволяющие включать или отключать использование различных компонентов в составной метрике EIGRP. Компания Cisco не рекомендует изменять эти значения в настройках, используя только метрики ширины полосы пропускания и задержки. Чтобы два маршрутизатора стали соседями, их параметры коэффициентов K должны совпадать. Проверить коэффициенты K на обоих маршрутизаторах можно при помощи команды `show ip protocols`.

Пример поиска и устранения неисправностей соседских отношений EIGRP

В примере 11.8 демонстрируются три проблемы, из-за которых маршрутизаторы EIGRP не могут стать соседями. В данном примере используется тот же проект сети, что и во всей главе, на рис. 11.5 представлены те же маршрутизаторы и те же интерфейсы, но со следующими проблемами.

- Маршрутизатор R2 был настроен IP-адресом 10.1.2.2/24, который принадлежит подсети, отличной от той, в которой располагаются маршрутизаторы R1, R3 и R4.
- Команда `router eigrp 199` задала на маршрутизаторе R3 номер ASN 199 вместо номера ASN 99, используемого на трех других маршрутизаторах.
- На маршрутизаторе R4 была настроена аутентификация MD5 (Message Digest 5), а другие маршрутизаторы аутентификацию не используют.



Рис. 11.5. Проблемы, препятствующие соседским отношениям EIGRP в сети LAN

Фактически маршрутизатор R1 способен обнаружить две из проблем, используя локальные команды и сообщения, как показано в примере 11.8. Маршрутизатор R1 создает незапрашиваемое регистрационное сообщение для проблемы несоответствия подсети, а команда `debug` на маршрутизаторе R1 способна выявить отказ аутентификации. Пример дополнен комментариями.

Пример 11.8. Наиболее распространенные проблемы, мешающие формированию соседских отношений EIGRP (R1)

```
! Сначала у маршрутизатора R1 нет никаких соседских отношений.
! Маршрутизатор R1 использует номер ASN (процесс) 99.
R1# show ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(99)

R1#
! Затем маршрутизатор R1 создает отображаемое на консоли регистрационное
! сообщение, заявляя, что маршрутизатор с IP-адресом 10.1.2.2
! не находится в той же подсети, что и маршрутизатор R1.
!
*Nov 15 16:19:14.740: %DUAL-6-NBRINFO: EIGRP-IPv4 99: Neighbor 10.1.2.2
(GigabitEthernet0/0) is blocked: not on common subnet (10.1.1.1/24)

! Далее маршрутизатор R1 включает отладку, выводящую сообщения для
! каждого пакета, полученного от маршрутизатора R4, в котором использован
! неправильный пароль (строка ключа аутентификации)
!
R1# debug eigrp packets
```

```
EIGRP Packets debugging is on
    (UPDATE, REQUEST, QUERY, REPLY, HELLO, IPXSAP, PROBE, ACK, STUB,
     SIAQUERY, SIAREPLY)
R1#

*Nov 15 16:20:30.865: EIGRP: Gi0/0: ignored packet from 10.1.1.4,
opcode = 5 (authentication off or key-chain missing)
```

В примере 11.8 приведен ряд доказательств несоответствия подсети на маршрутизаторе R2 и проблем аутентификации на маршрутизаторе R4, но никакой информации о неправильном номере ASN, заданном на маршрутизаторе R3. В примере 11.9 приведены выдержки вывода двух команд `show` на маршрутизаторе R3, обе демонстрируют номер ASN, заданный на этом маршрутизаторе. Применение тех же команд на всех маршрутизаторах позволяет заметить, что маршрутизаторы R1, R2 и R4 используют номер ASN 99, тогда как маршрутизатор R3 использует номер 199 (см. пример 11.9).

Пример 11.9. Отображение неправильного номера ASN (199) на маршрутизаторе R3

```
R3# show ip protocols
Routing Protocol is "eigrp 199"
!
! Первая строка вывода команды show ip eigrp interfaces отображает
! номер ASN 199

!
R3# show ip eigrp interfaces
EIGRP-IPv4 Interfaces for AS(199)
              Xmit Queue     Mean  Pacing Time  Multicast   Pendin
Interfac Peers Un/Reliable   SRTT  Un/Reliable  Flow Timer  Routes
Gi0/0    0     0/0           0     0/1          0           0
Gi0/1    0     0/0           0     0/1          0           0
```

Поиск и устранение неисправностей соседских отношений OSPF

Точно так же, как и в протоколе маршрутизации EIGRP, с помощью команды `show ip ospf neighbor` можно увидеть соседние маршрутизаторы, параметры конфигурации которых прошли проверку процессом маршрутизации и признаны правильными (см. табл. 11.2). Тем не менее в протоколе OSPF требуется совпадение еще одного параметра — значения MTU. Если этот параметр не совпал, устройство все равно будет присутствовать в таблице соседних маршрутизаторов, но протокол не будет работать корректно (подробно эта проблема описана ниже). Итак, первым этапом в процессе поиска и устранения неисправностей в протоколе OSPF будет, как обычно, инспекция таблицы соседних устройств.

В примере 11.10 показан вывод команды `show ip ospf neighbor` на маршрутизаторе R2 согласно рис. 11.4. Все четыре маршрутизатора находятся в той же подсети LAN, в области 0 (при правильной конфигурации). Таким образом, все четыре маршрутизатора формируют правильные соседские отношения OSPF.

Пример 11.10. Нормальная работа. Команда `show ip ospf neighbors` на маршрутизаторе R2

```
R2# show ip ospf neighbor
Neighbor ID     Pri     State           Dead Time   Address     Interface
1.1.1.1         1       FULL/BDR 00:    00:37       10.1.1.1    GigabitEthernet0/0
3.3.3.3         1       2WAY/DROTHER    00:00:37    10.1.1.3    GigabitEthernet0/0
4.4.4.4         1       FULL/DR         00:00:31    10.1.1.4    GigabitEthernet0/0
```

В первую очередь обратите внимание на значения в первом столбце, идентифицирующие соседей по их идентификатору маршрутизатора (RID). В сети данного примера все четыре маршрутизатора используют легко запоминающиеся идентификаторы RID. Кроме первого, столбец `Address` выводит IP-адреса интерфейсов, используемых данным соседом в общей подсети.

Краткий обзор состояний соседних маршрутизаторов в протоколе OSPF (подробно описанных в главе 11) поможет лучше понять информацию, показанную в примере. Состояние связи с соседними устройствами в протоколе маршрутизации OSPF при нормальной работе маршрутизаторов должно быть одним из двух: двусторонний канал (two-way) или полная синхронизация (full). Два устройства, которые не обмениваются между собой информацией напрямую, должны установить двусторонний канал; обычно это два невыделенных маршрутизатора (non-DR) в сегменте локальной сети. В большинстве случаев два маршрутизатора все же должны полностью синхронизировать свои базы LSDB. По завершении этого процесса два устройства будут в состоянии полной синхронизации (full). В примере 11.6 маршрутизатор R4 является устройством DR, маршрутизатор R1 —устройством BDR, поэтому маршрутизаторы R2 и R3 будут невыделенными устройствами (non-DR или DROTHER) и не должны обмениваться маршрутами напрямую. Следовательно, состояние канала связи маршрутизатора R2 и маршрутизатора R3 (RID 3.3.3.3) в примере 11.6 будет отображаться как двусторонний канал (two-way).

ВНИМАНИЕ!

Следует помнить, что в двух соседних маршрутизаторах OSPF номер процесса маршрутизации (process ID) в команде `router ospf` *идентификатор*. В примере 11.6 у всех маршрутизаторов идентификаторы разные.

Если в выводе команды `show ip ospf neighbor` отсутствует один или более маршрутизатор, то прежде чем переходить к локализации проблемы расширенными командами, следует проверить, могут ли устройства обмениваться пакетами ping в своей подсети. Если могут, а соседнее устройство отсутствует в таблице, то следует проверить, совпадают ли параметры, которые проверяют устройства при установлении связи друг с другом. В табл. 11.4 перечислены требования к параметрам и указаны команды, с помощью которых их можно проверить.

В этом разделе рассматривается несколько проблем соседства OSPF в обычной сети с четырьмя маршрутизаторами на рис. 11.4, со всеми интерфейсами в области 0. Однако в проект были внесены следующие проблемы.

- Оба интерфейса LAN маршрутизатора R2 расположены в области 1, тогда как интерфейсы G0/0 трех других маршрутизаторов — в области 0.

- Маршрутизатор R3 использует тот же RID (1.1.1.1), что и маршрутизатор R1.
- Таймеры Hello/Dead на интерфейсе G0/0 маршрутизатора R4 были настроены значениями 5/20, вместо значений 10/40, используемых (стандартно) на маршрутизаторах R1, R2 и R3.

Ключевая тема

Таблица 11.4. Требования к соседним устройствам в протоколе OSPF и команды для локализации ошибок

Требование к соседнему устройству	Команды для локализации проблемы
Устройства должны находиться в одной подсети	`show interfaces`, `debug ip ospf hello`
Аутентификация должна пройти успешно	`debug ip ospf adj`
Таймеры Hello, Hold и Dead соседних устройств должны совпадать	`show ip ospf interface`, `debug ip ospf hello`
Интерфейсы устройств должны быть в одной области	`debug ip ospf adj`, `show ip ospf interface brief`
Идентификаторы маршрутизаторов (Router ID) должны быть уникальными	`show ip ospf`

Для справки: эти проблемы представлены на рис. 11.6.

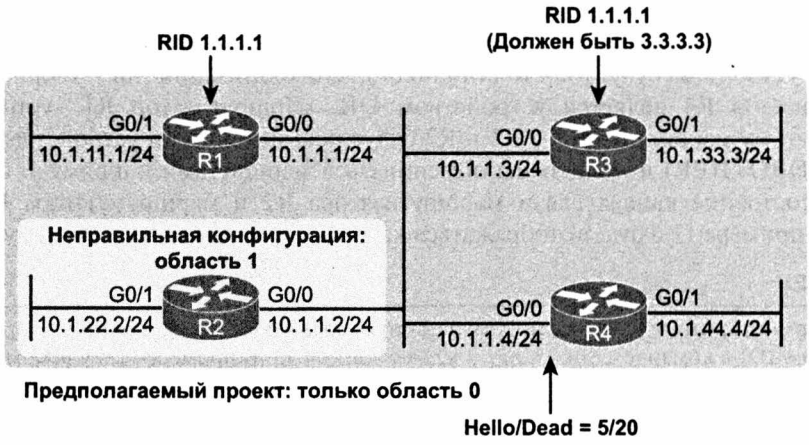


Рис. 11.6. Проблемы, препятствующие соседским отношениям OSPF в сети LAN

Поиск несоответствия области

Ранее в этой главе упоминалось применение команды `show ip ospf interface` для вывода номера области и выявления несоответствия области OSPF. В данном разделе описано выявление той же проблемы с использованием команды `debug ip ospf adj` (пример 11.11). Эта команда выводит сообщения, связанные с событиями соседей OSPF, и сообщения, идентифицирующие несоответствие области (с маршрутизатором R2).

Пример 11.11. Поиск несоответствия области при помощи команды debug на маршрутизаторе R1

```
R1# debug ip ospf adj
OSPF adjacency events debugging is on
R1#
*Nov 15 13:42:02.288: OSPF-1 ADJ Gi0/0: Rcv pkt from 10.1.1.2, area
0.0.0.0, mismatched area 0.0.0.1 in the header
R1#
R1# undebug all
All possible debugging has been turned off
```

Как уже упоминалось в табл. 11.4, команда `debug ip ospf adj` позволяет выявить проблемы несоответствия области OSPF и аутентификации. Первые выделенные строки в примере выводят сокращенную информацию о пакете ("`Rcv pkt`"), полученном от 10.1.1.2, являющегося IP-адресом маршрутизатора R2. В остальных строках упоминаются область маршрутизатора R1 (0.0.0.0) и область, требуемая другим маршрутизатором (0.0.0.1). (Обратите внимание, что эти сообщения выводят 32-разрядный номер области в формате десятичного числа с разделительными точками.)

Поиск двойных идентификаторов маршрутизатора OSPF

В примере 11.12 показано, что оба маршрутизатора, R1 и R3, пытаются использовать одинаковый идентификатор RID 1.1.1.1. Интересно, что оба маршрутизатора автоматически создают регистрационное сообщение для проблемы двойного идентификатора RID OSPF; одно из таких сообщений представлено в конце примера 11.12. На экзамене достаточно использовать команды `show ip ospf` на маршрутизаторах R3 и R1, что позволит легко вывести RID на каждом маршрутизаторе и заметить, что они оба используют то же значение.

Пример 11.12. Сравнение идентификаторов OSPF на маршрутизаторах R1 и R3

```
! Далее на R3:
! R3 выводит RID 1.1.1.1
!
R3# show ip ospf
  Routing Process "ospf 3" with ID 1.1.1.1
  Start time: 00:00:37.136, Time elapsed: 02:20:37.200
! Строки опущены для краткости
! ------------------------------------------------------------------------
! Возвращаемся к R1: он также использует RID 1.1.1.1

R1# show ip ospf
Routing Process "ospf 1" with ID 1.1.1.1
Start time: 00:01:51.864, Time elapsed: 12:13:50.904
Supports only single TOS(TOS0) routes
Supports opaque LSA
Supports Link-local Signaling (LLS)
Supports area transit capability
Supports NSSA (compatible with RFC 3101)
Event-log enabled, Maximum number of events: 1000, Mode: cyclic
Router is not originating router-LSAs with maximum metric
Initial SPF schedule delay 5000 msecs
Minimum hold time between two consecutive SPFs 10000 msecs
```

```
Maximum wait time between two consecutive SPFs 10000 msecs
Incremental-SPF disabled
Minimum LSA interval 5 secs
Minimum LSA arrival 1000 msecs
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msecs
Retransmission pacing timer 66 msecs
Number of external LSA 0. Checksum Sum 0x000000
Number of opaque AS LSA 0. Checksum Sum 0x000000
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Number of areas transit capable is 0
External flood list length 0
IETF NSF helper support enabled
Cisco NSF helper support enabled
Reference bandwidth unit is 100 mbps
  Area BACKBONE(0) (Inactive)
    Number of interfaces in this area is 3
    Area has no authentication
    SPF algorithm last executed 00:52:42.956 ago
    SPF algorithm executed 9 times
    Area ranges are
    Number of LSA 1. Checksum Sum 0x00C728
    Number of opaque link LSA 0. Checksum Sum 0x000000
    Number of DCbitless LSA 0
    Number of indication LSA 0
    Number of DoNotAge LSA 0
    Flood list length 0
*May 29 00:01:25.679: %OSPF-4-DUP_RTRID_NBR: OSPF detected duplicate
router-id 1.1.1.1 from 10.1.1.3 on interface GigabitEthernet0/0
```

В первую очередь сосредоточьтесь на проблеме двойных идентификаторов RID. Первая строка вывода команды `show ip ospf` на этих двух маршрутизаторах сразу демонстрирует двойные идентификаторы 1.1.1.1. Маршрутизатор R1 должен использовать идентификатор 1.1.1.1, а маршрутизатор R3 — другой RID (возможно, 3.3.3.3), поэтому для решения проблемы достаточно изменить идентификатор RID на маршрутизаторе R3 и перезапустить процесс OSPF. Для этого используется подкоманда OSPF `router-id 3.3.3.3` и команда режима EXEC `clear ip ospf process`.

Кроме того, уделите минуту внимания регистрационному сообщению, созданному на каждом маршрутизаторе при наличии двойных идентификаторов RID.

И наконец, обратите внимание на то, что первая строка вывода команд `show ip ospf` в примере 11.12 также демонстрирует первопричину проблемы соседских отношений OSPF. Идентификатор PID OSPF — это число в команде `router ospf`, и оно должно быть уникальным. Кроме того, та же первая строка вывода в примере 11.12 демонстрирует, что маршрутизатор R3 использует команду `router ospf 3` с фразой "`Process "ospf 3"`", тогда как маршрутизатор R1 использует команду `router ospf 1` с фразой "`Process "ospf 1"`". Когда эти номера не совпадают, проблем нет.

Поиск несоответствия таймеров OSPF Hello и Dead

И наконец, переходим к проблеме несоответствия конфигурации таймеров OSPF Hello и Dead на маршрутизаторе R4 по сравнению с таковой у маршрутизато-

ров R1, R2 и R3. Хотя протокол EIGRP позволяет соседям использовать разные таймеры Hello, протокол OSPF — не позволяет. Поэтому такое несоответствие не позволяет маршрутизатору R4 стать соседом любому из трех остальных маршрутизаторов OSPF.

В примере 11.13 показан самый простой способ поиска несоответствия — команда `show ip ospf interface` на маршрутизаторах R1 и R4. Эта команда выводит таймеры Hello и Dead для каждого интерфейса (выделены в примере). Маршрутизатор R1 использует значения 10 и 40 (Hello и Dead), а маршрутизатор R4 — значения 5 и 20.

Пример 11.13. Поиск несоответствия таймеров OSPF Hello и Dead

```
R1# show ip ospf interface G0/0
GigabitEthernet0/0 is up, line protocol is up
  Internet Address 10.1.1.1/24, Area 0, Attached via Network Statement
  Process ID 1, Router ID 1.1.1.1, Network Type BROADCAST, Cost: 1
  Topology-MTID  Cost  Disabled  Shutdown  Topology Name
  0              1     no        no        Base
Transmit Delay is 1 sec, State DR, Priority 1
Designated Router (ID) 1.1.1.1, Interface address 10.1.1.1
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
! Строки опущены для краткости
! ------------------------------------------------------------------------
! Переходим к маршрутизатору R4
!
R4# show ip ospf interface Gi0/0
GigabitEthernet0/0 is up, line protocol is up
Internet Address 10.1.1.4/24, Area 0, Attached via Network Statement
Process ID 4, Router ID 10.1.44.4, Network Type BROADCAST, Cost: 1
  Topology-MTID  Cost  Disabled  Shutdown  Topology Name
  0              1     no        no        Base
Transmit Delay is 1 sec, State DR, Priority 1
Designated Router (ID) 10.1.44.4, Interface address 10.1.1.4
No backup designated router on this network
Timer intervals configured, Hello 5, Dead 20, Wait 20, Retransmit 5
! Строки опущены для краткости
```

Команда `debug ip ospf hello` также способна раскрыть эту проблему, поскольку она выводит сообщение для каждого таймера Hello, позволяя выявить несоответствие таймеров Hello/Dead, как показано в примере 11.14.

Пример 11.14. Поиск несоответствия таймеров OSPF Hello и Dead

```
R1# debug ip ospf hello
OSPF hello events debugging is on
R1#
*Nov 15 14:05:10.616: OSPF-1 HELLO Gi0/0: Rcv hello from 10.1.44.4 area 0
10.1.1.4
*Nov 15 14:05:10.616: OSPF-1 HELLO Gi0/0: Mismatched hello parameters
from 10.1.1.4
*Nov 15 14:05:10.616: OSPF-1 HELLO Gi0/0: Dead R 20 C 40, Hello R 5 C 10
Mask R 255.255.255.0 C 255.255.255.0
```

Хотя сообщения отладки может быть трудно понять, их значение помогут прояснить комментарии. В выделенном сообщении символ "C" означает "configured value" (настроенное значение), другими словами, значение, заданное на локальном маршрутизаторе, в данном случае на маршрутизаторе R1. Символ "R" в сообщении означает "received value" (полученное значение), или значение, полученное в принятом сообщении Hello. В данном случае:

- "`Dead R 20 C 40`" означает, что маршрутизатор R1 принял сообщение Hello со значением 20 таймера Dead, в то время как на маршрутизаторе R1 задано значение 40;
- "`Hello R 5 C 10`" означает, что маршрутизатор R1 принял сообщение Hello со значением 5 таймера Dead, в то время как на маршрутизаторе R1 задано значение 10.

Обратите внимание, что любые проблемы несоответствия подсети IP могут быть также обнаружены при той же отладке на основании полученных и настроенных масок подсети.

Другие проблемы OSPF

У протокола OSPFv2 может быть несколько других проблем, две из которых компания Cisco включала в экзаменационные темы по поиску и устранению неисправностей OSPF. В последнем разделе данной главы коротко обсуждаются эти две дополнительные темы: тип сети OSPF и размер *максимального блока передачи* (Maximum Transmission Unit — MTU) интерфейса.

Несоответствие типа сети OSPF

Для каждого интерфейса протокол OSPF определяет концепцию типа сети. *Тип сети* (network type) информирует протокол OSPF о канале связи, подключенном к интерфейсу. В частности, тип сети указывает маршрутизатору следующее:

- может ли маршрутизатор динамически обнаружить соседей на канале связи (или нет);
- выбран ли маршрутизатор как DR и BDR (или нет).

До сих пор в этой книге описывались только два типа сети OSPF, установленных на основании стандартной настройки. Последовательные интерфейсы, использующие такие протоколы двухточечного канала связи, как HDLC или PPP, стандартно используют *двухточечный* (point-to-point) тип сети OSPF. Интерфейсы Ethernet стандартно используют *широковещательный* (broadcast) тип сети OSPF. Оба типа позволяют маршрутизаторам динамически обнаруживать соседние маршрутизаторы OSPF, но только широковещательный тип сети позволяет выбирать маршрутизатор как DR/BDR.

Команда `show ip ospf interface` выводит текущий тип сети интерфейса OSPF. В примере 11.15 показан маршрутизатор R1 из прежних примеров, с широковещательным типом сети на интерфейсе G0/0.

Пример 11.15. Отображение типа сети OSPF на интерфейсе

```
R1# show ip ospf interface g0/0
GigabitEthernet0/0 is up, line protocol is up
  Internet Address 10.1.1.1/24, Area 0, Attached via Network Statement
  Process ID 1, Router ID 1.1.1.1, Network Type BROADCAST, Cost: 1
! Строки опущены для краткости
```

Тип сети OSPF на интерфейсе вполне можно изменить, и выбор неподходящих параметров на маршрутизаторах может не позволить им стать соседями OSPF. Инженеры обычно либо оставляют стандартное значение этого параметра, либо изменяют его для всех маршрутизаторов на том же канале связи. Но при плохом выборе и использовании разных типов сети на разных соседних маршрутизаторах могут возникнуть проблемы.

Например, если маршрутизаторы R1 и R2 объединенной сети из примеров этой главы все еще подключены к тем же сетям VLAN своими интерфейсами G0/0, то оба они стандартно используют широковещательный тип сети OSPF. При широковещательном типе сети OSPF эти маршрутизаторы лучше всего взаимодействуют через свои интерфейсы Ethernet. В результате оба динамически узнают друг о друге как о маршрутизаторе OSPF и оба пытаются использовать DR/BDR. Но если тип сети интерфейса G0/0 маршрутизатора R1 был изменен на двухточечный, то возникнет проблема. В результате маршрутизаторы фактически становятся соседями, но оказываются не в состоянии обмениваться своими базами LSDB, как показано в примере 11.16, где маршрутизатор R1 больше не изучает маршруты OSPF.

Пример 11.16. Несоответствие типов сети OSPF приводит к отказу обмена базами LSDB

```
R1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)# interface gigabitethernet0/0
R1(config-if)# ip ospf network point-to-point
R1(config-if)# ^Z
R1#
R1# show ip route ospf
Codes: L - local, 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, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

R1#
! Строки опущены для краткости
```

Обратите внимание, что в рабочих сетях обычно используются стандартные типы сетей OSPF, если нет серьезных причин переопределить эти значения. В главе 14 рассмотрен общий случай настройки нестандартного значения при использовании одного специфического стиля конфигурации Frame Relay.

Несоответствие параметров MTU

Размер блока MTU задает параметр интерфейса, используемый логикой маршрутизации уровня 3 маршрутизатора, и определяет наибольший размер пакета сетевого уровня, передаваемого через каждый интерфейс маршрутизатора. Например, размер блока MTU IPv4 интерфейса определяет максимальный размер пакета IPv4, который маршрутизатор может перенаправить через интерфейс.

Маршрутизаторы зачастую используют стандартный размер блока MTU в 1500 байтов, но его можно и изменить. Подкоманда интерфейса `ip mtu` *`размер`* задает размер блока MTU пакетов IPv4, а команда `ipv6 mtu` *`размер`* — пакетов IPv6.

По странному стечению обстоятельств, два маршрутизатора OSPFv2 могут фактически стать соседями OSPF и достичь состояния полного согласования, даже если они используют разные параметры MTU IPv4 на своих интерфейсах. Но если они не в состоянии обмениваться базами LSDB, то в конечном счете их соседские отношения потерпят неудачу.

Концепции, лежащие в основе происходящего при несоответствии размеров блока MTU у протоколов OSPFv2 и OSPFv3, одинаковы. В главе 17 приведен пример данной конкретной проблемы для протокола OSPFv3 наряду со многими подробностями.

Обзор

Резюме

- Этапы поиска и устранения неисправностей протоколов маршрутизации включают анализ проекта сети и выявление интерфейсов, на которых должны быть разрешены протокол, выявление соседей, которые должны быть подключены к этим интерфейсам, проверка активности протокола на этих интерфейсах и исследование процесса, чтобы определить, почему соседи не находятся.
- Протоколы EIGRP и OSPF требуют разрешить протокол маршрутизации на интерфейсе при помощи подкоманды маршрутизатора `network`.
- Подкоманда маршрутизатора `passive-interface` может быть настроена так, чтобы маршрутизатор не пытался искать соседей на интерфейсе.
- Протоколы маршрутизации позволяют легко создавать соседские отношения, используя протокол Hello.
- Протокол маршрутизации должен быть разрешен на интерфейсе.
- Если два маршрутизатора OSPF используют одинаковый идентификатор RID, на одном из маршрутизаторов его следует изменить, а затем перезапустить процесс OSPF.
- Тип сети информирует протокол OSPF о канале связи, подключенном к интерфейсу.
- Размер блока MTU задает параметр интерфейса, используемый логикой маршрутизации уровня 3 маршрутизатора, и определяет наибольший размер пакета сетевого уровня, передаваемого через каждый интерфейс маршрутизатора. Например, размер блока MTU IPv4 интерфейса определяет максимальный размер пакета IPv4, который маршрутизатор может перенаправить через интерфейс.
- Несоответствие параметров MTU позволяет установить соседские отношения, но не позволяет обмен базами LSDB.

Ключевые темы

Повторите все ключевые темы данной главы, отмеченные пиктограммой "Ключевая тема". Ключевые темы и соответствующие им страницы перечислены в табл. 11.5.

Таблица 11.5. Ключевые темы главы 11

Элемент	Описание	Страница
Список	Два действия, выполняемые протоколами маршрутизации EIGRP и OSPF при их включении на интерфейсе	378
Табл. 11.1	Ключевые команды для поиска интерфейсов, участвующих в протоколе маршрутизации	379

Окончание табл. 11.5

Элемент	Описание	Страница
Табл. 11.2	Требования к соседям в протоколах EIGRP и OSPF	388
Табл. 11.3	Требования к соседям EIGRP и наилучшие команды show/debug	390
Табл. 11.4	Требования к соседним устройствам в протоколе OSPF и команды для локализации ошибок	394

Заполните таблицы и списки по памяти

Распечатайте приложение Г с веб-сайта или его раздел, относящийся к этой главе, и заполните таблицы и списки по памяти. В приложении Д приведены заполненные таблицы и списки для самоконтроля.

Таблицы команд

Хоть и не обязательно заучивать информацию из таблиц данного раздела, ниже приведен список команд конфигурации и пользовательских команды главы. Фактически команды стоит запомнить, чтобы лучше понять содержимое главы и выполнить задачи по подготовке к экзамену. Чтобы проверить, насколько хорошо вы запомнили команды, закройте левую сторону таблицы листом бумаги, читайте описания с правой стороны и пытайтесь вспомнить команду.

Таблица 11.6. Конфигурационные команды главы 11

Команда	Описание
`ip hello-interval eigrp` *`номер_автономной_системы значение_таймера`*	Подкоманда интерфейса, устанавливающая интервал Hello EIGRP для данного процесса EIGRP
`ip hold-time eigrp` *`номер_автономной_системы секунд`*	Подкоманда интерфейса, устанавливающая время задержки EIGRP для данного интерфейса
`ip ospf hello-interval` *`секунд`*	Подкоманда интерфейса, устанавливающая период передачи сообщений Hello
`ip ospf dead-interval` *`число`*	Подкоманда интерфейса, устанавливающая таймер Dead OSPF
`passive-interface` *`тип номер`*	Подкоманда маршрутизатора и для OSPF и для EIGRP, указывающая протоколу маршрутизации прекратить передачу сообщений Hello, а также прекратить пытаться обнаруживать соседей на этом интерфейсе

Таблица 11.7. Команды `show` главы 11

Команда	Описание
`show ip protocols`	Выводит параметры протокола маршрутизации и текущие значения таймера, включая рабочую копию команд `network` протоколов маршрутизации и список пассивных интерфейсов

Окончание табл. 11.7

Команда	Описание
`show ip eigrp interfaces`	Выводит интерфейсы, на которых разрешен протокол EIGRP по каждому процессу EIGRP, кроме пассивных интерфейсов
`show ip route eigrp`	Выводит только те маршруты из таблицы маршрутизации, которые изучены по протоколу EIGRP
`show ip eigrp neighbors`	Выводит соседей EIGRP и их состояние
`show ip ospf interface brief`	Выводит интерфейсы, на которых разрешен протокол OSPF по каждому процессу EIGRP (на основании команд `network`), включая пассивные интерфейсы
`show ip ospf interface [`*тип номер*`]`	Выводит подробные параметры OSPF для всех или только выбранных интерфейсов, включая таймеры Hello, Dead и области OSPF
`show ip route ospf`	Выводит маршруты в таблице маршрутизации, изученные по протоколу OSPF
`show ip ospf neighbor`	Выводит соседей и их текущее состояние на интерфейсе
`show ip ospf`	Выводит группу сообщений о самом процессе OSPF, выводя идентификатор маршрутизатора OSPF в первой строке
`show interfaces`	Выводит длинный набор сообщений по каждому интерфейсу, содержащих конфигурацию, состояние и информацию счетчиков
`show interfaces description`	Выводит для каждого интерфейса по одной строке, содержащей краткую информацию о состоянии

Таблица 11.8. Команды `debug` главы 11

Команда	Описание
`debug eigrp packets`	Выводит регистрационные сообщения для пакетов EIGRP, пересекающих маршрутизатор
`debug ip ospf adj`	Выводит регистрационные сообщения для событий смежности, связанных с соседними маршрутизаторами
`debug ip ospf events`	Выводит регистрационные сообщения для каждого действия, предпринятого протоколом OSPF, включая получение сообщений
`debug ip ospf packet`	Выводит регистрационные сообщения, описывающие содержимое всех пакетов OSPF
`debug ip ospf hello`	Выводит регистрационные сообщения, описывающие таймеры Hello и их отказы
`undebug all`	Пользовательская команда, отменяющая текущий режим отладки

Обзор части III

Проследите свой прогресс изучения материала части по контрольному списку в следующей таблице. Подробно задачи описаны ниже.

Контрольный список обзора части III

Задача	Первая дата завершения	Вторая дата завершения
Повторите вопросы из обзоров глав		
Ответьте на вопросы обзора части		
Повторите ключевые темы		
Создайте диаграмму связей первопричин проблем OSPF и EIGRP		
Создайте диаграмму связей команд OSPF и EIGRP		

Повторите вопросы из обзоров глав

Ответьте снова на вопросы обзоров глав этой части, используя программное обеспечение PCPT. Инструкция по запуску программного обеспечения PCPT с вопросами обзоров глав только этой части приведена в разделе "Как просмотреть вопросы только обзоров глав конкретной части" введения к книге.

Ответьте на вопросы обзора части

Ответьте на вопросы обзора этой части, используя программное обеспечение PCPT. Инструкция по запуску программного обеспечения PCPT с вопросами обзоров только этой части приведена в разделе "Как просмотреть вопросы только обзоров частей" введения к книге.

Повторите ключевые темы

Снова просмотрите темы прочитанных глав, отмеченные пиктограммой "Ключевая тема". Если понятны не все их подробности, уделите время повторному изучению.

Создайте диаграмму связей первопричин проблем OSPF и EIGRP

Глава 11 посвящена проблемам поиска и устранения неисправностей, связанных как с протоколом OSPF, так и с протоколом EIGRP, а именно с интерфейсами и соседскими отношениями. Для этой первой диаграммы связей обзора части постарайтесь вспомнить все элементы, способные создать проблемы, препятствующие работе протокола маршрутизации в объединенных сетях IPv4 и обсуждаемые в данной части. Другими словами, обдумайте первопричины, а затем организуйте их в диаграмму связей.

Начните организацию диаграммы связей с перечня того, что вспомните. Затем, обнаружив несколько взаимосвязанных первопричин, сгруппируйте их в категории по своему усмотрению. Нет единственно правильной или неправильной организации первопричин.

Например, могли бы быть отмечены такие первопричины, как отключение интерфейса LAN на маршрутизаторе или несоответствие IP-адресов (адреса в разных подсетях). Затем их можно отнести к таким категориям, как "Подключение IP к той же подсети" (IP Connectivity on Same Subnet) или "Доступность в той же подсети" (Pingable Same Subnet), как показано на рис. Ч3.1.



Рис. Ч3.1. Пример диаграммы связей первопричин проблем протокола маршрутизации IPv4

ВНИМАНИЕ!

Более подробная информация по этой теме приведена в разделе "О диаграммах связей" введения.

Создайте диаграмму связей команд OSPF и EIGRP

В этой части обсуждалась также настройка и проверка протоколов OSPF и EIGRP. Создайте диаграмму связей команд, как во многих других обзорах частей. Первый уровень организации должен подразумевать противопоставление протоколов OSPF и EIGRP, а затем настройки и проверки. В области проверки организуйте команды, как в главе 10, по командам, имеющим отношение к интерфейсам, соседям, топологии и маршрутам.

Ответы приведены в приложении E на веб-сайте, но ваши диаграммы связей могут выглядеть иначе.

Мир сетей предлагает огромное разнообразие возможных сетей WAN. В части IV две из них рассматриваются достаточно глубоко, чтобы позволить реализовать их на маршрутизаторах Cisco, — это двухточечные глобальные сети (глава 12) и сети Frame Relay (главы 13 и 14). В главе 15 приведен общий обзор множества других типов сетей WAN, благодаря которому читатели ознакомятся с основными средствами каждой из технологий.

Часть IV. Глобальные сети

Глава 12. “Реализация двухточечных сетей WAN”

Глава 13. “Концепции протокола Frame Relay”

Глава 14. “Реализация протокола Frame Relay”

Глава 15. “Другие типы глобальных сетей”

Обзор части IV

Глава 12

Реализация двухточечных сетей WAN

Глобальные сети на базе выделенных линий (известных также как последовательные каналы) требуют намного меньше внимания, чем большинство других тем, по крайней мере, с точки зрения экзаменов CCENT и CCNA. Простота выделенных линий позволяет кратко рассмотреть их на экзамене ICND1 в составе общего обсуждения маршрутизации IP.

В данной главе глобальные сети на базе выделенных линий обсуждаются значительно глубже, чем в других главах. Здесь кратко повторяются концепции выделенной линии из книги по ICND1, чтобы заложить основу обсуждения других концепций. Важнее всего то, что в этой главе рассматриваются настройка, проверка, а также этапы поиска и устранения неисправностей выделенных линий, использующих уже знакомые вам *высокоуровневый протокол управления каналом* (High-Level Data Link Control — HDLC) и *протокол двухточечного соединения* (Point-to-Point Protocol — PPP).

Настоящая глава имеет три главных раздела. В первом рассматриваются использующие протокол HDLC сети WAN на базе выделенных линий, включая подробные сведения о самих физических каналах связи, а также о настройке протокола HDLC. Во втором разделе обсуждается протокол PPP — альтернативный протокол канала передачи данных, который можно использовать вместо протокола HDLC, уделяя основное внимание концепциям и конфигурации. В заключительном разделе речь пойдет о типичных первопричинах проблем последовательного канала и их поиске.

В этой главе рассматриваются следующие экзаменационные темы
Технологии маршрутизации IP
Настройка и проверка состояния последовательного интерфейса
Технологии WAN
Настройка и проверка простого последовательного соединения WAN
Настройка и проверка соединения PPP между маршрутизаторами Cisco
Различные технологии WAN
T1/E1
Поиск и устранение неисправностей
Поиск и устранение проблем реализации WAN
Последовательные интерфейсы
PPP

Основные темы

Протокол HDLC в сети WAN на базе выделенных линий

Физическая выделенная линия WAN работает как перекрещенный кабель Ethernet, соединяющий два маршрутизатора, но без ограничений по дистанции. Как показано на рис. 12.1, каждый маршрутизатор способен осуществлять передачу в любое время (дуплексная передача). Скорость также симметрична, т.е. оба маршрутизатора передают биты с той же скоростью.



Рис. 12.1. Выделенная линия: одинаковая скорость, два направления, всегда включена

Хотя выделенная линия и предоставляет средство передачи битов на физическом уровне, для передачи битов по каналу связи маршрутизаторы должны также использовать на канале связи WAN протокол канала связи. Как известно, маршрутизаторы получают фреймы на интерфейсах LAN, а затем маршрутизатор извлекает содержимое пакета сетевого уровня. Прежде чем перенаправить пакет далее, маршрутизатор инкапсулирует содержимое в такой пакет протокола канала связи WAN, как высокоуровневый протокол управления каналом (HDLC). Это показано на этапе 2 рис. 12.2. (Обратите внимание: на рисунке не представлены концевики канала связи в каждом фрейме, но в действительности у каждого фрейма есть и заголовок и концевик канала связи.)

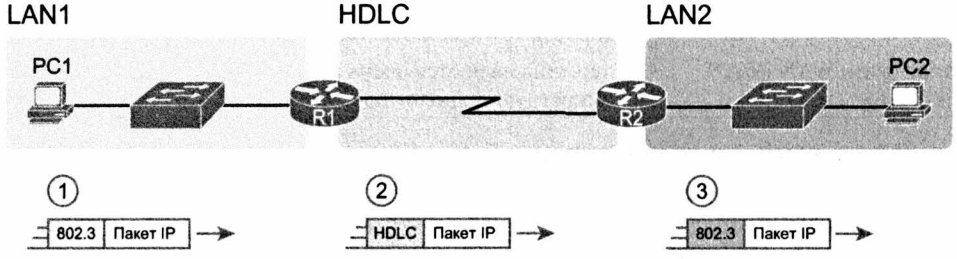


Рис. 12.2. Использование протокола HDLC маршрутизаторами для инкапсуляции пакетов

Рис. 12.1 и 12.2 дают представление о деталях уровня 1 и уровня 2 выделенных линий глобальных сетей соответственно. Первый раздел этой главы снова начинается с обсуждения каналов связи, сначала уровня 1, затем уровня 2, а завершается подробным объяснением конфигурации протокола HDLC.

ВНИМАНИЕ!

В разделах от текущего и до раздела "Настройка протокола HDLC" повторяются некоторые из концепций книги по экзамену ICND1. Те, кто помнит описание выделенных линий достаточно хорошо, могут лишь просмотреть эти темы.

Выделенные линии уровня 1

Выделенные линии используются довольно давно, примерно двадцать лет, т.е. дольше, чем локальные сети. Они и сейчас существуют как служба WAN.

В результате такого длительного существования у них появилось несколько разных названий. Первое название, *арендованная линия* (leased line), появилось благодаря тому факту, что использующая выделенную линию компания не владеет ею, а вносит ежемесячную арендную плату за ее использование. Как правило, она арендуется у *телефонной компании* (telco). Однако сейчас компании, предоставляющие любые формы подключения к глобальным сетям, включая Интернет, называют *провайдерами служб* (service provider). Некоторые из этих названий приведены в табл. 12.1, поскольку они могут встретиться в реальной сетевой задаче.

Таблица 12.1. Разные названия выделенной линии

Название	Описание
Арендованный канал (leased circuit), канал (circuit)	Термины *линия* (line) и *канал* (circuit) зачастую используют как синонимы в терминологии телефонной компании; канал означает электрический канал между двумя конечными точками
Последовательный канал (serial link), последовательная линия (serial line)	Термины *канал связи* (link) и *линия* (line) также зачастую используют как синонимы. Термин *последовательный* (serial) в данном случае свидетельствует о том факте, что биты передаются последовательно и что маршрутизаторы используют последовательные интерфейсы
Двухточечный канал связи (point-to-point link), двухточечная линия (point-to-point line)	Свидетельство того факта, что топология располагается между двумя и только двумя точками. (Некоторые устаревшие выделенные линии допускали несколько устройств.)
Линия T1	Конкретный тип выделенной линии, передающей данные на скорости 1,544 мегабит в секунду (1,544 Мбит/с)
Канал связи WAN (WAN link), канал связи (link)	Оба термина являются очень общими, без ссылки на конкретную технологию

Физические компоненты выделенной линии

Чтобы создать выделенную линию, телефонная компания должна иметь некий физический канал передачи данных между двумя маршрутизаторами на его концах. Физическая кабельная проводка должна соединять здания, где находится каждый маршрутизатор. Затем телефонная компания должна создать некий эквивалент сквозного канала из двух проводов, по одной для передачи данных в каждом направлении (дуплексная передача). На рис. 12.3 приведен один из примеров того, как телефонная компания использует несколько коммутаторов традиционных *телефонных станций* (Central Office — CO) для создания короткой выделенной линии между двумя маршрутизаторами.

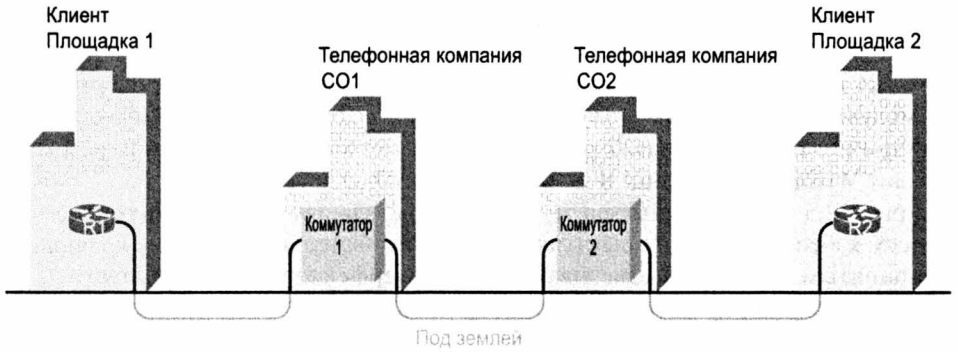


Рис. 12.3. Возможная кабельная проводка телефонной компании для короткой выделенной линии

Деталей в центре рис. 12.3, вероятно, даже больше, чем вам когда-либо понадобится знать о выделенных линиях глобальных сетей, по крайней мере, с точки зрения клиента телефонной компании. Как правило, большинство сетевых инженеров рассматривают выделенные линии не более чем с точки зрения, представленной на рис. 12.4, где показано несколько ключевых компонентов и терминов для оборудования на концах выделенной линии.

Абонентское оконечное оборудование (Customer Premise Equipment — CPE). Этот телефонный термин означает устройства, находящиеся на конце канала связи со стороны клиента.

Модуль обслуживания канала/модуль обработки данных (Channel Service Unit/Data Service Unit — CSU/DSU). Это устройство обеспечивает функцию *синхронизации* (clocking), физически контролирующую синхронизацию и скорость, на которой последовательный интерфейс маршрутизатора передает и получает каждый бит по последовательному кабелю.

Последовательный кабель (serial cable). Короткий кабель, соединяющий модуль CSU и последовательный интерфейс маршрутизатора.

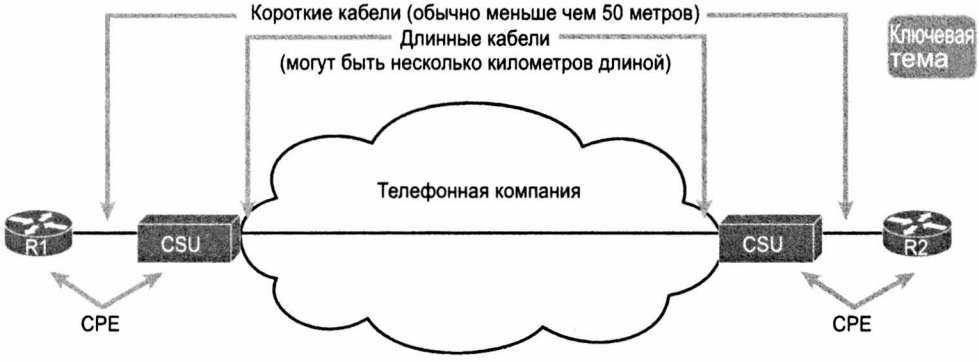


Рис. 12.4. Двухточечная выделенная линия: компоненты и терминология

Модуль CPE включает несколько отдельно управляемых частей. Внешний модуль CSU/DSU должен быть подключен последовательным кабелем к модулю CSU последовательного интерфейса маршрутизатора. Сейчас большинство маршрутизаторов ис-

пользуют последовательные интерфейсы, которые обычно являются частью сменной платы на маршрутизаторе и называются *интерфейсными платами WAN* (WAN interface card — WIC). У плат WIC единый стиль физических разъемов (размер/форма), тогда как у модулей CSU есть несколько типов разъемов. Поэтому при установке выделенной линии инженер должен выбрать правильный тип кабеля с разъемами, подходящими к плате WIC на одном конце и модулю CSU/DSU на другом.

На рис. 12.5 представлены три типа последовательных кабелей. На верхнем конце у всех кабелей есть интеллектуальный последовательный разъем, являющийся общепринятым для плат последовательных интерфейсов Cisco. На другом конце каждого кабеля имеется один из стандартных физических последовательных разъемов, используемых модулями CSU/DSU.

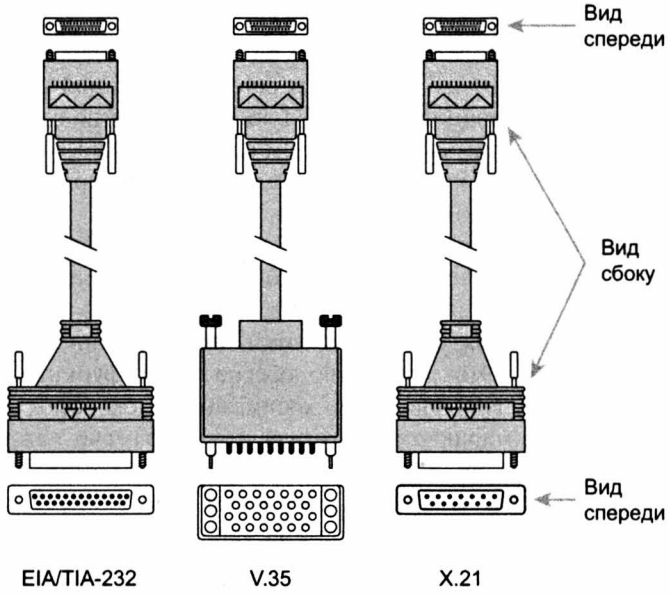


Рис. 12.5. Последовательные кабели, соединяющие модули CSU с маршрутизатором

В настоящее время большинство выделенных линий используют платы Cisco WIC с интегрированным модулем CSU/DSU. Когда аппаратные средства плат WIC включают те же функции, что и модули CSU/DSU, внешние модули CSU/DSU не нужны.

На рис. 12.5, в отличие от рис. 12.4, внешний модуль CSU/DSU и последовательный кабель на каждом конце отсутствуют, кабель от телефонной компании непосредственно подключается к плате WIC.

На рис. 12.6 показан маршрутизатор с четырьмя слотами WIC. Все слоты на лицевой панели представлены без установленных плат WIC. На переднем плане представлена плата WIC-4T1/E1, имеющая четыре последовательных канала с интегрированными модулями CSU/DSU. На передней панели платы WIC расположено четыре порта RJ-48; у этих разъемов тот же размер и форма, что и у разъемов RJ-45.

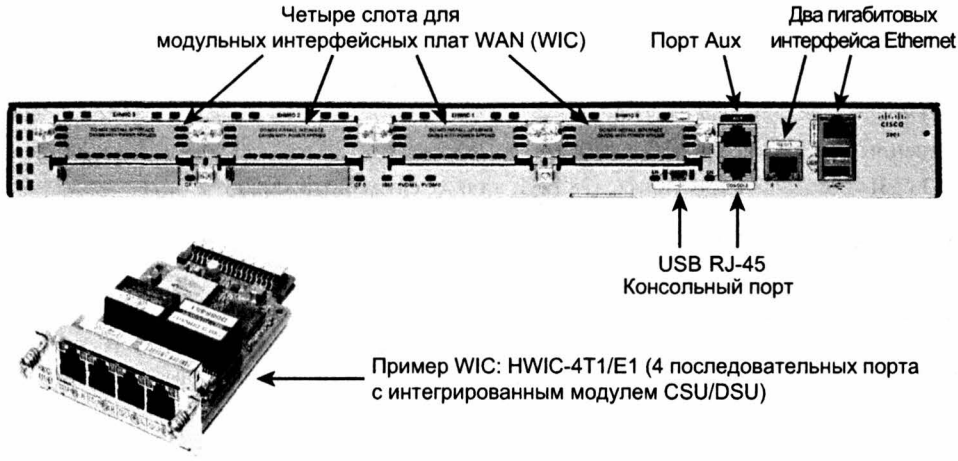


Рис. 12.6. Маршрутизатор с набором плат WIC, обладающих интегрированными модулями CSU/DSU и портами RJ-48

Выделенные линии и канальная система T

Телефонные компании предлагают широкое разнообразие скоростей для выделенных линий. Но клиент телефонной компании не может выбрать любую скорость, так как она зависит от выбранного стандарта довольно старой технологии — канальной системы T.

В 1950–1960-х годах американская компании Bell разработала и развернула канальную систему T для цифровой передачи голоса, стандартизировав различные скорости передачи, включая 64 Кбит/с, 1,544 и 44,736 Мбит/с.

Та же компания Bell разработала технологию *мультиплексирования с разделением времени* (Time-Division Multiplexing — TDM), позволяющую комбинировать разнообразие базовых скоростей на одной линии. Например, один популярный стандарт DS1 (Digital Signal level 1 — *цифровой сигнальный уровень 1*), или T1, комбинирует в один физический канал со скоростью 1,544 Мбит/с 24 канала DS0 (по 64 Кбит/с) плюс один служебный канал на 8 Кбит/с. Но для обеспечения гибкости предлагаемых клиентам скоростей телефонная компания может установить канал T1 ко многим площадкам, работающим на нескольких более или менее медленных скоростях, кратных скорости 64 Кбит/с.

Теперь вернемся к скорости выделенной линии. Что можно фактически приобрести? В основном из более медленных скоростей можно получить любую скорость, кратную 64 Мбит/с, вплоть до полной скорости канала T1. На более высоких скоростях можно получить скорости, кратные скорости канала T1, вплоть до скорости канала T3 (табл. 12.2).

Таблица 12.2. Скорости сетей WAN

Ключевая тема

Название линии	Скорость передачи информации в битах
DS0	64 Кбит/с
Усеченный T1	Кратно 64 Кбит/с, до 24X

Окончание табл. 12.2

Название линии	Скорость передачи информации в битах
DS1 (T1)	1,544 Мбит/с (24 DS0 до 1,536 Мбит/с, а также служебный канал на 8 Кбит/с)
Усеченный T3	Кратно 1,536 Мбит/с, до 28X
DS3 (T3)	44,736 Мбит/с (28 DS1, а также служебный канал)

Роль модуля CSU/DSU

Этот последний раздел, в котором обсуждаются каналы связи WAN в рабочей корпоративной объединенной сети, посвящен роли модулей CSU/DSU (для краткости называемый модулем CSU). В нескольких следующих подразделах, вплоть до рис. 12.7, подразумевается использование выделенной линии с внешним модулем CSU/DSU (см. рис. 12.4).

ВНИМАНИЕ!

Многие называют блоки CSU/DSU просто блоками CSU.

Модуль CSU располагается между выделенной линией телефонной компании и маршрутизатором; он понимает оба мира и их соглашения на уровне 1. На стороне телефонной компании это означает, что модуль CSU подключен к линии от телефонной компании, поэтому он должен понимать все детали канальной системы T, технологии TDM и знать скорость, используемую телефонной компанией. Модуль CSU следует настроить так, чтобы он соответствовал параметрам телефонной компании и работал на той же скорости. Например, модуль CSU, подключенный к усеченному каналу T1 на 256 Кбит/с, требует совершенно иной конфигурации по сравнению с модулем, подключенным к каналу T1 (1,544 Мбит/с).

На стороне маршрутизатора модуль CSU подключается к маршрутизатору и выполняет роль оборудования DCE или DTE соответственно. Модуль CSU, действуя как устройство DCE (Data Circuit-Terminating Equipment — *терминальное оборудование канала передачи данных*), контролирует скорость маршрутизатора. Маршрутизатор, действуя как устройство DTE (Data Terminal Equipment — *терминальное оборудование*), контролируется синхросигналами от модуля CSU (устройства DCE). Таким образом, модуль CSU указывает маршрутизатору, когда передавать и получать биты; маршрутизатор пытается передавать и получать биты только тогда, когда устройство DCE создает в кабеле соответствующие электрические импульсы (синхроимпульсы).

Концепции устройств DCE и DTE немного похожи на играющего ребенка, готового бросать мячи родителю с такой скоростью, с которой возможно. Но ребенок должен ждать, пока отец крикнет "Давай!". Отец регулярно кричит "Давай! Давай! Давай! Давай!" в том темпе, в котором он может ловить мячи. Модуль CSU/DSU обладает конфигурацией, задающей ему скорость для синхронизации маршрутизатора, где модуль CSU кричит "Давай!", изменяя в последовательном кабеле электрический ток на некоторых проводах (сигналы синхронизации).

На рис. 12.7 представлена схема основных концепций и ролей модулей CSU/DSU.



Рис. 12.7. Роли устройств DCE и DTE для модуля CSU/DSU, а также последовательного интерфейса маршрутизатора

Создание канала связи WAN в лабораторных условиях

Для практических занятий при подготовке к экзаменам CCENT и CCNA вполне можно купить подержанный маршрутизатор и коммутатор для профессиональной практики. Так можно создать эквивалент выделенной линии без реальной выделенной линии от телефонной компании и без модулей CSU/DSU, достаточно описанного ниже трюка с кабелями.

В этом небольшом разделе содержится достаточно информации, для того чтобы создать канал связи WAN в своей домашней лаборатории.

При создании реального канала связи WAN с реальной телефонной компанией между площадками последовательные кабели, обычно используемые между маршрутизатором и внешним модулем CSU/DSU, называют *кабелями DTE* (DTE cable). Например, в концептуальной схеме на рис. 12.4 между каждым маршрутизатором и блоком CSU использовался бы последовательный кабель DTE.

Эквивалентный канал связи WAN можно создать, просто соединив последовательные интерфейсы двух маршрутизаторов, используя один кабель DTE и немного измененный кабель DCE, без модулей CSU и без выделенной линии от телефонной компании. У кабеля DCE есть разъем с гнездом (“мама”), а у кабеля DTE — разъем с вилкой (“папа”), позволяющие соединить эти два кабеля непосредственно. Такое физическое соединение обеспечивает путь для данных. Кабель DCE создает также эквивалент перекрещенного кабели Ethernet, меняя местами пары передающих и принимающих проводов, как показано на рис. 12.8.

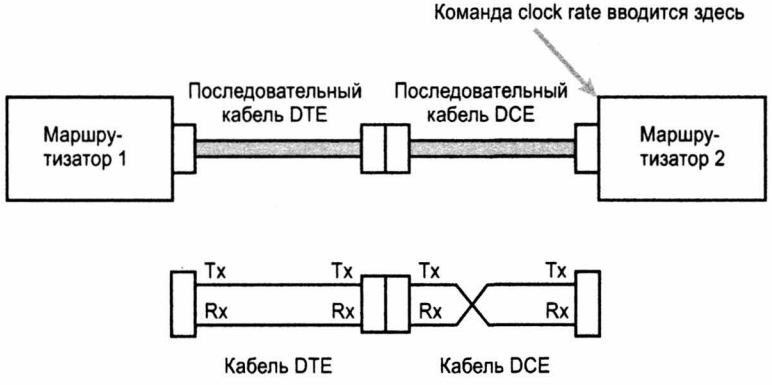


Рис. 12.8. Последовательное соединение использует кабели DTE и DCE

На рис. 12.8, *сверху*, представлены детали соединительных кабелей. На рис. 12.8, *снизу*, показано, что последовательный кабель DTE действует как прямой кабель, а кабель DCE меняет местами передающую и принимающую пары.

ВНИМАНИЕ!

Многие производители для удобства комплектуют устройства единым кабелем, объединяющим в одном оба кабеля, представленных на рис. 12.8. Примеры можно найти при поиске в сети по ключевым словам "Cisco serial crossover".

И наконец, чтобы на маршрутизаторе с подключенным кабелем DCE заработал канал связи, он должен обеспечить синхронизацию. Последовательный интерфейс маршрутизатора способен обеспечить синхронизацию, но это возможно, только если к интерфейсу подключен кабель DCE, а в конфигурации есть команда `clock rate`. (Более новые версии операционной системы IOS позволяют маршрутизатору обнаружить подключенный к последовательному интерфейсу кабель DCE, а без команды `clock rate` в конфигурации маршрутизатор автоматически добавляет ее, чтобы канал связи мог работать.)

Выделенные линии уровня 2 и протокол HDLC

Выделенная линия является службой уровня 1. Другими словами, она обещает доставлять биты, передаваемые между устройствами, соединенными с выделенной линией. Однако сама выделенная линия не определяет используемый ею протокол канального уровня. Одним из возможных протоколов канала связи для выделенной линии является протокол HDLC.

У протокола HDLC лишь несколько больших функций для работы с простой двухточечной топологией двухточечной выделенной линии. В первую очередь заголовок фрейма позволяет получающему маршрутизатору узнать, что поступил новый фрейм. Кроме того, как и у всех других протоколов канала связи, концевик протокола HDLC содержит поле *контрольной суммы фрейма* (Frame Check Sequence — FCS), позволяющее получающему маршрутизатору выяснить, не произошло ли ошибок при передаче фрейма.

Компания Cisco добавила к стандартизированному ISO протоколу HDLC еще одну функцию, введя в заголовок HDLC дополнительное поле (Type) и получив собственную версию Cisco протокола HDLC, как показано на рис. 12.9. Поле Type позволяет маршрутизаторам Cisco поддерживать несколько типов пакетов сетевого уровня, передаваемых через канал связи HDLC. (Оригинальный стандарт HDLC, появившийся задолго до маршрутизаторов, поля Type не имел.) Например, канал связи HDLC между двумя маршрутизаторами Cisco может перенаправить и пакеты IPv4, и IPv6, поскольку поле Type позволяет идентифицировать тип пакета, инкапсулируемого в каждом фрейме HDLC.

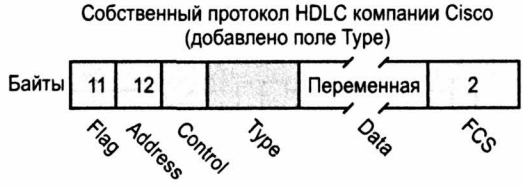


Рис. 12.9. Формат фрейма HDLC

Сейчас у полей Address и Control протокола HDLC немного задач. На канале связи только с двумя маршрутизаторами, когда один маршрутизатор передает фрейм, он однозначно поступит только на другой маршрутизатор канала связи. Важные задачи у полей Address и Control были в минувшие годы, сегодня они не у дел.

ВНИМАНИЕ!

Если интересно, почему у фрейма HDLC есть поле Address вообще, то в прошлом телефонные компании предоставляли и многоточечные каналы. Эти каналы включали несколько устройств, поэтому был возможен больше чем один получатель, а поле адреса позволяло идентифицировать правильного получателя.

Зачастую маршрутизаторы используют HDLC на выделенной линии в качестве протокола канала связи, как показано на рис. 12.10. Маршрутизаторы используют протокол HDLC точно так же, как и любой другой протокол канала связи, для перемещения пакетов на следующий маршрутизатор. На рис. 12.10 показаны три уже знакомых этапа маршрутизации и роль протокола HDLC на этапе 2. (Обратите внимание, что на рисунке не показаны концевики канала связи во фреймах.)

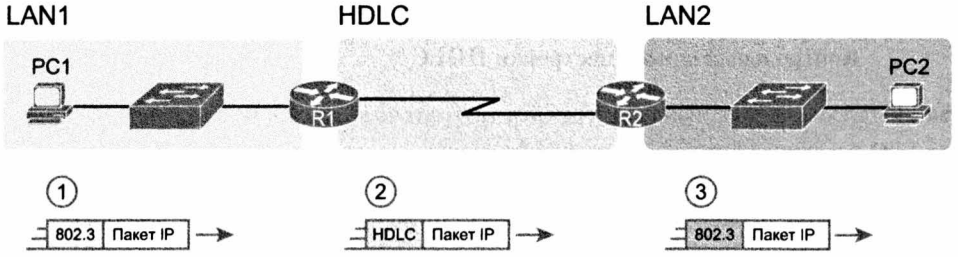


Рис. 12.10. Общая концепция деинкапсуляции и реинкапсуляции пакетов IP маршрутизаторами

Ниже приведено описание этапов на рисунке.

1. Для передачи пакета IP на маршрутизатор R1 компьютер PC1 инкапсулирует пакет IP во фрейме Ethernet.
2. Маршрутизатор R1 деинкапсулирует (извлекает) пакет IP, затем инкапсулирует (помещает) пакет во фрейм HDLC, используя заголовок и концевик HDLC, а потом перенаправляет фрейм HDLC маршрутизатору R2.
3. Маршрутизатор R2 извлекает пакет IP, помещает его во фрейм Ethernet и перенаправляет фрейм Ethernet на компьютер PC2.

Таким образом, выделенная линия с протоколом HDLC создает канал связи WAN между двумя маршрутизаторами, чтобы они могли перенаправить пакеты устройствам в подключенных к ним локальных сетях. Сама выделенная линия обеспечивает физические средства передачи битов в обоих направлениях. Фреймы HDLC обеспечивают средства инкапсуляции пакетов сетевого уровня, чтобы они пересекли канал связи между маршрутизаторами.

Настройка протокола HDLC

Вернемся на мгновение к интерфейсам LAN маршрутизатора. Для перенаправления трафика IP интерфейсам маршрутизатора не требуется никакой настройки,

связанной с уровнями 1 и 2. Если кабель подключен правильно, стандартные параметры уровня 1 вполне приемлемы. Интерфейсы маршрутизатора Ethernet, конечно, используют изначально протокол канала связи Ethernet. Маршрутизатору достаточно задать на интерфейсе IP-адрес и, возможно, включить интерфейс командой `no shutdown`, если интерфейс находится в состоянии `administratively down` (административно отключен).

Аналогично последовательные интерфейсы на маршрутизаторах Cisco не нуждаются в специфических командах конфигурации уровня 1 или 2. Для уровня 1 кабели, конечно же, должны быть проложены, но маршрутизатор пытается использовать последовательный интерфейс, только если отдана команда `no shutdown`. Для уровня 2 операционная система IOS стандартно использует на последовательных интерфейсах протокол HDLC. Подобно интерфейсам Ethernet, последовательные интерфейсы маршрутизатора обычно нуждаются только в команде `ip address` и, возможно, в команде `no shutdown`.

Но для последовательных каналов существует множество необязательных команд. Ниже приведены некоторые из этапов настройки конфигурации с указанием условий, в которых необходимы некоторые команды.



Контрольный список настройки HDLC

Этап 1 Используя подкоманду интерфейса `ip address`, задайте IP-адрес интерфейса

Этап 2 Следующие этапы обязательны только при выполнении определенных условий.

A. Если уже используется подкоманда интерфейса `encapsulation` *`протокол`*, для протокола, отличного от HDLC, разрешите использование протокола HDLC подкомандой интерфейса `encapsulation hdlc`. В качестве альтернативы верните интерфейс к его стандартной настройке инкапсуляции подкомандой интерфейса `encapsulation` *`протокол`*, чтобы отключить текущий протокол.

B. Если линия интерфейса находится в состоянии `administratively down` (административно отключена), включите интерфейс подкомандой интерфейса `no shutdown`.

C. Если последовательный канал является сквозным лабораторным каналом (или эмулятором), задайте в конфигурации частоту синхронизации подкомандой интерфейса `clock rate` *`скорость`*, и только на одном маршрутизаторе с кабелем DCE (команда `show controllers serial` *`номер`*)

Этап 3 Следующая последовательность действий необязательна и не влияет ни на работу канала связи, ни на передачу трафика IP.

A. Настройте скорость канала связи, используя подкоманду интерфейса `bandwidth` *`скорость_в_Кбит/с`*, чтобы она соответствовала фактической скорости канала связи.

B. В целях документирования задайте описание задачи интерфейса, используя подкоманду интерфейса `description` *`текст`*

Практически при настройке маршрутизатора Cisco без имевшейся ранее конфигурации интерфейса и установленного нормально работающего последовательного канала связи с модулем CSU/DSU, вероятно, понадобятся команды конфигурации `ip address` и `no shutdown`.

На рис. 12.11 приведена типичная объединенная сеть, а пример 12.1 демонстрирует соответствующую конфигурацию HDLC. В данном случае последовательный канал был создан со сквозным последовательным каналом в лабораторных условиях и требует этапов 1 (`ip address`) и 2C (`clock rate`) из приведенного выше списка. Он также демонстрирует необязательный этап 3B (`description`).

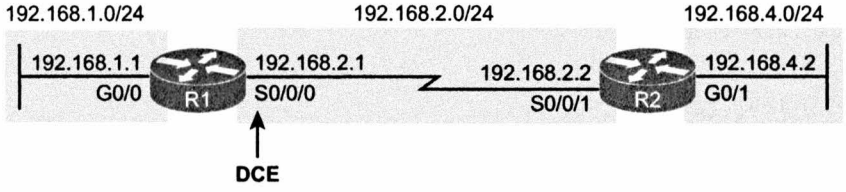


Рис. 12.11. Типичный последовательный канал между двумя маршрутизаторами

Пример 12.1. Конфигурация HDLC

```
R1# show running-config
! Показаны только важные строки
interface GigabitEthernet0/0
  ip address 192.168.1.1 255.255.255.0
!
interface Serial0/0/0
  ip address 192.168.2.1 255.255.255.0
  description link to R2
  clock rate 2000000
!
router eigrp 1
  network 192.168.1.0
  network 192.168.2.0
```

Конфигурация на маршрутизаторе R1 относительно проста. Соответствующая конфигурация на интерфейсе S0/0/1 маршрутизатора R2 просто нуждается в команде `ip address`, а также в стандартных командах `encapsulation hdlc` и `no shutdown`. Команда `clock rate` необязательна на маршрутизаторе R2, поскольку к маршрутизатору R1 подключен кабель DCE, а к маршрутизатору R2 должен быть подключен кабель DTE.

В примере 12.2 приведены две команды, демонстрирующие конфигурацию на маршрутизаторе R1, и некоторые другие стандартные настройки. Сначала приведен вывод команды `show controllers` для интерфейса S0/0/0, подтверждающей, что к маршрутизатору R1 действительно подключен кабель DCE и что была установлена тактовая частота 2000000 битов в секунду. Вначале команда `show interfaces S0/0/0` выводит различные параметры конфигурации, включая стандартное значение инкапсуляции (HDLC) и стандартный параметр ширины полосы пропускания на последовательном интерфейсе (значение 1544 означает 1544 Кбит/с, или 1,544 Мбит/с). Она также выводит IP-адрес, маску в префиксном стиле (/24) и описание, заданные в примере 12.1.

Пример 12.2. Проверка параметров конфигурации на маршрутизаторе R1

```
R1# show controllers serial 0/0/0
Interface Serial0/0/0
Hardware is SCC
DCE V.35, clock rate 2000000
! Строки опущены для краткости

R1# show interfaces s0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is WIC MBRD Serial
  Description: link to R2
  Internet address is 192.168.2.1/24
  MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set
  Keepalive set (10 sec)
  Last input 00:00:01, 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
     276 packets input, 19885 bytes, 0 no buffer
     Received 96 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     284 packets output, 19290 bytes, 0 underruns
     0 output errors, 0 collisions, 5 interface resets
     0 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out
     7 carrier transitions
     DCD=up DSR=up DTR=up RTS=up CTS=up
```

И наконец, маршрутизатор использует последовательный интерфейс, только если он в состоянии up/up, как показано в первой строке вывода команды `show interfaces S0/0/0` примера 12.2. По правде говоря, первое слово состояния относится к уровню 1, а второе — к уровню 2. Для более быстрого выяснения состояния интерфейса можно использовать команду `show ip interface brief` или `show interfaces description`, как показано в примере 12.3.

Пример 12.3. Краткий список интерфейсов и их состояний

```
R1# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     192.168.1.1     YES manual up                    up
GigabitEthernet0/1     unassigned      YES manual administratively down down
Serial0/0/0            192.168.2.1     YES manual up                    up
Serial0/0/1            unassigned      YES NVRAM  administratively down down
Serial0/1/0            unassigned      YES NVRAM  administratively down down
Serial0/1/1            unassigned      YES NVRAM  administratively down down

R1# show interfaces description
Interface              Status         Protocol  Description
```

```
Gi0/0              up             up         LAN at Site 1
Gi0/1              admin down     down
Se0/0/0            up             up         link to R2
Se0/0/1            admin down     down
Se0/1/0            admin down     down
Se0/1/1            admin down     down
```

Протокол PPP в сети WAN на базе выделенных линий

Протокол двухточечного соединения (Point-to-Point Protocol — PPP) выполняет ту же роль, что и протокол HDLC: протокол канала связи для последовательных каналов. Однако протокол HDLC был создан в мире без маршрутизаторов, а определенный в 1990-х годах протокол PPP, напротив, был разработан для работы с маршрутизаторами, протоколом TCP/IP, другими протоколами сетевого уровня и еще с многими другими дополнительными возможностями.

В этом разделе сначала обсуждается концепция протокола PPP, включая один пример дополнительного средства протокола PPP (аутентификация), а завершается он несколькими примерами конфигурации, использующими протокол PPP.

Концепции протокола PPP

Протокол PPP предоставляет несколько простых, но важных функций, которые необходимы для выделенной линии, соединяющей два устройства.

Задачи протокола PPP

Ключевая тема

- Определение заголовка и концевика, обеспечивающих передачу фрейма данных по каналу связи.
- Поддержка синхронных и асинхронных каналов связи.
- Поле Type в заголовке протокола позволяет нескольким протоколам третьего уровня передавать по тому же каналу связи.
- Встроенные инструменты аутентификации: *протокол аутентификации по паролю* (Password Authentication Protocol — PAP) и *протокол аутентификации с предварительным согласованием* (Challenge Handshake Authentication Protocol — CHAP).
- Протоколы управления для каждого протокола более высокого уровня, работающего поверх протокола PPP, облегчают интеграцию и поддержку этих протоколов.

Далее поле протокола, аутентификация и протоколы управления рассматриваются подробней.

Формат фрейма PPP

В отличие от стандартной версии протокола HDLC, стандартная версия протокола PPP определяет поле протокола, которое идентифицирует тип пакета во фрейме. Когда был создан протокол PPP, это поле позволяло передавать по единому каналу связи пакеты многих разных протоколов третьего уровня. Сейчас поле Type протокола все еще выполняет ту же функцию, обеспечивая передачу пакетов, как

правило, двух разных версий протокола IP (IPv4 и IPv6). На рис. 12.12 представлен формат фрейма PPP, очень похожий на таковой у собственного протокола HDLC компании Cisco, включая поле Type протокола (см. рис. 12.9).

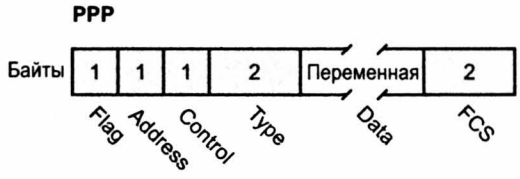


Рис. 12.12. Формат фрейма PPP

Протоколы управления PPP

Кроме подобного HDLC формата фрейма, протокол PPP определяет набор протоколов управления уровня 2, выполняющих различные функции управления каналом связи. Эти дополнительные протоколы немного напоминают дополнительные протоколы Ethernet, такие как *протокол распределенного связующего дерева* (Spanning Tree Protocol — STP). У протокола Ethernet есть заголовки и концевики, обеспечивающие доставку фреймов, а также определение таких вспомогательных протоколов, как STP, облегчающее процесс передачи фрейма. Аналогично протокол PPP определяет формат фрейма (см. рис. 12.12), а также другие протоколы, помогающие контролировать последовательный канал.

Протокол PPP разделяет протоколы управления на две основные категории.

Ключевая тема

Сравнение протоколов LCP и NCP протокола PPP

Протокол управления каналом (Link Control Protocol — LCP). У этого протокола несколько разных индивидуальных функций, каждая из которых сосредоточивается на самом канале связи, игнорируя протокол уровня 3, передающий данные через него.

Протокол управления сетью (Network Control Protocol — NCP). Это категория протоколов, по одному на каждый протокол сетевого уровня. Каждый протокол выполняет функции, специфические для соответствующего протокола уровня 3.

Протокол LCP PPP реализует функции управления, работающие независимо от протокола уровня 3. Для средств, связанных с любыми протоколами более высокого уровня, обычно протоколами уровня 3, протокол PPP использует набор *протоколов управления* (Control Protocol — CP) PPP, таких, как *протокол управления IP* (IP Control Protocol — IPCP). Протокол PPP использует один экземпляр протокола LCP для канала связи и по одному экземпляру протокола NCP для каждого протокола уровня 3, определенного на канале связи. Например, на канале связи PPP, использующем протоколы IPv4, IPv6 и *протокол обнаружения устройств Cisco* (Cisco Discovery Protocol — CDP), должен применяться один экземпляр протокола LCP плюс протокол IPCP (для IPv4), протокол IPv6CP (для IPv6) и CDPCP (для CDP).

В табл. 12.3 приведены функции протокола LCP, названия средства LCP и их краткое описание. После таблицы одно из средств протокола PPP, аутентификация, рассматривается более подробно.

Таблица 12.3. Средства протокола LCP PPP

Функция	Средство LCP	Описание
Обнаружение петлевого канала связи	Магическое число	Обнаруживает зацикливание канала связи и отключает интерфейс, позволяя маршрутизатору найти рабочий маршрут
Обнаружение ошибок	*Контроль качества канала* (Link-quality monitoring — LQM)	Отключает интерфейс, превысивший процентный порог ошибок, обеспечивая маршрутизацию по лучшим маршрутам
Поддержка многоканальной связи	Многоканальный протокол PPP	Балансировка трафика по нескольким параллельным каналам связи
Аутентификация	PAP и CHAP	Обеспечивает обмен именами и паролями, чтобы каждое устройство могло идентифицировать и проверить устройство на другом конце канала связи

Аутентификация PPP

В сети *аутентификация* (authentication) позволяет одному устройству проверить другое устройство, с которым должна осуществляться связь (коммуникация). Другими словами, аутентификация подтверждает подлинность другой стороны.

Например, если маршрутизаторы R1 и R2 общаются по последовательному каналу, используя протокол PPP, то маршрутизатор R1 мог бы потребовать от устройства R2 доказательства того, что оно действительно является маршрутизатором R2. В этом случае маршрутизатор R1 может аутентифицировать маршрутизатор R2 в ходе процесса аутентификации.

Чаще всего аутентификация WAN необходима при использовании коммутируемых линий. Однако настройка средств аутентификации остается той же, независимо от того, используется ли выделенная или коммутируемая линия.

Протокол PPP определяет два протокола аутентификации: PAP и CHAP. Оба протокола требуют обмена сообщениями между устройствами, но с разными подробностями. При протоколе PAP аутентифицируемое устройство заявляет о себе сообщением, содержащим секретный пароль в виде открытого текста, как показано на рис. 12.13.

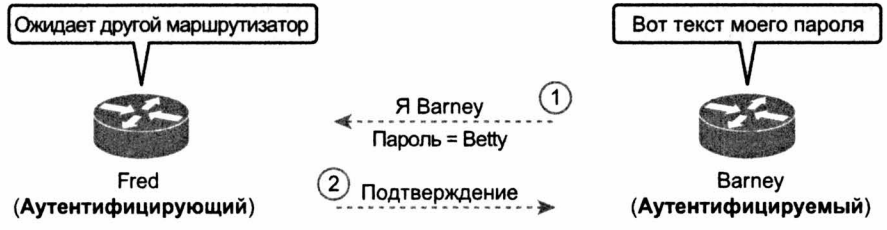


Рис. 12.13. Процесс аутентификации PAP

На рис. 12.13 показано, что при установке канала связи аутентификация происходит в два этапа. На этапе 1 устройство Barney передает совместно используемый пароль в открытом виде. Устройство Fred, желающее аутентифицировать устрой-

ство Barney (т.е. удостовериться, что Barney — это на самом деле Barney), видит пароль и, убедившись в его правильности, отсылает назад подтверждение, что Barney прошел процесс аутентификации.

Протокол CHAP защищен много лучше, он использует другие сообщения и скрывает пароль. Аутентифицирующее устройство (Fred) начинает с передачи сообщения *challenge* (вызов), запрашивающего ответ от другого устройства. Главное отличие в том, что ответное сообщение скрывает аутентификационный пароль, как показано на рис. 12.14, он посылает хешированную версию пароля. Если устройство Fred подтверждает правильность хешированного пароля, то оно отсылает третье сообщение, подтверждающее успех аутентификации.

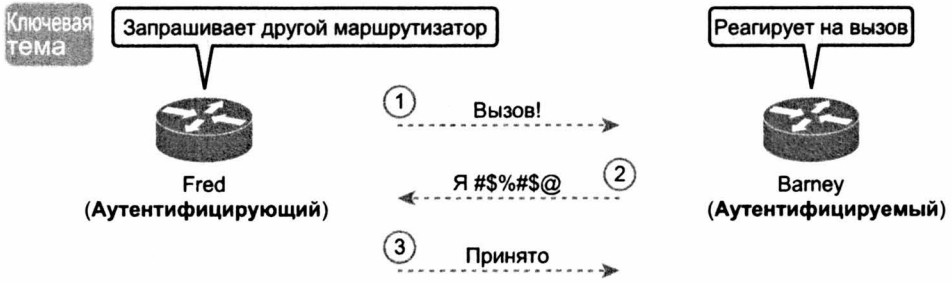


Рис. 12.14. Процесс аутентификации CHAP

И рис. 12.13, и 12.14 демонстрируют последовательности успешной аутентификации. При неудаче (например, при неподходящем пароле) передается другое заключительное сообщение. Кроме того, при неудаче аутентификации протокол PPP оставляет интерфейс в состоянии `up/down`, и маршрутизатор больше не может передавать и получить фреймы через него.

Протокол PAP менее защищен, чем протокол CHAP, поскольку он передает имя хоста и пароль в открытом текстовом сообщении. Их можно легко прочитать, если некто подключит к каналу связи инструмент трассировки. Вместо этого протокол CHAP использует односторонний алгоритм хеширования MD5 (Message Digest 5), получающий пароль, никогда не передающийся по каналу связи, а также совместно используемое случайное число.

Кроме того, протокол CHAP использует хешированное значение только один раз, чтобы злоумышленник не мог просто скопировать его и послать позднее. Для этого вызов CHAP (первое сообщение) сообщает случайное число. Вызываемый маршрутизатор запускает алгоритм хеширования, используя полученное случайное число и секретный пароль, а результат отсылает назад, на пославший вызов маршрутизатор. Последний запускает тот же алгоритм, используя случайное число (посланное им по каналу связи) и пароль (хранящийся локально); если результаты совпадают, то пароль принимается. Впоследствии, при следующей аутентификации, аутентифицирующий маршрутизатор создаст и использует другое случайное число.

Протоколы PAP и CHAP — это лишь некоторые из протоколов управления каналом PPP. В следующем разделе рассматривается настройка и проверка протокола PPP.

Настройка протокола PPP

По сравнению с протоколом HDLC, настройка протокола PPP требует только одного изменения: применения команды `encapsulation ppp` на обоих концах канала связи. Как и у протокола HDLC, здесь можно дополнительно задать и другие элементы, такие как ширина полосы пропускания интерфейса (`bandwidth`) и описание интерфейса (`description`). Кроме того, интерфейс, безусловно, следует включить (`no shutdown`). Перевод конфигурации с протокола HDLC на PPP требует лишь команды `encapsulation ppp` на последовательных интерфейсах обоих маршрутизаторов.

В примере 12.4 приведена базовая конфигурация, использующая два маршрутизатора, представленных на рис. 12.11, и ту же объединенную сеть, что и для примера протокола HDLC. Пример включает настройку IP-адресов, но для работы протокола PPP это не обязательно.

Пример 12.4. Базовая настройка протокола PPP

```
! Пример начинается на маршрутизаторе R1
interface Serial0/0/0
  ip address 192.168.2.1 255.255.255.0
  encapsulation ppp
  clockrate 2000000
! ------------------------------------------------------------------------
! Далее следует настройка на маршрутизаторе R2
interface Serial0/0/1
  ip address 192.168.2.2 255.255.255.0
  encapsulation ppp
```

Команда `show interfaces` в примере 12.5 выводит подробности протокола PPP на маршрутизаторе R1. Вывод выглядит точно так же, как и для протокола HDLC, вплоть до первой выделенной строки. Две выделенные строки подтверждают конфигурацию ("`Encapsulation PPP`"), а также то, что протокол LCP закончил свою работу успешно, как свидетельствует фраза "`LCP Open`". И наконец, вывод демонстрирует тот факт, что оба протокола управления (CP), CDPCP и IPCP, также были успешно разрешены. Все это подтверждает правильную работу протокола PPP.

Пример 12.5. Выяснение состояния протоколов PPP, LCP и NCP при помощи команды `show interfaces`

```
R1# show interfaces serial 0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is WIC MBRD Serial
  Description: link to R2
  Internet address is 192.168.2.1/24
  MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
  Open: IPCP, CDPCP, loopback not set
! Строки опущены для краткости
```

Настройка и проверка аутентификации CHAP

В простейшем варианте использования аутентификации CHAP нужно ввести всего несколько команд. В конфигурации аутентификации используется пароль, указанный локально в каждом из устройств. Как альтернатива может быть использована служба *аутентификации, авторизации и учета* (Authentication, Authorization, and Accounting — AAA), в которой все учетные записи задаются на специализированном сервере, а не маршрутизаторе.

Для перехода от конфигурации, использующей только протокол PPP, к конфигурации, в которую добавлена аутентификация CHAP, необходимо пройти следующие этапы.

Ключевая тема

Список команд для настройки аутентификации CHAP

Этап 1 Укажите названия устройств с помощью команды `hostname` *имя* в режиме глобальной конфигурации маршрутизатора

Этап 2 С помощью команды `username` *имя* `password` *пароль* в глобальном режиме конфигурации задайте параметры аутентификации дистанционного устройства. В качестве имени пользователя используется имя (hostname) дистанционного маршрутизатора, в качестве пароля — пароль привилегированного пользователя

Этап 3 Включите аутентификацию CHAP в соответствующих интерфейсах маршрутизаторов с помощью команды `ppp authentication chap`

На рис. 12.15 показана конфигурация на маршрутизаторах R1 и R2, разрешающая протоколы PPP и CHAP на канале связи. Рисунок демонстрирует, что имя в команде `hostname` на одном маршрутизаторе должно соответствовать имени в команде `username` на другом маршрутизаторе. Кроме того, здесь также показано, что пароли (в данном случае `mypass`), определенные в каждой команде `username`, также должны совпадать.

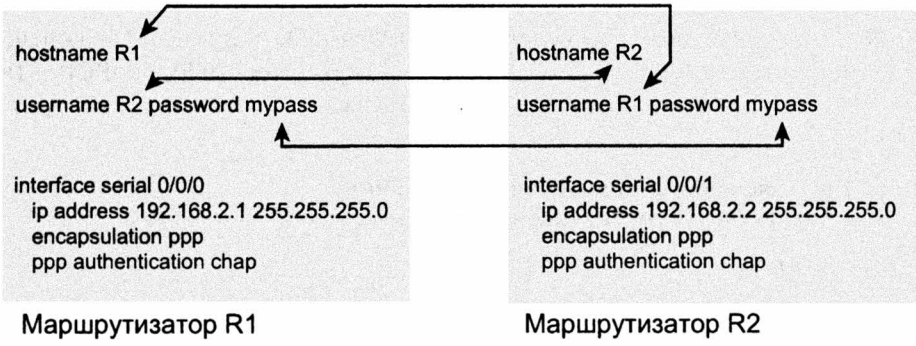


Рис. 12.15. Конфигурация CHAP

Поскольку аутентификация CHAP является функцией протокола LCP, то, если аутентификация заканчивается неудачно, протокол LCP приостанавливает работу и интерфейс переходит в состояние "`up`" и "`down`" (физический уровень включен, канальный — выключен).

Поиск и устранение неисправностей в последовательных каналах

В этом разделе описано, как локализовать и устранять проблемы, связанные с каналами WAN, в частности, с двухточечными соединениями, которые были также описаны в томе I. В данном разделе не повторяются темы, связанные с поиском и устранением неисправностей в технологиях IP, описанных в предыдущих частях, а основное внимание уделяется именно технологиям уровня 2 эталонной модели в последовательных каналах.

С помощью простой команды `ping` можно установить, возможно ли пересылать через последовательный канал пакеты IP. Например, используя команду `ping 192.168.2.2` в схеме сети, представленной на рис. 12.11, используемом и для примеров конфигурации HDLC и PPP, для маршрутизатора R1, можно убедиться в работоспособности канала или подтвердить его отказ.

Если команда `ping` возвращает отрицательный результат, то проблема может быть связана с уровнями 1 и 2, а также с уровнем 3. Проще всего локализовать наиболее вероятную причину отказа — это просмотреть коды состояния интерфейса, которые приведены в табл. 12.4.

Таблица 12.4. Коды состояния интерфейсов и их значение, если команда `ping` возвращает отрицательный результат

Ключевая тема

Код состояния канала	Код состояния протокола	Вероятная причина/уровень
Administratively down	Down	Интерфейс выключен
Down	Down	Уровень 1
Up	Down	Уровень 2
Up	Up	Уровень 3

Процесс поиска неисправностей в последовательном канале состоит из трех простых этапов.

Этап 1 Из локального маршрутизатора необходимо проверить командой `ping` IP-адрес дистанционного устройства на последовательном канале

Этап 2 Если команда `ping` возвращает отрицательный результат для обоих маршрутизаторов, скорее всего, проблема связана с нижними уровнями. Обратитесь к приведенной далее табл. 12.4

Этап 3 Если команда `ping` возвращает положительный результат, проверьте, обменивается ли протокол маршрутизации маршрутной информацией через данный канал, как обсуждалось в главе 11

ВНИМАНИЕ!

Коды состояния интерфейсов можно просмотреть с помощью команд `show interfaces`, `show ip interface brief` и `show interfaces description`.

Ниже подробно рассмотрены ситуации, в которых команда `ping` возвращает отрицательный результат, и комбинации кодов, представленные в табл. 12.4.

Поиск и устранение неисправностей уровня 1

Коды состояния интерфейсов, обычно называемые состояниями интерфейсов, играют ключевую роль в процессе локализации проблем в последовательных каналах распределенных сетей. На практике коды состояний на разных концах канала могут отличаться, поэтому следует проверять оборудование и интерфейсы с двух сторон, чтобы точнее диагностировать проблему.

Например, последовательный канал отключается при административном отключении последовательного интерфейса на любом из двух маршрутизаторов подкомандой интерфейса `shutdown`. Когда один маршрутизатор отключает свой последовательный интерфейс, другой маршрутизатор переходит в состояние `down/down` (состояние линии `down`, состояние протокола линии `down`), даже если второй маршрутизатор не отключен. Для устранения проблемы достаточно настроить на интерфейсе команду конфигурации `no shutdown`.

Состояние линии `down` последовательных интерфейсов на обоих концах последовательного канала (т.е. оба конца в состоянии `down/down`) обычно указывает на некую проблему уровня 1. Наиболее известные причины этого состояния приведены на рис. 12.16. У последовательного интерфейса маршрутизатора R2 никаких проблем нет вообще, а на рис. 12.16, *в центре* и *слева*, показаны наиболее распространенные первопричины, по которым последовательный интерфейс маршрутизатора R2 переходит в состояние `down/down`.

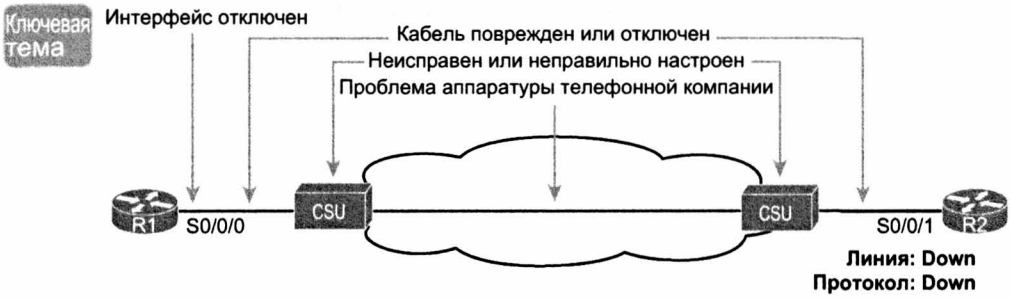


Рис. 12.16. Проблемы, приводящие к состоянию `down/down` на маршрутизаторе R2

Поиск и устранение неисправностей уровня 2

Проблемы канального уровня на последовательных каналах обычно приводят к состоянию `up/down` последовательного интерфейса по крайней мере одного из маршрутизаторов. Другими словами, состояние линии (первый код состояния) — `up`, а второе состояние (состояние протокола линии) — `down`. Типы этих проблем приведены в табл. 12.5.

ВНИМАНИЕ!

Как и в других главах этой книги, посвященных поиску и устранению неисправностей, в табл. 12.5 перечислены наиболее распространенные проблемы, но далеко не все.

Таблица 12.5. Наиболее вероятные причины неработоспособности канального уровня (уровня 2) в последовательных каналах

Ключевая тема

Код состояния линии	Код состояния протокола	Наиболее вероятная причина неработоспособности
Up	Down (стабильно) на двух концах канала[1]	На концах канала указаны разные протоколы с помощью команды `encapsulation`
Up	Down на одном конце канала, Up — на другом	Тестовые пакеты (keepalive) отключены на том конце канала, который находится в рабочем состоянии
Up	Down на обоих концах канала	Аутентификация PAP/CHAP была неудачной

[1]В данном случае состояние может изменяться с `up/up` на `up/down`, потом снова `up/up` и так далее, в то время как маршрутизатор продолжает попытки наладить работу инкапсуляции.

Первая из указанных в табл. 12.5 проблем — несоответствие протоколов канального уровня на разных концах канала — выявляется и исправляется очень просто. С помощью команды `show interfaces` можно посмотреть, какой тип инкапсуляции указан (в строке 7 вывода команды) для интерфейса. Альтернативный вариант — просмотреть конфигурацию устройства и выяснить, какая инкапсуляция указана для интерфейсов. При этом следует помнить, что по умолчанию в маршрутизаторах Cisco используется инкапсуляция HDLC. Решить проблему просто: следует изменить в одном из маршрутизаторов инкапсуляцию для интерфейса с помощью команды `encapsulation`, чтобы она совпадала на разных концах канала.

Вторая проблема в интерфейсах последовательных каналов требует более детального обсуждения, чтобы понять, каковы ее симптомы и последствия. В следующем разделе эта проблема рассматривается достаточно подробно.

Отказ тестового пакета

Тестовые пакеты (keepalive) позволяют маршрутизатору выяснить, что канал связи больше не работает. Как только маршрутизатор обнаруживает, что канал связи больше не работает, он может перевести интерфейс в состояние `down`, позволяя протоколу маршрутизации использовать конвергенцию для поиска другого маршрута, если он есть.

Стандартно маршрутизаторы посылают друг другу сообщения keepalive каждые 10 секунд. Сообщение keepalive для протокола HDLC — это собственное сообщение Cisco, в то время как протокол PPP определяет сообщение keepalive как часть протокола LCP. Оба протокола используют *интервал keepalive* (keepalive interval) — период времени между тестовыми пакетами.

Регулярное прохождение тестовых пакетов свидетельствует об исправности соединения, в то время как их отсутствие — о нарушении канала связи. В частности, если маршрутизатор не получает сообщений keepalive от другого маршрутизатора на протяжении нескольких интервалов keepalive (стандартно трех или пяти, в зависимости от версии IOS), маршрутизатор отключает интерфейс, полагая, что интерфейс другого маршрутизатора больше не работает. Пока оба маршрутизатора передают тестовые пакеты, или если они отключены на обоих маршрутизаторах, канал связи работает.

Но если на одном конце канала тестовые пакеты отключены, а на другом включены, произойдет ошибка. Эта ошибка нарушает только каналы связи HDLC; протокол PPP эту проблему предотвращает. На рис. 12.17 приведен пример, когда при протоколе HDLC на маршрутизаторе R1 по ошибке были отключены тестовые пакеты.

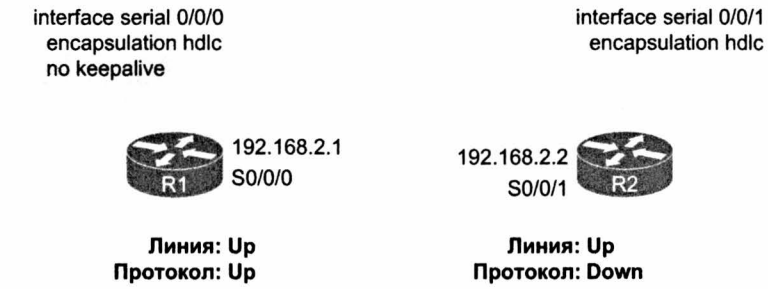


Рис. 12.17. Причины состояния `down/down` *на маршрутизаторе R2*

В случае, приведенном на рис. 12.17, интерфейс маршрутизатора R2 отключился потому, что

- маршрутизатор R1 не посылает сообщений keepalive, так как они отключены;
- маршрутизатор R2 все еще ожидает получения сообщений keepalive, поскольку они еще включены.

Не получив сообщений keepalive на протяжении достаточно многих интервалов keepalive, маршрутизатор R2 переводит канал связи в состояние `up/down`. Через некоторое время маршрутизатор R2 может перевести канал связи в состояние `up/up`, а затем еще через три интервала keepalive вернуть его назад в состояние `up/down`.

Пример 12.6 демонстрирует поиск доказательств рассогласования разрешений на передачу сообщений keepalive. В начале примера содержится вывод команды `show interfaces S0/0/0` на маршрутизаторе R1, где выделенная строка подтверждает наличие в конфигурации маршрутизатора R1 параметра `no keepalive`. В примере показана та же команда на маршрутизаторе R2, что подтверждает разрешение тестовых пакетов и состояние интерфейса `up/down`.

Пример 12.6. Проблемы линии, вызванные разрешением тестовых пакетов только на маршрутизаторе R2

```
! На R1 тестовые пакеты отключены, он остается в состоянии up/up.
R1# show interfaces s0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is WIC MBRD Serial
  Description: link to R2
  Internet address is 192.168.2.1/24
  MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set
  Keepalive not set
! Строки опущены для краткости
! ------------------------------------------------------------
! На R2 тестовые пакеты все еще включены (стандартно)
```

```
R2# show interfaces S0/0/1
Serial0/0/1 is up, line protocol is down
  Hardware is WIC MBRD Serial
  Internet address is 192.168.2.2/24
  MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set
  Keepalive set (10 sec)
! Строки опущены для краткости
```

Ошибки в аутентификации CHAP и PAP

Как было сказано выше, неудачная аутентификация PAP/CHAP (т.е. когда имя или пароль пользователя неправильные) приведет к тому, что коды состояний интерфейсов маршрутизатора в канале будут "up" и "down" (канал включен, протокол выключен). Чтобы убедиться в том, что именно аутентификация является причиной такого кода состояния интерфейса, следует ввести команду `debug ppp authentication`. В примере 12.7 показан вывод такой команды для протокола аутентификации CHAP (который настроен так, как показано в примере 12.5). В данном примере аутентификация CHAP работает корректно.

Пример 12.7. Отладочные сообщения при корректной аутентификации CHAP

```
R1# debug ppp authentication
PPP authentication debugging is on
R1#
*Nov 18 23:34:30.060: %LINK-3-UPDOWN: Interface Serial0/0/0, changed
state to up
*Nov 18 23:34:30.060: Se0/0/0 PPP: Using default call direction
*Nov 18 23:34:30.060: Se0/0/0 PPP: Treating connection as a dedicated
line
*Nov 18 23:34:30.060: Se0/0/0 PPP: Session handle[58000009] Session id[7]
*Nov 18 23:34:30.064: Se0/0/0 CHAP: O CHALLENGE id 1 len 23 from "R1"
*Nov 18 23:34:30.084: Se0/0/0 CHAP: I CHALLENGE id 1 len 23 from "R2"
*Nov 18 23:34:30.084: Se0/0/0 PPP: Sent CHAP SENDAUTH Request
*Nov 18 23:34:30.084: Se0/0/0 CHAP: I RESPONSE id 1 len 23 from "R2"
*Nov 18 23:34:30.084: Se0/0/0 PPP: Received SENDAUTH Response PASS
*Nov 18 23:34:30.084: Se0/0/0 CHAP: Using hostname from configured host-
name
*Nov 18 23:34:30.084: Se0/0/0 CHAP: Using password from AAA
*Nov 18 23:34:30.084: Se0/0/0 CHAP: O RESPONSE id 1 len 23 from "R1"
*Nov 18 23:34:30.084: Se0/0/0 PPP: Sent CHAP LOGIN Request
*Nov 18 23:34:30.084: Se0/0/0 PPP: Received LOGIN Response PASS
*Nov 18 23:34:30.088: Se0/0/0 CHAP: O SUCCESS id 1 len 4
*Nov 18 23:34:30.088: Se0/0/0 CHAP: I SUCCESS id 1 len 4
```

В протоколе CHAP используется трехэтапный процесс, показанный на рис. 12.14, сообщения пересылаются в обоих направлениях, т.е. обоими устройствами. Три выделенные строки относятся к процессу аутентификации маршрутизатором R1 устройства R2 следующим образом.

1. Эта строка ссылается на сообщение Challenge протокола CHAP, посланное маршрутизатором R1, а символ O означает "output" (вывод). Конец строки свидетельствует о том, что сообщение послано маршрутизатором с именем хоста R1.
2. Эта строка ссылается на сообщение Response протокола CHAP, посланное маршрутизатором R2, а символ I означает "input" (ввод), свидетельствуя, что сообщение поступило на маршрутизатор R1.
3. Эта строка ссылается на сообщение Success протокола CHAP, посланное (O) маршрутизатором R1. Оно свидетельствует об успешной аутентификации.

Здесь можно также увидеть те же три сообщения для аутентификации устройства R2 на маршрутизаторе R1, но в примере они не выделены.

При неудачной аутентификации CHAP вывод команды debug демонстрируют несколько вполне очевидных сообщений. В примере 12.8 приведен результат, при этом используется та же объединенная сеть с двумя маршрутизаторами (см. рис. 12.15), что и в примере конфигурации CHAP. Но на сей раз пароль не подошел и протокол CHAP потерпел неудачу.

Пример 12.8. Отладочные сообщения, подтверждающие отказ протокола CHAP

```
R1# debug ppp authentication
PPP authentication debugging is on
! Строки опущены для краткости
*Nov 18 23:45:48.820: Se0/0/0 CHAP: O CHALLENGE id 1 len 23 from "R1"
*Nov 18 23:45:48.820: Se0/0/0 CHAP: I RESPONSE id 1 len 23 from "R2"
*Nov 18 23:45:48.820: Se0/0/0 CHAP: O FAILURE id 1 len 25 msg is "Authen-
tication failed"
```

Поиск и устранение неисправностей уровня 3

В самом начале главы было сказано, что процесс поиска и устранения неисправностей в последовательном канале лучше всего начинать с проверки пакетами ping IP-адреса интерфейса маршрутизатора на другом конце канала. Следует отметить, что, даже если интерфейс находится в состоянии "up" и "up" (канал включен, протокол включен), проверка ping все равно может давать отрицательный результат из-за ошибок в конфигурации уровня 3. В некоторых случаях проверка ping может быть успешной, но протоколы маршрутизации могут не работать. В этом достаточно коротком разделе описаны признаки, которые несколько различаются в протоколах HDLC и PPP, а также перечислены соответствующие им ошибки.

Сначала рассмотрим протокол HDLC, предполагая, что физический и канальный уровни соединения работают корректно. В таком случае у обоих маршрутизаторов интерфейсы будут находиться в состоянии "up" и "up" (физический уровень включен, протокол включен). Тем не менее, если IP-адреса последовательных интерфейсов двух маршрутизаторов принадлежат разным подсетям, проверка ping даст отрицательный результат, поскольку у маршрутизаторов нет соответствующих маршрутов. Например, если в схеме сети на рис. 12.7 IP-адрес последовательного интерфейса маршрутизатора R1 будет 192.168.2.1, а для последовательного интерфейса маршрутизатора R2 указать адрес 192.168.3.2 (вместо 192.168.2.2) с маской

подсети /24, напрямую подключенные к устройствам подсети будут разными и соответственно разными будут и маршруты. В такой ситуации у устройств не будет маршрутов, совпадающих с подсетью противоположного конца канала, и IP-адреса интерфейса.

Найти и исправить ошибку, связанную с несовпадающими подсетями в протоколе HDLC, относительно просто. Обнаружить проблему можно с помощью проверки `ping` IP-адреса противоположного конца канала — она даст отрицательный результат. Если оба кода состояния интерфейсов на разных концах канала показывают рабочее состояние линии и протокола, то проблема, скорее всего, как раз и состоит в несоответствии IP-адресов.

Для каналов связи PPP с рассогласованием в конфигурации IP-адреса и маски проверка `ping` IP-адреса другого маршрутизатора фактически проходит. Но несовпадение подсетей IP предотвращает формирование соседских отношений EIGRP и OSPF, поэтому имеет смысл следовать правилам и поместить IP-адреса обоих последовательных интерфейсов в ту же подсеть.

Протокол PPP позволяет сработать команде `ping` при несоответствии подсетей за счет добавления к маршруту хоста длины префикса /32 для IP-адреса другого маршрутизатора. Это осуществляется в ходе работы протокола управления IP. Именно этот случай демонстрируется в примере 12.9.

ВНИМАНИЕ!

Маршрут с префиксом /32 называют *маршрутом хоста*.

Пример 12.9. Успешная проверка `ping` в соединении PPP, когда подсети интерфейсов не совпадают

```
R1# show ip route
! Легенда опущена для краткости
    192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C      192.168.1.0/24 is directly connected, GigabitEthernet0/0
L      192.168.1.1/32 is directly connected, GigabitEthernet0/0
     192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.2.0/24 is directly connected, Serial0/0/0
L       192.168.2.1/32 is directly connected, Serial0/0/0
      192.168.3.0/32 is subnetted, 1 subnets
C       192.168.3.2 is directly connected, Serial0/0/0

R1# ping 192.168.3.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

По первой выделенной строке в примере можно определить, что в таблице маршрутизации устройства есть нормальный маршрут к напрямую подключенной подсети 192.168.2.0/24. С точки зрения маршрутизатора R1 эта подсеть подключена к интерфейсу S0/0/0, поскольку в нее попадает его IP-адрес 192.168.2.1/24. Во второй выделенной строке виден маршрут хоста, созданный протоколом PPP, соответ-

ствующий новому IP-адресу последовательного интерфейса маршрутизатора R2 (192.168.3.2). У маршрутизатора R2 будет похожий маршрут, 192.168.2.1/32, к противоположному концу канала. Следовательно, у обоих устройств будут маршруты, которые они могут использовать для пересылки пакетов IP на другой конец канала, даже при том, что адрес другого маршрутизатора находится в другой подсети. Поэтому команда `ping` будет возвращать положительный результат, несмотря на то, что маршрутизаторы настроены неправильно.

В табл. 12.6 приведено сравнение протоколов HDLC и PPP в последовательных каналах, когда IP-адреса интерфейсов относятся к разным подсетям (предполагается, что других ошибок нет).

Таблица 12.6. Признаки, связанные с несовпадающими подсетями на разных концах последовательного канала

Признак	HDLC	PPP
Проверка `ping` противоположного конца канала дает положительный результат	Нет	Да
Протоколы маршрутизации могут обмениваться маршрутной информацией через канал	Нет	Нет

Обзор

Резюме

- Хотя выделенная линия и предоставляет средство передачи битов на физическом уровне, для передачи битов по каналу связи маршрутизаторы должны также использовать на канале связи WAN протокол канала связи.
- При установке выделенной линии инженер должен выбрать правильный тип кабеля с разъемами, подходящими к плате WIC на одном конце и модулю CSU/DSU на другом.
- Модуль CSU располагается между выделенной линией телефонной компании и маршрутизатором; он воспринимает оба мира и их соглашения на уровне 1.
- Сама выделенная линия не определяет протокол канального уровня, используемый на выделенной линии.
- Протокол HDLC предоставляет одну возможность для протокола канала связи, но протокол двухточечного соединения канала передачи данных (уровня 2) специально разработан для облегчения связи по выделенным линиям.
- Протокол PPP определяет два типа управляющих сообщений.
- Протоколы PAP и CHAP используются для аутентификации конечных точек канала связи PPP.
- Тестовые пакеты позволяют маршрутизатору выяснить, что канал связи больше не работает.
- При неудачной аутентификации протоколы PAP и CHAP переводят оба маршрутизатора в состояние "`up/down`".
- Для каналов связи PPP с рассогласованием в конфигурации IP-адреса и маски проверка `ping` IP-адреса другого маршрутизатора фактически проходит. Но несовпадение подсетей IP предотвращает формирование соседских отношений EIGRP и OSPF.

Контрольные вопросы

Ответьте на эти вопросы. Ответы можно найти на последней странице главы. Полное объяснение ответов приведено в приложении B на веб-сайте.

1. Что из следующего обычно подключается к четырехжильному кабелю выделенной линии, предоставляемой телефонной компанией?

   А) Последовательный интерфейс маршрутизатора без внутреннего модуля CSU/DSU.

   Б) Модуль CSU/DSU.

   В) Последовательный интерфейс маршрутизатора с внутренним трансивером (transceiver).

   Г) Последовательный интерфейс коммутатора.

2. Какие из следующих полей в заголовке HDLC, используемом маршрутизаторами Cisco, компания Cisco добавила помимо стандарта ISO HDLC?

   А) Flag.

   Б) Type.

   В) Address.

   Г) FCS.

3. Два маршрутизатора соединены последовательным каналом, каждый использует свой интерфейс S0/0/0. В настоящее время канал связи работает, используя протокол PPP. Сетевой инженер хочет перейти на использование собственного протокола HDLC компании Cisco, включающего поле типа протокола. Какие из следующих команд применяются для успешного перехода на протокол HDLC? (Выберите два ответа.)

   А) `encapsulation hdlc`.

   Б) `encapsulation cisco-hdlc`.

   В) `no encapsulation ppp`.

   Г) `encapsulation-type auto`.

4. В каком из методов аутентификации протокола PPP пароль не передается в виде открытого текста?

   А) MD5.

   Б) PAP.

   В) CHAP.

   Г) DES.

5. Есть два маршрутизатора без какой-либо конфигурации. Они соединены друг с другом в лабораторной сети, при этом кабель DTE подключен к маршрутизатору R1, а кабель DCE — к маршрутизатору R2. Сетевой инженер хочет установить соединение PPP между устройствами. Какие из команд нужно ввести в маршрутизаторе R1, чтобы устройства могли обмениваться пакетами ping, если на физическом уровне лабораторное подключение работает правильно? (Выберите два ответа.)

   А) `encapsulation ppp`.

   Б) `no encapsulation hdlc`.

   В) `clock rate`.

   Г) `ip address`.

6. В результате выполнения некоторой команды группы `show` была получена следующая информация.

```
Serial0/0/1 is up, line protocol is up
  Hardware is GT96K Serial
  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 PPP, LCP Open
  Open: CDPCP, IPCP, loopback not set
```

   Что из перечисленного ниже справедливо для интерфейса S0/0/1? (Выберите два ответа.)

А) В интерфейсе используется инкапсуляция HDLC.

Б) В интерфейсе используется инкапсуляция PPP.

В) В настоящий момент через интерфейс не может быть передан трафик протокола IPv4.

Г) Через данный канал в настоящий момент могут передаваться фреймы протокола PPP.

7. В результате выполнения команды `show interfaces` была получена следующая информация для интерфейса, в котором настроен протокол PPP.

```
Serial0/0/1 is up, line protocol is down
  Hardware is GT96K Serial
  Internet address is 192.168.2.1/24
```

Поверка противоположного конца канала командой `ping` дает отрицательный результат. Каковы причины неработоспособности соединения, если предположить, что проблемы могут быть связаны только непосредственно с каналом? (Выберите два ответа.)

А) Модуль CSU/DSU, подключенный к маршрутизатору на другом конце канала, выключен.

Б) IP-адрес, заданный на интерфейсе маршрутизатора на другом конце канала, не принадлежит подсети 192.168.2.0/24.

В) Аутентификация CHAP была неудачной.

Г) В интерфейсе маршрутизатора на другом конце канала настроена инкапсуляция HDLC.

Д) Все ответы не верны.

Ключевые темы

Повторите все ключевые темы данной главы, отмеченные пиктограммой "Ключевая тема". Ключевые темы и соответствующие им страницы указаны в табл. 12.7.

Таблица 12.7. Ключевые темы главы 12

Элемент	Описание	Страница
Рис. 12.4	Двухточечная выделенная линия: компоненты и терминология	411
Табл. 12.2	Скорости сетей WAN	413
Рис. 12.7	Роли устройств DCE и DTE для модуля CSU/DSU, а также последовательного интерфейса маршрутизатора	415
Список	Контрольный список настройки HDLC	418
Список	Задачи протокола PPP	421
Список	Сравнение протоколов LCP и NCP протокола PPP	422
Рис. 12.14	Процесс аутентификации CHAP	424
Список	Список команд для настройки аутентификации CHAP	426
Рис. 12.16	Проблемы, приводящие к состоянию down/down на маршрутизаторе R2	428
Табл. 12.5	Наиболее вероятные причины неработоспособности канального уровня (уровня 2) в последовательных каналах	429

Заполните таблицы и списки по памяти

Распечатайте приложение Г с веб-сайта или его раздел, относящийся к этой главе, и заполните таблицы и списки по памяти. В приложении Д приведены заполненные таблицы и списки для самоконтроля.

Ключевые термины

После первого прочтения главы попытайтесь дать определения следующим ключевым терминам. Но не расстраивайтесь, если не все получится сразу, в главе 22 описано, как использовать эти термины на завершающем этапе подготовки к экзамену.

выделенная линия (leased line), телефонная компания (telco), последовательный канал (serial link), канал связи WAN (WAN link), линия T1 (T1), цифровой сигнал уровня 0 (Digital Signal level 0 — DS0), цифровой сигнал уровня 1 (Digital Signal level 1 — DS1), линия T3 (T3), абонентское оконечное оборудование (Customer Premise Equipment — CPE), модуль обслуживания канала/модуль обработки данных (Channel Service Unit/Data Service Unit — CSU/DSU), последовательный кабель (serial cable), оконечное оборудование канала передачи данных (Data Circuit-terminating Equipment — DCE), терминальное оборудование (Data Terminal Equipment — DTE), высокоуровневый протокол управления каналом (High-Level Data Link Control — HDLC), протокол двухточечного соединения (Point-to-Point Protocol — PPP), протокол аутентификации с предварительным согласованием вызова (Challenge Handshake Authentication Protocol — CHAP), протокол управления IP (IP Control Protocol — IPCP), тестовый пакет (keepalive), протокол управления каналом (Link Control Protocol — LCP)

Таблицы команд

Хоть и не обязательно заучивать информацию из таблиц данного раздела, ниже приведен список команд конфигурации и пользовательских команд главы. Фактически команды стоит запомнить, чтобы лучше понять содержимое главы и выполнить задания по подготовке к экзамену. Чтобы проверить, насколько хорошо вы запомнили команды, закройте левую сторону таблицы листом бумаги, читайте описания с правой стороны и пытайтесь вспоминать команду.

Таблица 12.8. Конфигурационные команды главы 12

Команда	Описание
`encapsulation {hdlc | ppp}`	Подкоманда интерфейса, задающая протокол последовательного канала передачи данных
`[no] shutdown`	Интерфейс административно отключен (команда `shutdown`) или включен (команда `no shutdown`)
`clock rate` *скорость_кбит/с*	Подкоманда последовательного интерфейса, задающая тактовую частоту в битах в секунду на интерфейсе, использующем кабель DCE
`bandwidth` *скорость_кбит/с*	Подкоманда интерфейса, задающая на маршрутизаторе предпочтительную скорость канала в килобайтах в секунду, но никак не влияющая на фактическую скорость

Окончание табл. 12.8

Команда	Описание
`description` *текст*	Подкоманда интерфейса, позволяющая установить текстовое описание интерфейса
`ppp authentication {pap | chap | pap chap | chap pap}`	Подкоманда интерфейса, разрешающая только аутентификацию PAP, только аутентификацию CHAP или обе (порядок имеет значение)
`username` *имя* `password` *пароль*	Глобальная команда, задающая имя пользователя и пароль, ожидаемые от дистанционного устройства (имя пользователя должно совпадать с названием дистанционного устройства)

Таблица 12.9. Команды EXEC главы 12

Команда	Описание
`show interfaces [`*тип номер*`]`	Выводит статистику и подробности конфигурации интерфейса, включая тип инкапсуляции
`show interfaces [`*тип номер*`] description`	Выводит для каждого интерфейса по одной строке, содержащей его описание и состояние (или только одну строку об общем количестве, если интерфейс включен)
`show ip interface brief`	Выводит для каждого интерфейса по одной строке, содержащей его состояние и IP-адрес
`show controllers serial` *номер*	Сообщает, подключен ли к интерфейсу кабель, и если да, то кабель ли это DTE или DCE
`debug ppp authentication`	Создает сообщения для каждого этапа процесса аутентификации PAP или CHAP
`debug ppp negotiation`	Создает отладочные сообщения для переговоров LCP и NCP между устройствами

Ответы на контрольные вопросы:

1 Б. 2 Б. 3 А и В. 4 В. 5 А и Г. 6 Б и Г. 7 В и Г.

Глава 13

Концепции протокола Frame Relay

Технология Frame Relay, некогда наиболее популярная технология WAN в компьютерных сетях, несколько утратила популярность, будучи замененной некоторыми другими средствами WAN. Имеется в виду технология виртуальных частных сетей (VPN), обсуждавшаяся в главе 7, и глобальные сети Ethernet, введение в которые приведено в первом томе. Кроме того, многие предприятия используют сети VPN с *мультипротокольной коммутацией по меткам* (Multiprotocol Label Switching — MPLS), следующие той же базовой модели служб, что и технология Frame Relay, причем обычно предоставляемых теми же провайдерами Frame Relay, но с существенными техническими преимуществами.

Хотя многие компании используют другие средства WAN, технология Frame Relay все еще используется, а некоторые компании все еще используют ее как базовую технологию WAN. Она может также использоваться для подключения VPN к MPLS и Интернету. Таким образом, технология Frame Relay некоторое время еще остается важной сетевой темой.

В данной главе описывается работа протокола Frame Relay, а в главе 14 — его настройка. Первый раздел этой главы сосредоточивается на основах технологии Frame Relay, а также на терминологии. Во втором разделе рассматривается адресация канала связи Frame Relay. Эта тема требует некоторого внимания, поскольку адреса Frame Relay необходимы как для настройки маршрутизатора, так и для поиска и устранения неисправностей. В последнем разделе этой главы рассматриваются некоторые проблемы сетевого уровня, связанные с использованием Frame Relay.

В этой главе рассматриваются следующие экзаменационные темы
Технологии WAN
Различные технологии WAN
Frame Relay

Основные темы

Обзор технологии Frame Relay

В технологии Frame Relay есть множество преимуществ и дополнительных функций по сравнению с двухточечными выделенными каналами WAN. Однако, чтобы обеспечить такие дополнительные возможности, в ней используются более сложные протоколы. Например, сети Frame Relay являются средами с многостанционным доступом, т.е. к соединению может быть подключено более двух устройств. Такой механизм работы среды в чем-то похож на используемый в локальной сети. Тем не менее, в отличие от локальных сетей, в среде Frame Relay на канальном уровне нет широковещания, поэтому данную технологию также называют *нешироковещательной средой с многостанционным доступом* (Nonbroadcast Multiaccess — NBMA). Более того, поскольку среда Frame Relay является многостанционной, в ней нужно использовать некоторую разновидность адреса, чтобы идентифицировать дистанционный маршрутизатор получателя.

На рис. 13.1 представлены стандартная физическая топология сети Frame Relay и связанная с ней терминология.

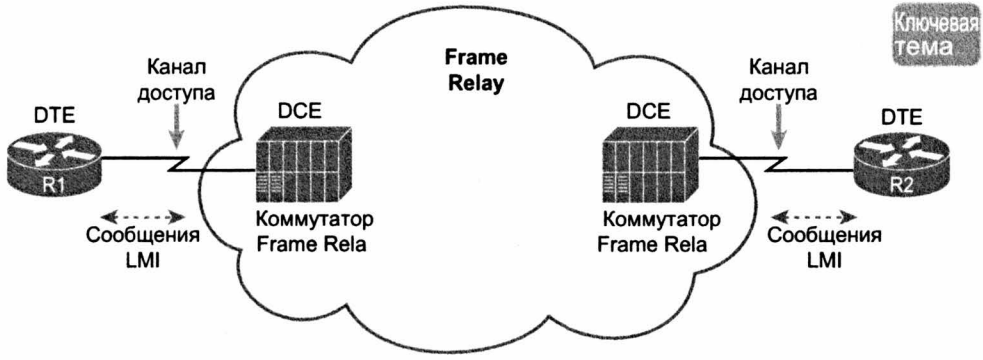


Рис. 13.1. Компоненты сети Frame Relay

На рис. 13.1 показаны наиболее общие компоненты сети Frame Relay. Между маршрутизатором клиента и коммутатором Frame Relay провайдера услуг прокладывается выделенная линия, которую называют *каналом доступа* (access link). Чтобы отслеживать работоспособность такого канала, устройства, не относящиеся к сети Frame Relay провайдера, называемые *терминальным оборудованием* (Data Terminal Equipment — DTE) канала передачи данных, периодически обмениваются служебными сообщениями с коммутатором Frame Relay. Такие тестовые сообщения (keepalive) вкупе с другими служебными фреймами описаны в протоколе *интерфейса локального управления* (Local Management Interface — LMI). Маршрутизаторы с точки зрения технологии Frame Relay являются устройствами DTE, а коммутаторы — устройствами DCE (Data Communications Equipment — коммуникационное оборудование канала передачи данных).

ВНИМАНИЕ!

У терминов *DCE* и *DTE* разные значения в разных контекстах. Здесь, в контексте служб Frame Relay, их роли описаны в предыдущем подразделе. На физической выделенной линии оборудование DCE обеспечивает синхронизацию на уровне 1, а оборудование DTE получает сигнал тактового генератора устройства DCE и реагирует на него. Это два разных (и общепринятых) случая использования этих двух терминов.

Следует отметить, что на рис. 13.1 показана физическая схема сети Frame Relay, а логическая схема будет выглядеть несколько по-другому. Логическая схема виртуальных каналов показана на рис. 13.2.



Рис. 13.2. Виртуальные каналы сети Frame Relay

Логический маршрут между двумя устройствами DTE представляет собой виртуальный канал. Полужирной пунктирной линией на рисунке показан виртуальный канал, и в дальнейшем на рисунках используется именно такая линия для обозначения логических маршрутов, чтобы их можно было легко заметить. Обычно провайдер конфигурирует все настройки виртуальных каналов, и такие заранее настроенные виртуальные каналы называют *постоянными* (Permanent Virtual Circuits — PVC).

В маршрутизаторах используются *идентификаторы канального подключения* (Data-Link Connection Identifier — DLCI) в качестве адреса в сети Frame Relay; с их помощью идентифицируют виртуальные каналы, по которым должны пересылаться фреймы. Следовательно, как показано на рис. 13.2, когда устройство R1 пересылает фрейм маршрутизатору R2, пакет уровня 3 инкапсулируется в заголовок Frame Relay и соответствующий концевик. В заголовке Frame Relay указано правильное значение идентификатора DLCI, поэтому коммутатор провайдера услуги Frame Relay может переслать такой фрейм нужному устройству (R2).

В табл. 13.1 приведены компоненты сети Frame Relay, показанные на рис. 13.1 и 13.2, а также их описание. Некоторые термины ниже объясняются более подробно.

Определения терминов, имеющих отношение к технологии Frame Relay, даны в документах Международного союза по телекоммуникациям (International Telecommunications Union — ITU) и национального Института стандартизации США (American National Standards Institute — ANSI). В 1990-х годах форум Frame Relay и консорциум производителей определили большинство первоначальных спецификаций. Со временем ITU и ANSI узаконили большинство из них как стандарты.

Теперь, ознакомившись с основными концепциями и ключевыми терминами Frame Relay, рассмотрим в нескольких следующих разделах его базовые функции немного подробней.

Таблица 13.1. Терминология и концепции Frame Relay



Термин	Описание
Виртуальный канал (Virtual Circuit — VC)	Логический канал, представляющий собой маршрут, по которому передаются фреймы между устройствами DTE. Виртуальные каналы особенно полезны при использовании разделяемых физических линий
Постоянный виртуальный канал (Permanent Virtual Circuit — PVC)	Предварительно настроенный виртуальный канал. По сути такой канал аналогичен выделенной линии
Коммутируемый виртуальный канал (Switched Virtual Circuit — SVC)	Виртуальный канал, устанавливаемый по мере необходимости. По своей сути он аналогичен коммутируемому соединению
Терминальное оборудование (Data Terminal Equipment — DTE)	Устройства DTE представляют собой оборудование на стороне клиента услуги Frame Relay. Обычно размещаются на стороне пользователя
Аппаратура передачи данных (Data Communications Equipment — DCE)	Устройства DCE представляют собой оборудование на стороне провайдера услуги Frame Relay. Обычно в качестве таких устройств используются коммутаторы Frame Relay. Зачастую подобные устройства называют *терминальным оборудованием канала* (circuit-terminating equipment)
Канал доступа (Access Link)	Выделенная линия между устройствами DCE и DTE
Скорость доступа (Access Rate — AR)	Скорость, определяемая тактовыми импульсами образующего канал оборудования. Чем выше скорость, тем выше стоимость канала
Согласованная скорость передачи информации (Committed Information Rate — CIR)	Скорость, с которой биты могут быть переданы по виртуальному каналу; обычно оговаривается в договоре между провайдером и потребителем услуги
Идентификатор канального подключения (Data-Link Connection Identifier — DLCI)	Адрес в технологии Frame Relay, используемый для идентификации виртуальных каналов
Нешироковещательный множественный доступ (Nonbroadcast Multiaccess — NBMA)	Сеть, в которой не рассылаются широковещательные фреймы и пакеты, но в которой может быть больше двух устройств
Локальный интерфейс управления (Local Management Interface — LMI)	Протокол, используемый для управления соединением между устройствами DCE и DTE. Обеспечивает передачу сигналов для коммутируемых виртуальных каналов, сигналов состояния для постоянных виртуальных каналов и *тестовых пакетов* (keepalive)

Виртуальные каналы

В технологии Frame Relay есть существенное преимущество перед двухточечными выделенными каналами — виртуальные каналы. На рис. 13.3 показана типичная сеть Frame Relay, соединяющая три хоста.

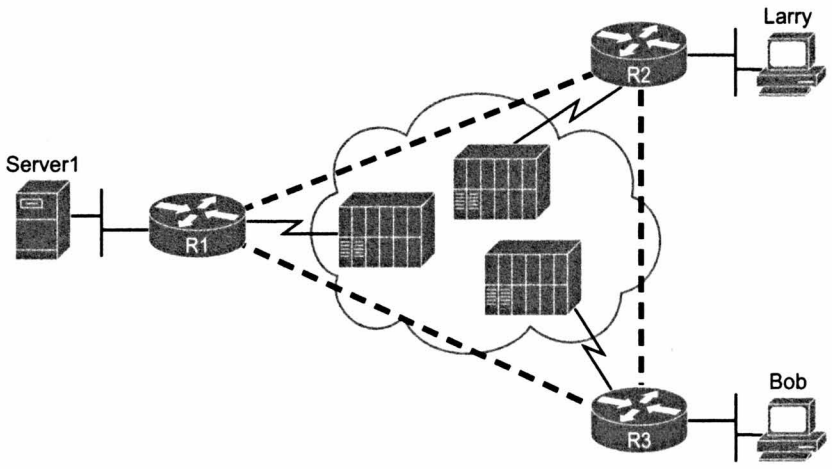


Рис. 13.3. Типичная сеть Frame Relay, соединяющая три хоста

Виртуальный канал представляет собой логический маршрут между двумя устройствами DTE среды Frame Relay. Само понятие *виртуальный канал* точно описывает принцип работы технологии. Такой канал работает как выделенная двухточечная линия с точки зрения логики передачи данных, т.е. позволяет доставлять потоки трафика между двумя точками в сети WAN. Между двумя точками нет физического канала, поэтому он и называется виртуальным. Например, в маршрутизаторе R1 (см. рис. 13.3) оканчиваются два виртуальных канала: один — от маршрутизатора R2, другой — от R3. Маршрутизатор R1 может доставлять трафик напрямую каждому маршрутизатору, просто пересылая его в соответствующий виртуальный канал.

Каналы связи и сама сеть Frame Relay совместно используют множество виртуальных каналов. Так, например, маршрутизатор R1 использует тот же канал доступа. Маршрутизатор R1 может послать один фрейм Frame Relay на маршрутизатор R2, а другой — на маршрутизатор R3, но оба они отправятся по тому же физическому каналу доступа.

Мало того, что один клиентский маршрутизатор совместно использует свой канал доступа со многими виртуальными каналами (VC), ту же сеть Frame Relay совместно использует множество клиентов. Изначально многие компании противились переходу на технологию Frame Relay, поскольку фактически они конкурировали за емкость физических каналов среды Frame Relay провайдера. Чтобы решить эту проблему, в технологию Frame Relay была внедрена концепция гарантированной *скорости передачи информации* (Committed Information Rate — CIR). Для каждого виртуального канала задается скорость CIR, с которой провайдер гарантирует передачу пользовательской информации. Таким образом, клиент может заменить выделенную линию каналом Frame Relay, скорость CIR которого будет равна скорости, использовавшейся ранее для выделенной линии.

Наибольшим преимуществом технологии Frame Relay по выделенным линиям является возможность подключения к каждой площадке только по одному каналу доступа между каждым маршрутизатором и провайдером Frame Relay. Следует отметить, что даже для рассмотренной выше сети из трех площадок намного дешевле использовать сеть Frame Relay, чем двухточечные каналы связи, поскольку каналы

доступа обычно относительно коротки, только до ближайшего *представительства* (Point of Presence — PoP) провайдера Frame Relay.

Технология Frame Relay и другие технологии коллективного доступа WAN имеют существенное преимущество по стоимости в больших корпоративных глобальных сетях. Представьте, например, организацию со 100 площадками, на каждой из которых по одному маршрутизатору. Для попарного соединения всех маршрутизаторов выделенными линиями компании понадобилось бы 4950 выделенных линий! Кроме того, каждому маршрутизатору понадобилось бы 99 последовательных интерфейсов. При использовании технологии Frame Relay каждому маршрутизатору достаточно было бы использовать один последовательный интерфейс и один канал доступа к облаку Frame Relay, в общей сложности для 100 каналов доступа. Затем провайдер Frame Relay может создать постоянные каналы (PVC) между каждой парой маршрутизаторов (в общей сложности 4950 каналов VC). Решение Frame Relay требует значительно меньше физических каналов связи, причем понадобится только один последовательный интерфейсе на каждом маршрутизаторе.

Сеть Frame Relay будет обходиться провайдеру много дешевле при создании и в обслуживании, чем набор выделенных линий. Следовательно, услуга на основе такой сети будет стоить дешевле и для клиента. Наиболее эффективным решением с точки зрения стоимости сеть Frame Relay является и для топологии сети, в которой с помощью каналов WAN нужно объединить несколько хостов.

В сети Frame Relay виртуальные каналы необязательно должны быть настроены между всеми хостами сети попарно. На рис. 13.3 показана схема, в которой все хосты соединены каналами. Такую топологию называют *полносвязной* (full-mesh). Если не все пары устройств соединены между собой каналами, то топологию называют *неполносвязной* (partial-mesh), пример такой схемы сети показан на рис. 13.4. Например, если маршрутизатор R1 является устройством головного офиса компании, а устройства R2 и R3 находятся в филиалах, то компании вряд ли понадобится соединять два филиала напрямую между собой. В таком случае будет использоваться неполносвязная топология.

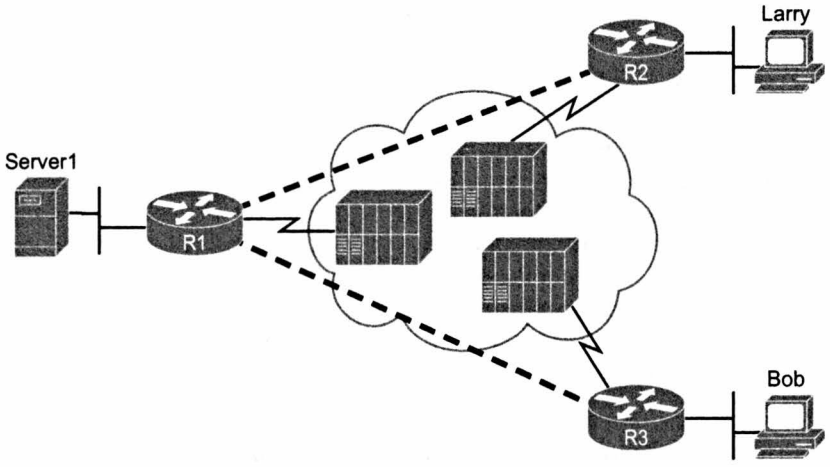


Рис. 13.4. Типичная неполносвязная сеть Frame Relay, соединяющая три хоста

В неполносвязной сети есть свои преимущества и недостатки по сравнению с полносвязной топологией. Главное преимущество заключается в том, что такая топология дешевле, поскольку провайдер обычно взимает плату за каждый виртуальный канал по отдельности. Недостаток вполне очевиден: трафик от маршрутизатора R2 к маршрутизатору R3 сначала передается маршрутизатору R1, а затем получателю. Если объем пересылаемых данных невелик, стоимость такой услуги также будет невысокой; если же данных передается много, то более дорогая полносвязная топология будет более эффективной, поскольку большие потоки трафика не будут передаваться через интерфейс доступа к сети маршрутизатора R1 дважды.

Типы LMI и инкапсуляции

В то время как каналы PVC предоставляют двум клиентским маршрутизаторам логический способ передачи фреймов друг другу, у технологии Frame Relay есть много физических и логических компонентов, совместная работа которых должна обеспечить работу каналов PVC. Физически каждый маршрутизатор нуждается в физическом канале доступа к некоему коммутатору Frame Relay. Провайдер должен также создать некую физическую сеть между этими коммутаторами, кроме того, ему придется выполнить некоторую работу, чтобы посланные по каналу PVC фреймы поступили по назначению.

Для управления всеми физическими каналами доступа и использующими его каналами PVC технология Frame Relay использует протокол *интерфейса локального управления* (Local Management Interface — LMI). Сообщения LMI передаются между устройствами DTE (например, маршрутизаторами) и устройствами DCE (например, коммутаторами Frame Relay, принадлежащими провайдеру служб).

В протоколе LMI наиболее важным, как с практической точки зрения, так и с точки зрения сертификационного экзамена, является запрос состояния канала. Такое сообщение выполняет две основные функции.

Ключевая тема **Две функции протокола LMI**

- Сообщения о состоянии канала используются в качестве тестовых (keepalive) для устройств DCE и DTE. Если в канале связи Frame Relay есть проблемы, отсутствие таких сообщений приведет к тому, что для канала будет указано нерабочее состояние (`down`).
- Сообщения о состоянии канала извещают оборудование об активном или неактивном состоянии постоянного виртуального канала. Несмотря на то что постоянный канал настроен статически, он может находиться в разных состояниях. Физический канал связи Frame Relay может быть в рабочем состоянии, но один или несколько виртуальных каналов в нем могут не работать. Маршрутизатору необходимо знать о том, что какие-то каналы работают, а какие-то — нет. Устройство получает такую информацию при посредничестве сообщений о состоянии каналов протокола LMI.

По историческим причинам у маршрутизаторов Cisco есть три параметра для трех вариантов протоколов LMI: Cisco, ITU и ANSI. Вполне очевидно, что сообщения разных вариантов протокола отличаются и поэтому не совместимы между со-

бой. Если в устройствах DCE и DTE на концах канала связи настроен протокол LMI одного и того же стандарта, канал работает правильно.

Настроить тип протокола LMI очень просто. На сегодняшний день в большинстве конфигураций сохраняется стандартная настройка протокола, которая подразумевает, что в маршрутизаторе срабатывает функция автоматического определения типа протокола, используемого коммутатором. Поэтому можно ничего не менять в конфигурации устройства, чтобы маршрутизатор сам определил стандарт LMI. Если же тип протокола в явном виде указывается в конфигурации, то функция автоматического определения отключается. В табл. 13.2 приведены три типа протокола LMI, разработавшие их организации и ключевое слово, используемое для указания протокола в команде режима конфигурирования интерфейса `frame-relay lmi-type`.

Таблица 13.2. Типы протокола LMI в технологии Frame Relay

Ключевая тема

Название	Стандарт	Параметр в операционной системе Cisco IOS
Cisco	Собственный протокол	`cisco`
ANSI	T1.617 Annex D	`ansi`
ITU	Q.933 Annex A	`q933a`

Инкапсуляция и фреймирование Frame Relay

Маршрутизатор, подключенный к сети Frame Relay, инкапсулирует пакеты уровня 3 в заголовок и концевик Frame Relay перед тем, как передать в канал связи. Формат заголовка и концевика определяется спецификацией протокола доступа к каналу передачи фреймов (Link Access Procedure Frame Bearer Services — LAPF), описанному в стандарте ITU Q.922-A. Разреженное фреймирование LAPF поддерживает обнаружение ошибок FCS в концевике, поле DLCI (подробно обсуждаемое далее в этой главе), а также нескольких других полей, показанных на рис. 13.5.



Рис. 13.5. Формат фрейма LAPF

Следует отметить, что фактически маршрутизаторы используют более длинный заголовок, чем заголовок LAPF, поскольку в нем нет всей информации, необходимой маршрутизаторам. В частности, на рис. 13.5 не показано поле типа протокола (Protocol Type). Во всех протоколах канального уровня такое поле должно присутствовать, чтобы можно было указать, какой именно тип пакета передается через канал. Если бы в технологии Frame Relay использовался только заголовок LAPF, устройства DTE (в том числе маршрутизаторы) не смогли бы передавать мультипротокольный трафик, поскольку не могли бы идентифицировать тип протокола верхнего уровня.

Чтобы решить проблему отсутствия поля типа протокола, были разработаны следующие усовершенствования.

- Компания Cisco и три других крупных игрока на рынке телекоммуникаций и сетевого оборудования разработали дополнительный заголовок, размещаемый между заголовком LAPF и заголовком пакета уровня 3. В этом заголовке есть двухбайтовое поле типа протокола, содержащее значения, совпадающие с теми, которые компания Cisco использует в протоколе HDLC.
- В спецификации RFC 1490 (позже ее заменили спецификацией RFC 2427; оба числа нужно запомнить), *многопротокольные соединения в среде Frame Relay*, указано альтернативное решение. Стандарт RFC 1490 был разработан для объединения устройств от разных производителей оборудования для сети Frame Relay. В этом документе описывается очень похожий на разработанный четырьмя компаниями заголовок, также размещаемый между заголовком LAPF и заголовком уровня 3. В дополнительном заголовке также есть поле типа протокола и множество дополнительных опциональных параметров.

На рис. 13.6 приведены два альтернативных формата фреймов.

Ключевая тема

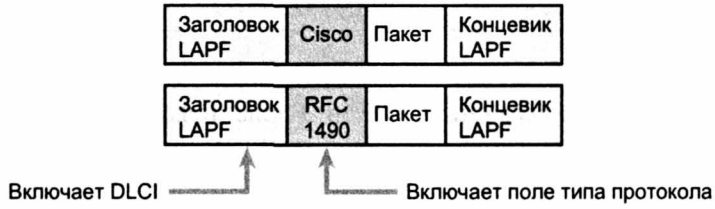


Рис. 13.6. Инкапсуляции Cisco и RFC 1490/2427

Маршрутизаторы должны договориться об используемой инкапсуляции; коммутаторы о ней не беспокоятся. Таким образом, в каждом виртуальном канале может быть использована своя инкапсуляция; в конфигурации инкапсуляции компании Cisco указывается ключевым словом `cisco`, второй вариант указывается ключевым словом `ietf`.

Теперь, после подробного ознакомления с основными концепциями и терминами технологии Frame Relay, рассмотрим адресацию с помощью идентификаторов DLCI.

Адресация в технологии Frame Relay

Адрес Frame Relay на базовом, концептуальном уровне называется *идентификатором канального подключения* (Data Link Connection Identifier — DLCI) и имеет некоторое сходство с уже знакомыми MAC- и IP-адресами. Все эти адреса существуют в виде двоичных значений, однако все они имеют некий более удобный формат: шестнадцатеричный для MAC-адресов, десятичное представление с разделительными точками для IP-адресов и десятичное для DLCI-адресов. Технология Frame Relay определяет идентификатор DLCI как 10-битовое десятичное число, как правило, с зарезервированными нижними и верхними значениями. (Конкретный диапазон не важен, поскольку значения назначает провайдер служб, но обычно он составляет 17–1000.)

Если изучить вопрос глубже, особенно то, как идентификаторы DLCI влияют на перенаправление фреймов Frame Relay, то сходство с MAC- и IP-адресами постепенно сменится на абсолютное различие. Этот раздел посвящен данной логике перенаправления. Сначала обсуждается концепция того, что адреса Frame Relay фактически идентифицируют один конец канала PVC. Затем обсуждение переходит к логике перенаправления, используемой в сетевой среде Frame Relay, и завершается раздел рассмотрением наиболее распространенных способов, которыми провайдеры служб могут назначать фактические значения идентификаторов DLCI.

Локальная адресация Frame Relay

Провайдер служб назначает каждому каналу PVC два локальных значения идентификатора DLCI: по одному на каждом конце канала PVC. Термин *локальный идентификатор DLCI* (local DLCI) объединяет несколько концепций, а слово *локальный* подчеркивает тот факт, что с точки зрения маршрутизатора локальный идентификатор DLCI — это идентификатор, используемый на том же конце канала, что и маршрутизатор. Данная концепция представлена на рис. 13.7.

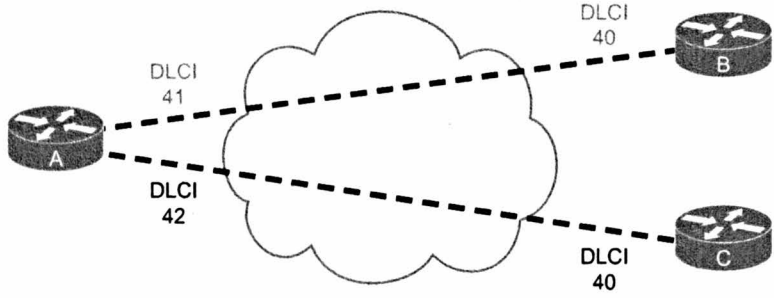


Рис. 13.7. Два канала PVC с идентификаторами DLCI на каждом конце

В этом примере канал PVC между маршрутизаторами A и B имеет два идентификатора DLCI, назначенных провайдером. На конце канала у маршрутизатора A используется локальный идентификатор DLCI 41, идентифицирующий канал PVC, а на конце маршрутизатора B — идентификатор DLCI 40, идентифицирующий тот же канал PVC. Точно так же у канала PVC между маршрутизаторами A и C есть два локальных идентификатора DLCI, по одному на каждом конце: у маршрутизатора A — 42; у маршрутизатора C — 40.

Провайдер служб может использовать любые значения DLCI в пределах корректного диапазона, за одним исключением.

Требование к уникальности используемых локальных идентификаторов DLCI на любом отдельном канале связи Frame Relay

Ключевая тема

Локальный идентификатор DLCI в пределах одного канала связи должен быть уникальным среди всех каналов PVC, которые используют один физический канал связи Frame Relay, поскольку идентификаторы DLCI Frame Relay значимы только локально.

Поскольку значение идентификатора DLCI выбирает провайдер, инженер корпоративной сети может не волноваться о неправильном выборе значения DLCI. Для справки: на каждом физическом канале связи от маршрутизатора к сети Frame Relay

значения идентификаторов DLCI должны быть уникальны. На рис. 13.7 провайдер определил два канала PVC, которые пересекают один канал связи Frame Relay R1: один с локальным идентификатором DLCI 41 и второй с локальным идентификатором DLCI 42. Если бы был добавлен другой канал PVC, подключенный к маршрутизатору A, то провайдер не мог бы использовать на канале связи R1 только значения 41 или 42 для локальных идентификаторов DLCI.

Локальному маршрутизатору видим (или известен) только локальный идентификатор DLCI. При настройке маршрутизатора задают только локальное значение идентификатора DLCI, но не значение идентификатора DLCI на другом конце канала PVC. Аналогично команды `show` отображают только локальные значения идентификаторов DLCI.

Перенаправление фреймов

Самое существенное различие между идентификаторам DLCI и двумя другими наиболее популярными в CCNA адресами (MAC и IP) кроется в процессе перенаправления. Заголовок Ethernet включает MAC-адреса отправителя и получателя, заголовок IP также включает IP-адреса отправителя и получателя. Но заголовок Frame Relay включает только одно поле DLCI, и оно идентифицирует сам канал PVC, а не отправителя или получателя.

Чтобы получить представление о том, как провайдер перенаправляет фрейм Frame Relay, учтите тот факт, что ему известны локальные идентификаторы DLCI, используемые на обоих концах канала PVC и канала связи, который подключен к маршрутизаторам. Например, на рис. 13.8 показано, что провайдеру известно, что между маршрутизаторами A и B существует канал PVC. Ему известно, что на стороне маршрутизатора A он использует локальный идентификатор DLCI 41, а на стороне маршрутизатора B — идентификатор DLCI 40. С учетом этого рис. 13.8 демонстрирует то, что происходит при передаче фрейма маршрутизатором A маршрутизатору B.

Ключевая тема

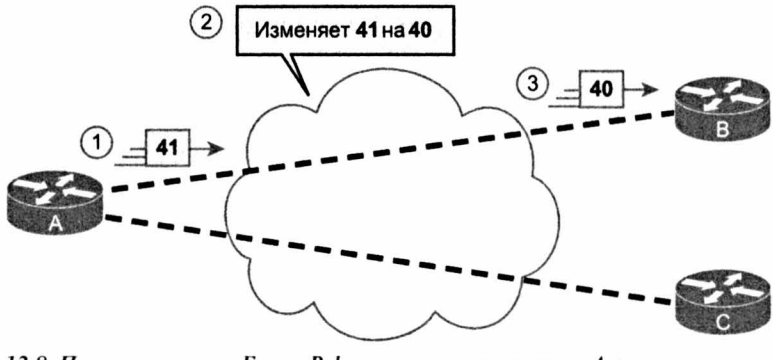


Рис. 13.8. Перенаправление Frame Relay от маршрутизатора A к маршрутизатору B

Рисунок демонстрирует три главных этапа. На первом маршрутизатор A решает послать фрейм по каналу PVC, подключенному к маршрутизатору B. С точки зрения маршрутизатора A канал PVC известен ему только как канал PVC с локальным идентификатором DLCI 41. Таким образом, маршрутизатор A посылает фрейм с идентификатором

фикатором DLCI 41 в заголовке. На втором этапе провайдер служб делает немало. Он ищет известную информацию об этом канале PVC, перенаправляют фрейм маршрутизатору B и *изменяет идентификатор DLCI на 40.* На третьем этапе, когда фрейм достигает маршрутизатора B, у него будет значение идентификатора DLCI 40. Маршрутизатор B совершенно правильно полагает, что фрейм поступил по каналу PVC от маршрутизатора A, поскольку единственное, что ему известно о канале PVC, так это то, что значением его локального идентификатора DLCI (на конце маршрутизатора B) является 40.

Обратите внимание на то, что, когда маршрутизатор A послал фрейм, он использовал свое локальное значение идентификатора DLCI (41), а когда маршрутизатор B получил фрейм, то увидел свой локальный идентификатор DLCI (40) для того же канала PVC.

Наконец, рассмотрим процесс передачи пакета маршрутизатором B назад маршрутизатору A. Маршрутизатору снова известны значения только локальных идентификаторов DLCI, как показано на рис. 13.9. Маршрутизатор B посылает фрейм с идентификатором DLCI 40, который идентифицирует канал PVC от маршрутизатора A до маршрутизатора B; сетевая среда (облако) изменяет идентификатор DLCI на 41; и маршрутизатор A получает фрейм с идентификатором DLCI 41.

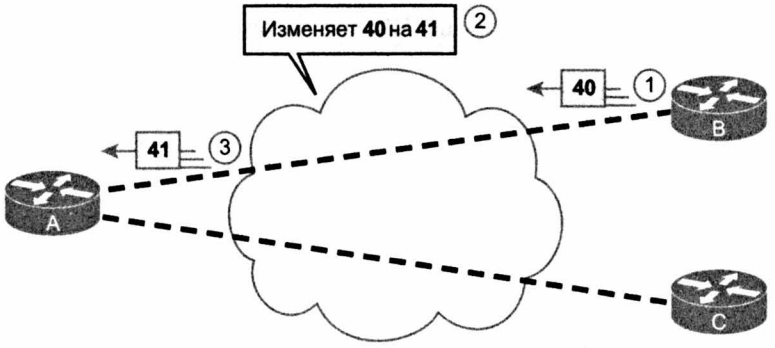


Рис. 13.9. Перенаправление Frame Relay от маршрутизатора B к маршрутизатору A

Та же идея используется в каждом канале PVC. На рис. 13.7 были представлены два канала PVC, включая канал PVC A–C с локальными идентификаторами DLCI 42 (на стороне A) и 40 (на стороне C). На рис. 13.10 представлены локальные идентификаторы DLCI в двух разных потоках фреймов: сначала от маршрутизатора A до C, а затем от маршрутизатора C назад к A.

На данном рисунке не показано действие сетевой среды (облака) по смене значений идентификаторов DLCI, но это действие все же имеет место. На этапе 1 маршрутизатор A передает фрейм с идентификатором DLCI 42. На этапе 2, когда он выходит из сетевой среды к маршрутизатору C, его идентификатор DLCI изменен на 40, что соответствует локальному идентификатору DLCI маршрутизатора C для данного канала PVC. Точно так же на этапе 3 маршрутизатор C посылает фрейм с локальным идентификатором DLCI 40. Сетевая среда изменяет идентификатор DLCI на 42, чтобы при выходе из сетевой среды к маршрутизатору A на этапе 4 фрейм предоставил маршрутизатору A локальный идентификатор DLCI 42.

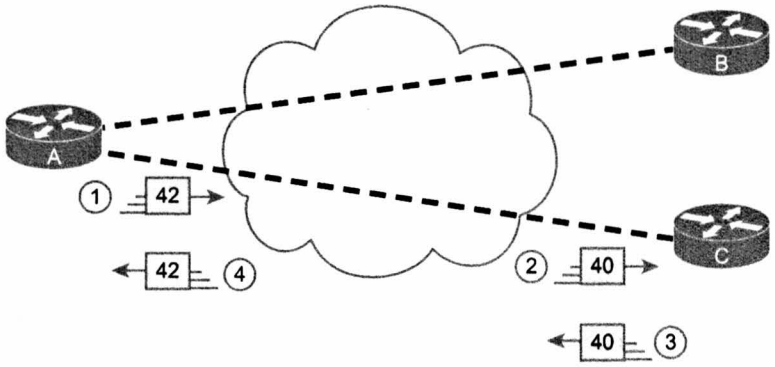


Рис. 13.10. Перенаправление Frame Relay между маршрутизаторами A и C

Адресация сетевого уровня в среде Frame Relay

Сети Frame Relay в чем-то похожи и на локальные сети, и на двухточечные каналы WAN, но в то же время отличаются от них в деталях. Отличия от других технологий добавляют некоторые дополнительные проблемы при передаче пакетов уровня 3 сети Frame Relay. В частности, в реализации технологии Frame Relay от компании Cisco есть три варианта разделения подсетей и IP-адресов для интерфейсов Frame Relay.

Ключевая тема **Три варианта адресации и топологии Frame Relay**

- Используется одна подсеть для всех устройств DTE Frame Relay.
- Для каждого виртуального канала выделяется собственная подсеть.
- Решение, в котором объединены два первых варианта.

В этом разделе рассматриваются три основных варианта IP-адресации поверх среды Frame Relay.

Адресация уровня 3 в среде Frame Relay: одна подсеть для всех устройств DTE

На рис. 13.11 показан первый вариант построения сети, в котором используется одна подсеть для всех устройств DTE Frame Relay. В данном случае построена полносвязная сеть Frame Relay, поскольку этот вариант адресации прежде всего используется в полносвязных топологиях виртуальных каналов. В полносвязной топологии маршрутизатор связан со всеми маршрутизаторами в сети виртуальными каналами, т.е. каждый из них может пересылать фреймы напрямую другим маршрутизаторам. Такой метод работы очень похож на передачу данных в обычной локальной сети, поэтому одна подсеть может использоваться для всех интерфейсов Frame Relay. В табл. 13.3 перечислены адреса, используемые в сети, показанной на рис. 13.11.

Сеть с использованием единой подсети для адресации исключительно проста и позволяет сэкономить адресное пространство. Она очень похожа на локальную сеть, поэтому ее проще понять и запомнить. Тем не менее многие компании используют неполносвязные сети Frame Relay, и схема с одной подсетью в таком случае не очень хорошо подойдет для решения задачи.

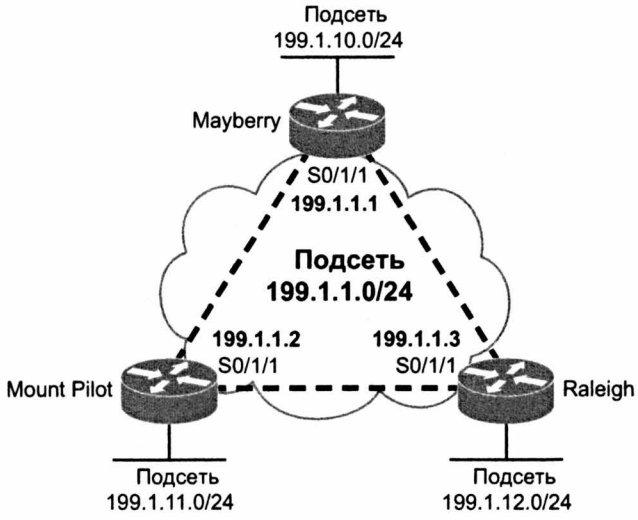


Рис. 13.11. IP-адреса в полносвязной топологии

Таблица 13.3. IP-адреса в полносвязной сети без использования субинтерфейсов

Маршрутизатор	IP-адрес интерфейса Frame Relay
Mayberry	199.1.1.1
Mount Pilot	199.1.1.2
Raleigh	199.1.1.3

Адресация уровня 3 в среде Frame Relay: выделение одной подсети на каждый виртуальный канал

Второй вариант IP-адресации, подразумевающий использование отдельной подсети для каждого виртуального канала, предназначен для неполносвязных сетей Frame Relay, например, такой, как на рис. 13.12. Маршрутизатор Boston не может пересылать фреймы маршрутизатору Charlotte напрямую, поскольку между ними не установлен виртуальный канал. Такая топология сети Frame Relay больше распространена по сравнению с предыдущей, поскольку многие организации стремятся сгруппировать приложения и серверы и развернуть их в некоторой центральной точке сети, а основной трафик в сети курсирует между дистанционными хостами и такими центральными серверами.

Проект подсетей с одной подсетью на канал VC использует ту же логику, что и набор двухточечных каналов связи. Использование нескольких подсетей вместо одной большой подсети действительно приводит к напрасной трате некоторых IP-адресов. Однако использование единой подсети в проекте с неполносвязной топологией (рис. 13.12) создает несколько проблем для протоколов маршрутизации, поскольку не все маршрутизаторы в подсети могут посылать сообщения друг другу непосредственно. Неполносвязная топология лучше работает с проектом одной подсети на каждый канал VC.

Ключевая тема

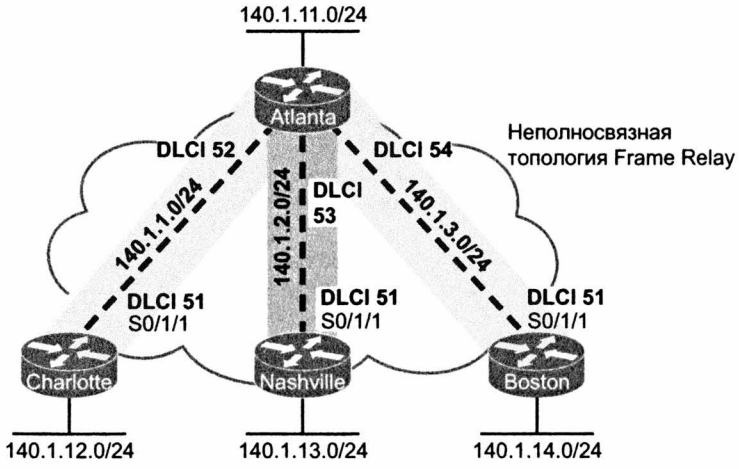


Рис. 13.12. IP-адреса в неполносвязной топологии

В табл. 13.4 перечислены IP-адреса для неполносвязной сети Frame Relay, показанной на рис. 13.12.

Таблица 13.4. IP-адреса в двухточечных каналах субинтерфейсов

Маршрутизатор	Подсеть	IP-адрес
Atlanta	140.1.1.0	140.1.1.1
Charlotte	140.1.1.0	140.1.1.2
Atlanta	140.1.2.0	140.1.2.1
Nashville	140.1.2.0	140.1.2.3
Atlanta	140.1.3.0	140.1.3.1
Boston	140.1.3.0	140.1.3.4

В операционной системе Cisco IOS есть специальная функция в конфигурации, называемая *субинтерфейсом*, которая позволяет разделять физический интерфейс на логические подканалы. За счет субинтерфейсов в маршрутизаторе Atlanta можно указать три IP-адреса на физическом интерфейсе Serial0/1/1. Маршрутизатор может трактовать каждый такой субинтерфейс и связанный с ним виртуальный канал как отдельное двухточечное последовательное соединение между устройствами. Каждому из трех субинтерфейсов физического интерфейса Serial0/1/1 будет назначен свой адрес (см. табл. 13.4). Пример настройки маршрутизатора Atlanta в соответствии с адресами в табл. 13.4, включая субинтерфейсы S0/1/1, приведены в главе 14.

ВНИМАНИЕ!

В схеме адресации используются подсети с префиксом /24, чтобы упростить математические расчеты. В реальных сетях для двухточечных субинтерфейсов используются обычно префиксы /30 (255.255.255.252), поскольку они позволяют выделить только два используемых адреса для канала, т.е. как раз нужное количество. Вполне очевидно, что использование разных масок в той же сети подразумевает использование протокола маршрутизации, поддерживающего маски VLSM.

Адресация уровня 3 в среде Frame Relay: гибридный подход

Третий вариант адресации уровня 3 представляет собой гибрид двух рассмотренных выше методов. Обратимся к рис. 13.13, на котором показаны три маршрутизатора, между которыми установлены виртуальные каналы, и два дистанционных маршрутизатора подключены отдельными каналами.

В таком случае можно использовать две схемы адресации уровня 3. В первой каждый канал интерпретируется как независимая группа хостов уровня 3. В этом варианте в сети Frame Relay понадобится пять подсетей. Тем не менее можно заметить, что маршрутизаторы А, Б и В соединены в полносвязной топологии, поэтому для них можно использовать одну подсеть. Два оставшихся виртуальных канала между маршрутизаторами А и Г, а также между маршрутизаторами А и Д можно рассматривать как две независимые группы хостов уровня 3. В результате понадобится всего три подсети.

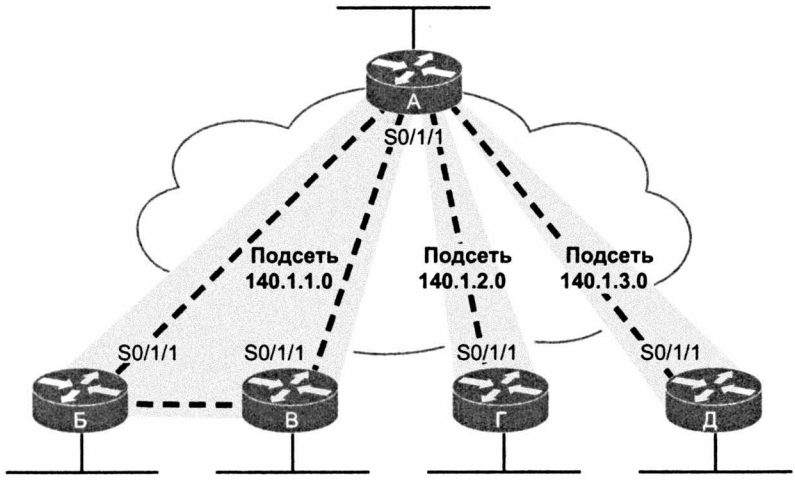


Рис. 13.13. Гибрид полносвязной и неполносвязной топологий

Чтобы реализовать практически любую из возможных схем адресации уровня 3 в рассматриваемой топологии, следует использовать субинтерфейсы. Двухточечные субинтерфейсы используются в отдельных каналах, т.е. между маршрутизаторами А и Г, а также между маршрутизаторами А и Д; интерфейсы для многостанционных подключений (multipoint) используются в том случае, когда более двух маршрутизаторов составляют одну группу, например маршрутизаторы А, Б и В.

Многостанционные (или многоточечные) интерфейсы предназначены для объединения нескольких виртуальных каналов; фактически в названии кроется принцип работы такого интерфейса — через него можно получить доступ ко многим хостам (т.е. станциям) напрямую.

В табл. 13.5 перечислены адреса и субинтерфейсы для схемы сети, показанной на рис. 13.13.

Таблица 13.5. IP-адреса для двухточечных и многоточечного субинтерфейсов

Маршрутизатор	Подсеть	IP-адрес	Тип субинтерфейса
А	140.1.1.0/24	140.1.1.1	Многоточечный
Б	140.1.1.0/24	140.1.1.2	Многоточечный
В	140.1.1.0/24	140.1.1.3	Многоточечный
А	140.1.2.0/24	140.1.2.1	Двухточечный
Г	140.1.2.0/24	140.1.2.4	Двухточечный
А	140.1.3.0/24	140.1.3.1	Двухточечный
Д	140.1.3.0/24	140.1.3.5	Двухточечный

Что специалист может увидеть в реальной сети? В большинстве случаев используются двухточечные субинтерфейсы, в которых для каждого виртуального канала выделена отдельная подсеть. Но для успешной сдачи экзамена CCNA следует знать все три варианта дизайна соединений WAN.

ВНИМАНИЕ!

В главе 14 приведены конфигурации для топологий, показанных на рис. 13.11–13.13.

Обзор

Резюме

- Сеть Frame Relay обычно изображается как облако, поскольку подробности составляющих ее устройств и соединений не видны.
- Сети Frame Relay предоставляют больше средств и преимуществ, чем простые двухточечные каналы связи WAN, но их протоколы подробней.
- Технология Frame Relay использует виртуальные каналы, определяющие логический путь между двумя устройствами DTE Frame Relay. Каналы VC действуют как двухточечный канал.
- Сети Frame Relay обеспечивают подключение к каждой площадке только по одному каналу доступа между каждым маршрутизатором и провайдером Frame Relay.
- Хотя есть три стандарта LMI (Cisco, ANSI и ITU), лучше оставить стандартное значение этого параметра, подразумевающее автоматическое распознавание стандарта, используемого устройством DCE.
- Адреса Frame Relay называют идентификаторами канального подключения (DLCI).
- Идентификаторы DLCI имеют смысл только локально, а не глобально. Они должны быть уникальными только в конфигурации маршрутизатора.
- Компания Cisco определяет три возможности для присвоения подсети и IP-адреса интерфейсам Frame Relay: одна подсеть, содержащая все оборудование DTE Frame Relay, по одной подсети на VC и комбинация первых двух возможностей.
- Технология Frame Relay не поддерживает широковещательные фреймы как сети LAN, поэтому маршрутизатор должен явно посылать широковещательный фрейм на каждый канал VC.

Контрольные вопросы

Ответьте на эти вопросы. Ответы можно найти на последней странице главы. Полное объяснение ответов приведено в приложении B на веб-сайте.

1. Что из нижеперечисленного является протоколом, используемым между устройством DTE и коммутатором сети Frame Relay?

   А) VC.
   Б) CIR.
   В) LMI.
   Г) Q.921.
   Д) DLCI.

2. Какие утверждения о технологии Frame Relay справедливы? (Выберите два ответа.)

А) Устройство DTE обычно размещается на хосте пользователя.

Б) Маршрутизаторы рассылают сообщения LMI друг другу, чтобы сигнализировать о состоянии виртуальных каналов (VC).

В) Адрес DLCI отправителя фрейма не должен изменяться, но адрес получателя может меняться по мере передачи фрейма через среду Frame Relay.

Г) Тип инкапсуляции Frame Relay на маршрутизаторе отправителя должен совпадать с типом инкапсуляции на маршрутизаторе получателя, чтобы получатель мог интерпретировать содержимое фрейма.

3. Как расшифровывается аббревиатура DLCI?

А) Data-link connection identifier (идентификатор канального подключения).

Б) Data-link connection indicator (индикатор канального подключения).

В) Data-link circuit identifier (идентификатор цепи канального подключения).

Г) Data-link circuit indicator (индикатор цепи канального подключения).

4. Маршрутизатор R1 получает фрейм, в котором указано значение DLCI, равное 222, от маршрутизатора R2. Какое из утверждений будет справедливым?

А) Значение 222 описывает маршрутизатор R1.

Б) Значение 222 описывает маршрутизатор R2.

В) Значение 222 представляет собой локальный DLCI-адрес для маршрутизатора R1, описывающий виртуальный канал между маршрутизаторами R1 и R2.

Г) Значение 222 представляет собой локальный DLCI-адрес для маршрутизатора R2, описывающий виртуальный канал между маршрутизаторами R1 и R2.

5. В компании FredsCo есть пять хостов, маршрутизаторы которых подключены к сети Frame Relay. Виртуальные каналы были настроены между всеми маршрутизаторами попарно. Какое минимальное количество подсетей понадобится компании для такой сети Frame Relay?

А) 1.

Б) 2.

В) 3.

Г) 4.

Д) 5.

Е) 10.

6. В компании BarneyCo есть один центральный офис и 10 удаленных филиалов. Каждый филиал соединен с центральным офисом с помощью постоянного виртуального канала (PVC) Frame Relay. Мистер Барни, президент компании, уволит любого сетевого инженера, который попытается настроить что-либо, помимо двухточечных каналов в такой сети. Какое минимальное количество подсетей понадобится компании для такой сети Frame Relay?

А) 1.

Б) 4.

В) 8.

Г) 10.

Д) 12.

Е) 15.

Ключевые темы

Повторите все ключевые темы данной главы, отмеченные пиктограммой "Ключевая тема". Ключевые темы и соответствующие им страницы перечислены в табл. 13.6.

Таблица 13.6. Ключевые темы главы 13

Элемент	Описание	Страница
Рис. 13.1	Компоненты сети Frame Relay	441
Табл. 13.1	Терминология и концепции Frame Relay	443
Список	Две функции протокола LMI	446
Табл. 13.2	Типы протокола LMI в технологии Frame Relay	447
Рис. 13.6	Инкапсуляции Cisco и RFC 1490/2427	448
Определение	Требование к уникальности используемых локальных идентификаторов DLCI на любом отдельном канале связи Frame Relay	449
Рис. 13.8	Перенаправление Frame Relay от маршрутизатора A к маршрутизатору B	450
Список	Три варианта адресации и топологии Frame Relay	452
Рис. 13.12	IP-адреса в неполносвязной топологии	454

Заполните таблицы и списки по памяти

Распечатайте приложение Г с веб-сайта или его раздел, относящийся к этой главе, и заполните таблицы и списки по памяти. В приложении Д приведены заполненные таблицы и списки для самоконтроля.

Ключевые термины

После первого прочтения главы попытайтесь дать определения следующим ключевым терминам. Но не расстраивайтесь, если не все получится сразу, в главе 22 описано, как использовать эти термины на завершающем этапе подготовки к экзамену.

канал доступа (access link), скорость доступа (Access Rate — AR), согласованная скорость передачи (Committed Information Rate — CIR), идентификатор канального подключения (Data-Link Connection Identifier — DLCI), устройство DCE Frame Relay (Frame Relay DCE), устройство DTE Frame Relay (Frame Relay DTE), интерфейс локального управления (Local Management Interface — LMI), широковещательный множественный доступ (Nonbroadcast Multiaccess — NBMA), постоянный виртуальный канал (Permanent Virtual Circuit — PVC), виртуальный канал (Virtual Circuit — VC)

Ответы на контрольные вопросы:

1 В. 2 А и Г. 3 А. 4 В. 5 А. 6 Г.

Глава 14

Реализация протокола Frame Relay

В главе 13 рассматривались принципы работы протокола Frame Relay. В этой главе речь пойдет о настройке функций маршрутизаторов Cisco, проверке работы каждой из них, а также о поиске и устранении проблем при передаче пакетов по сети Frame Relay.

В этой главе рассматриваются следующие экзаменационные темы
Технологии WAN
Настройка и проверка Frame Relay на маршрутизаторах Cisco
Поиск и устранение неисправностей
Поиск и устранение проблем реализации WAN Frame Relay

Основные темы

Настройка и проверка протокола Frame Relay

Конфигурация Frame Relay может быть лишь базовой или несколько более сложной, в зависимости от того, сколько используется стандартных параметров. Операционная система Cisco IOS автоматически выясняет тип интерфейса LMI и устанавливает соответствие между идентификатором DLCI и адресом следующего транзитного перехода (с помощью протокола Inverse ARP). Если в сети используются только маршрутизаторы Cisco, то стандартная инкапсуляция Cisco работает без какого-либо дополнительного конфигурирования. Если при этом сеть Frame Relay спроектирована для работы с одной подсетью, то можно настроить маршрутизаторы на использование их физических интерфейсов без каких-либо субинтерфейсов, что еще более сокращает конфигурирование. Фактически при максимально возможном использовании стандартных настроек единственной новой командой конфигурирования (по сравнению с распределенной сетью WAN, состоящей из двухточечных каналов) является команда инкапсуляции `encapsulation frame-relay`.

Вопросы по протоколу Frame Relay на экзамене могут вызвать трудности по двум причинам. Во-первых, протокол Frame Relay содержит множество опциональных параметров, которые могут быть включены в конфигурацию. Во-вторых, для сетевых инженеров, у которых уже есть определенный опыт работы с протоколом Frame Relay, этот опыт может включать в себя работу с тремя главными опциональными параметрами конфигурации Frame Relay (физической, многоточечной и двухточечный), однако программа экзамена охватывает все опциональные параметры. Поэтому при подготовке к экзамену важно, чтобы читатель просмотрел примеры всех вариантов соединений, которые включены в программу экзамена.

Планирование конфигурации протокола Frame Relay

Прежде чем станет ясно, с чего начинать конфигурирование, инженер должен выполнить довольно объемную работу по планированию этого процесса. Хотя на большинстве современных предприятий уже имеются установленные соединения протокола Frame Relay, при планировании новых площадок необходимо рассмотреть приведенные ниже вопросы и сообщить о них провайдеру протокола Frame Relay, что, в свою очередь, оказывает определенное влияние на настройку конфигурации маршрутизаторов Frame Relay.

- Определите, для каких физических площадок необходимо установить каналы доступа Frame Relay, и определите частоту синхронизации (clock rate), т.е. физическую скорость доступа (access rate), используемую на каждом канале.
- Определите каждый виртуальный канал за счет идентификации конечных точек и согласованную скорость CIR для каждого канала.
- Согласуйте тип интерфейса LMI (обычно задаваемого провайдером).

В дополнение к этому инженер должен выбрать конкретный стиль конфигурации на основе изложенных ниже положений. Для этого нет необходимости консультироваться с провайдером услуг Frame Relay.

- Выберите схему создания подсетей IP: одна подсеть для всех виртуальных каналов, по одной подсети для каждого виртуального канала или одна подсеть для каждой полносвязной (meshed) сети.
- Определите, следует ли назначать IP-адреса физическому, многоточечному или двухточечному субинтерфейсу.
- Выберите, каким виртуальным каналам потребуется использовать инкапсуляцию IETF вместо стандартного значения `cisco`. Инкапсуляция IETF обычно используется в тех случаях, когда один из маршрутизаторов не является устройством компании Cisco.

По завершении планирования этапы конфигурирования непосредственно вытекают из решений, принятых при планировании сети. Ниже обобщены этапы конфигурирования, главным образом для напоминания при подготовке к экзамену (нет необходимости запоминать все этапы, — этот список предназначен лишь для помощи в понимании конфигурации).

Ключевая тема

Последовательность настройки протокола Frame Relay

Этап 1 Настройте на физическом интерфейсе инкапсуляцию Frame Relay (команда интерфейса `encapsulation frame-relay interface`)

Этап 2 Настройте IP-адрес на интерфейсе или субинтерфейсе (подкоманда `ip address`)

Этап 3 (Необязательный.) Укажите вручную тип интерфейса LMI на каждом физическом последовательном интерфейсе (команда режима конфигурирования интерфейса `frame-relay lmi-type`)

Этап 4 (Необязательный.) Измените стандартный тип инкапсуляции `cisco` на `ietf`, выполнив следующие действия.
A. Для всех виртуальных каналов данного интерфейса добавьте ключевое слово `ietf` в команде интерфейса `encapsulation frame-relay`.
B. Для отдельного виртуального канала добавьте ключевое слово `ietf` в команде субинтерфейса `frame-relay interfacedlci` (только для двухточечных субинтерфейсов) или в команде `frame-relay map`.

Этап 5 (Необязательный.) Если вы не используете протокол Inverse ARP для преобразования идентификатора DLCI в IP-адрес маршрутизатора следующего перехода, то задайте статическую привязку адреса с помощью команды субинтерфейса `frame-relay map ip` *`ip-адрес идентификатор-dlci`* `broadcast`

Этап 6 На субинтерфейсах установите соответствие между одним (в случае двухточечного интерфейса) или несколькими (в случае многоточечного интерфейса) идентификаторами DLCI и субинтерфейсом одним из двух способов.
A. С помощью команды субинтерфейса `frame-relay interface-dlci` *`идентификатор-dlci`*.
B. Как побочный эффект статической привязки адреса — с помощью команды субинтерфейса `frame-relay map ip` *`идентификатор-dlci ip-адрес`* `broadcast` (только для многоточечных субинтерфейсов).

Далее в этом разделе рассматриваются примеры всех этих этапов конфигурирования, а также обсуждается вопрос о том, как проверить работу сети Frame Relay и убедиться в том, что она работает правильно.

Настройка с использованием физических интерфейсов и одной подсети IP

Первый пример иллюстрирует наиболее простой вариант сети Frame Relay, в котором используются только первые два этапа контрольного списка. Он включает в себя следующие действия.

- Установка канала доступа к трем маршрутизаторам.
- Создание полносвязной топологии каналов PVC.
- Использование одной подсети (сети 199.1.1.0 класса C) в сети протокола Frame Relay.
- Конфигурация физических интерфейсов.

Для интерфейса LMI, протокола Inverse ARP и инкапсуляции используются стандартные установки. В примерах 14.1–14.3 приведена конфигурация сети, показанная на рис. 14.1.

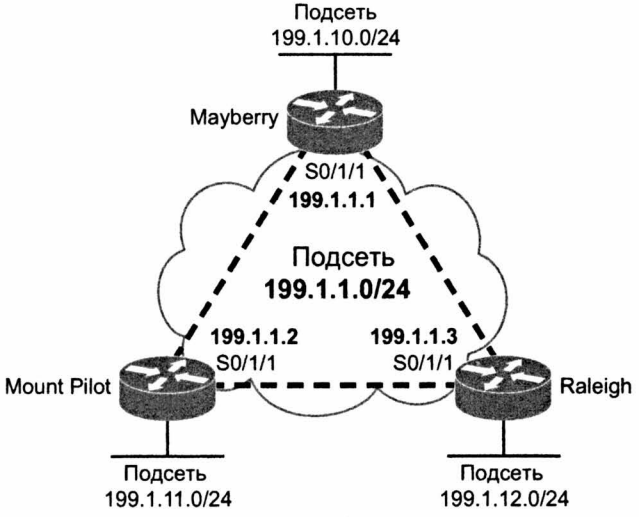


Рис. 14.1. Полносвязная топология с IP-адресами

Пример 14.1. Конфигурация маршрутизатора Mayberry

```
interface serial0/1/1
  encapsulation frame-relay
  ip address 199.1.1.1 255.255.255.0
!
interface gigabitethernet 0/0
  ip address 199.1.10.1 255.255.255.0
!
router eigrp 1
  network 199.1.1.0
  network 199.1.10.0
```

Пример 14.2. Конфигурация маршрутизатора Mount Pilot

```
interface serial0/1/1
  encapsulation frame-relay
  ip address 199.1.1.2 255.255.255.0
!
interface gigabitethernet 0/0
  ip address 199.1.11.2 255.255.255.0
!
router eigrp 1
  network 199.1.1.0
  network 199.1.11.0
```

Пример 14.3. Конфигурация маршрутизатора Raleigh

```
interface serial0/1/1
  encapsulation frame-relay
  ip address 199.1.1.3 255.255.255.0
!
interface gigabitethernet 0/0
  ip address 199.1.12.3 255.255.255.0
!
router eigrp 1
  network 199.1.1.0
  network 199.1.12.0
```

Конфигурация проста по сравнению с теоретическими принципами работы протокола. Команда `encapsulation frame-relay` предписывает маршрутизаторам использовать протоколы канального уровня технологии Frame Relay вместо стандартного протокола HDLC. Отметим, что IP-адреса всех трех последовательных интерфейсов маршрутизаторов принадлежат к той же сети класса C и данная простая конфигурация использует преимущества следующих стандартных настроек операционной системы Cisco IOS.

- Тип интерфейса LMI определяется автоматически.
- Типом инкапсуляции является Cisco.
- Идентификаторы DLCI каналов PVC определяются с помощью сообщений состояния интерфейса LMI.
- Протокол Inverse ARP включен и запускается после получения сообщения состояния о том, что виртуальные каналы включены (`up`).

Настройка инкапсуляции и типа LMI

В большинстве случаев применения стандартных значений, как в предыдущих примерах, вполне достаточно. Но для демонстрации альтернативной конфигурации предположим, что к требованиям проекта на рис. 14.1 были добавлены еще два:

- маршрутизатор Raleigh требует инкапсуляции IETF на обоих виртуальных каналах;
- типом LMI для маршрутизатора Mayberry должен быть ANSI, а автоматическое обнаружение типа LMI использоваться не должно.

Для изменения этих стандартных установок должны быть выполнены этапы, описанные как необязательные (этапы 3 и 4) в контрольном списке конфигурации, который приведен выше. В примерах 14.4 и 14.5 показаны изменения, которые были бы внесены для хостов Mayberry и Raleigh.

Пример 14.4. Конфигурация маршрутизатора Mayberry с учетом новых требований

```
interface serial0/1/1
  encapsulation frame-relay
  frame-relay lmi-type ansi
  frame-relay map ip 199.1.1.3 53 ietf
  ip address 199.1.1.1 255.255.255.0
! Остальные команды конфигурации совпадают с командами примера 14.1.
```

Пример 14.5. Конфигурация маршрутизатора Raleigh с учетом новых требований

```
interface serial0/1/1
  encapsulation frame-relay ietf
  ip address 199.1.1.3 255.255.255.0
! Остальные команды конфигурации совпадают с командами примера 14.3.
```

Эти конфигурации отличаются от предыдущих (см. примеры 14.1 и 14.2). Для маршрутизатора Raleigh изменена инкапсуляция обоих каналов PVC с помощью ключевого слова `ietf` в команде `encapsulation`. Это ключевое слово применяется ко всем виртуальным каналам на данном интерфейсе. Однако для маршрутизатора Mayberry изменить инкапсуляцию таким же способом нельзя, поскольку только одному из двух виртуальных каналов, которые заканчиваются на маршрутизаторе Mayberry, необходимо использовать инкапсуляцию IETF — другому нужно использовать инкапсуляцию Cisco. Поэтому для маршрутизатора Mayberry приходится использовать команду `frame-relay map`, в которой делается ссылка на данный идентификатор DLCI виртуального канала маршрутизатора Raleigh с помощью ключевого слова `ietf`. С помощью этой команды можно изменить тип инкапсуляции отдельно по каждому виртуальному каналу, в отличие от конфигурации на участке Raleigh, которая изменяет конфигурацию всех виртуальных каналов.

Вторым заметным изменением является альтернативное конфигурирование интерфейса LMI. Конфигурация интерфейса LMI на маршрутизаторе Mayberry будет правильно работать без каких-либо изменений, поскольку используемое автоматическое обнаружение LMI определит ANSI как тип интерфейса LMI. Однако при вводе подкоманды интерфейса `frame-relay lmi-type ansi` маршрутизатор Mayberry должен использовать стандарт ANSI, поскольку указанная команда не только устанавливает тип интерфейса LMI, но и отключает автоматическое согласование типа интерфейса LMI.

ВНИМАНИЕ!

Установка интерфейса LMI осуществляется по отдельным физическим интерфейсам, даже если используются субинтерфейсы, поэтому команда `frame-relay lmi-type` всегда является подкомандой для физического интерфейса.

Для маршрутизатора Mount Pilot необходимо настроить команду `frame-relay interface-dlci` с ключевым словом `ietf` для виртуального канала к маршрутизатору Raleigh, так же как и для Mayberry. Это изменение в примерах не показано.

Привязка адресов в протоколе Frame Relay

На рис. 14.1 не показаны настройки идентификаторов DLCI, используемых для виртуальных каналов. Конфигурации работают как нужно, и, откровенно говоря, эта сеть работала бы, даже если бы вы ничего не знали об идентификаторах DLCI.

Протокол Frame Relay сопоставляет IP-адрес следующей транзитной точки перехода, находящейся в сети Frame Relay, с идентификатором DLCI, обычно используемым для передачи фреймов на данное устройство следующей транзитной точки перехода, причем с той же целью, что и протокол ARP в сети LAN. На рис. 14.2 представлена та же сеть, но на сей раз с представленными локальными значениями DLCI.

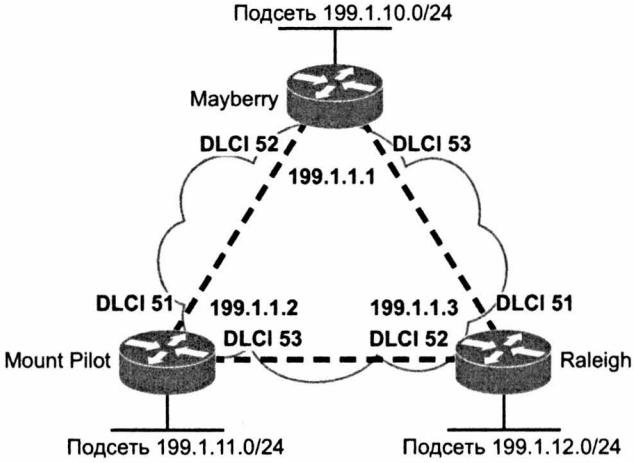


Рис. 14.2. Полносвязная топология с показанными глобальными идентификаторами DLCI

Сопоставление (mapping) протокола Frame Relay создает связь между адресом уровня 3 и соответствующим ему адресом уровня 2. Этот принцип аналогичен понятию кеша ARP для интерфейсов LAN. Например, кеш *протокола преобразования адресов* (IP Address Resolution Protocol — ARP), используемый в сетях LAN, представляет собой пример сопоставления адреса уровня 3 с адресом уровня 2. При использовании протокола ARP известен IP-адрес другого устройства в той же локальной сети LAN, но не известен его MAC-адрес; когда завершается работа протокола ARP, устройству становится известным LAN-адрес (уровня 2) другого устройства. Аналогично маршрутизаторам, использующим протокол Frame Relay, необходимо сопоставление адреса уровня 3 маршрутизатора и идентификатора DLCI, используемого для достижения другого маршрутизатора.

В данном разделе обсуждаются основные причины использования механизма сопоставления адресов для соединений сети LAN и сети Frame Relay, при этом основное внимание уделяется протоколу Frame Relay. Ниже приведено общее определение сопоставления адресов.

Основные понятия и определения сопоставления адресов протокола Frame Relay

Ключевая тема

Информация, отражающая привязку адреса уровня 3 маршрутизатора следующего транзитного узла к адресу уровня 2, используемого для его достижения, называется сопоставлением. Такое сопоставление необходимо в сетях с многостанционным доступом.

Размышления о маршрутизации сделают необходимость в сопоставлении более очевидной. Рассмотрим, например, пакет, поступающий на интерфейс LAN маршрутизатора Mayberry, предназначенный для сети 199.1.11.0/24 класса C с интерфейса LAN маршрутизатора Mount Pilot. Как показано на рис. 14.3, маршрутизатор проходит обычные этапы перенаправления, удаляя заголовок и концевик Ethernet из пакета, чтобы перенаправить пакет через интерфейс S0/1/1 маршрутизатора Mayberry на маршрутизатор Mount Pilot и далее. Но какой идентификатор DLCI маршрутизатор Mayberry должен поместить в новый заголовок Frame Relay?

На рис. 14.3, *слева*, представлены таблицы, используемые маршрутизатором Mayberry для выбора правильного идентификатора DLCI. Сначала маршрутизатор Mayberry находит маршрут для перенаправления пакета и выясняет IP-адрес следующего транзитного маршрутизатора. Затем в таблице сопоставления Frame Relay находится тот же IP-адрес следующего транзитного маршрутизатора наряду с идентификатором DLCI, используемым для передачи фрейма на этот адрес (эквивалент таблицы ARP). Наконец, маршрутизатор Mayberry помещает этот идентификатор DLCI (52 — локальный идентификатор DLCI маршрутизатора Mayberry для канала PVC к маршрутизатору Mount Pilot) в заголовок Frame Relay.

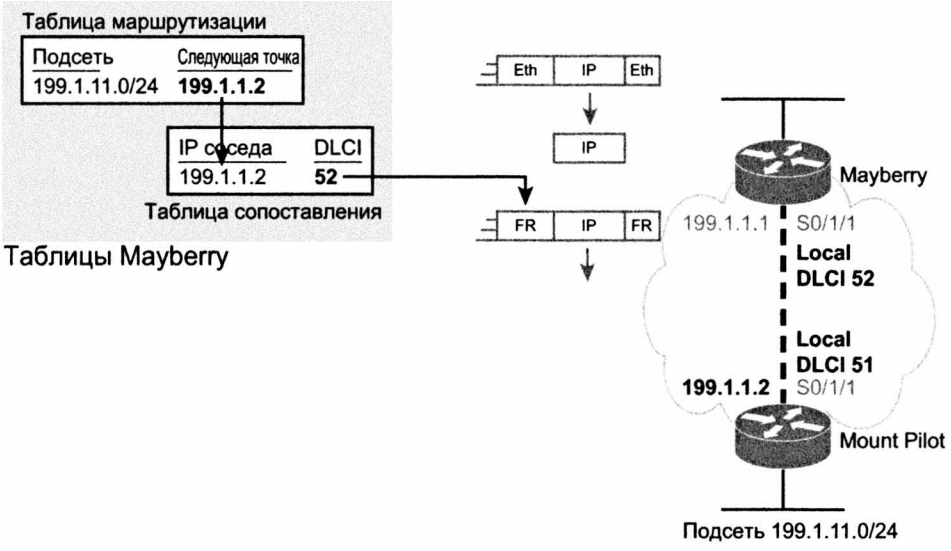


Рис. 14.3. Логика выбора правильного идентификатора DLCI на маршрутизаторе Mayberry

Интересно, что, подобно протоколу ARP, протокол Frame Relay осуществляет сопоставление адресов внутренне, без необходимости разрешения. Пример 14.6 объединяет все элементы сопоставления на рис. 14.3. В примере представлена таб-

лица маршрутизации, каналы PVC (включая идентификаторы DLCI) и таблица сопоставления Frame Relay на маршрутизаторе Mayberry.

Пример 14.6. Команды show маршрутизатора Mayberry, демонстрирующие сопоставление адресов

```
Mayberry# show ip route
Codes: L - local, 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, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

     199.1.1.0/24 is variably subnetted, 2 subnets, 2 masks
C      199.1.1.0/24 is directly connected, Serial0/1/1
L      199.1.1.1/32 is directly connected, Serial0/1/1
     199.1.10.0/24 is variably subnetted, 2 subnets, 2 masks
C      199.1.10.0/24 is directly connected, GigabitEthernet0/0
L      199.1.10.1/32 is directly connected, GigabitEthernet0/0
D      199.1.11.0/24 [90/2172416] via 199.1.1.2, 00:00:03, Serial0/1/1
D      199.1.12.0/24 [90/2172416] via 199.1.1.3, 00:19:14, Serial0/1/1

Mayberry# show frame-relay pvc

PVC Statistics for interface Serial0/1/1 (Frame Relay DTE)
            Active     Inactive     Deleted     Static
Local          2           0           0          0
Switched       0           0           0          0
Unused         0           0           0          0

DLCI = 52, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Seri-
al0/1/1

    input pkts 37 output pkts 39 in bytes 2542
    out bytes 2752 dropped pkts 0 in pkts dropped 0
    out pkts dropped 0 out bytes dropped 0
    in FECN pkts 0 in BECN pkts 0 out FECN pkts 0
    out BECN pkts 0 in DE pkts 0 out DE pkts 0
    out bcast pkts 26 out bcast bytes 1664
    5 minute input rate 0 bits/sec, 0 packets/sec
    5 minute output rate 0 bits/sec, 0 packets/sec
    pvc create time 00:20:02, last time pvc status changed 00:20:02

DLCI = 53, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Seri-
al0/1/1

    input pkts 37 output pkts 37 in bytes 2618
    out bytes 2746 dropped pkts 0 in pkts dropped 0
    out pkts dropped 0 out bytes dropped 0
    in FECN pkts 0 in BECN pkts 0 out FECN pkts 0
    out BECN pkts 0 in DE pkts 0 out DE pkts 0
```

```
    out bcast pkts 25 out bcast bytes 1630
    5 minute input rate 0 bits/sec, 0 packets/sec
    5 minute output rate 0 bits/sec, 0 packets/sec
    pvc create time 00:20:02, last time pvc status changed 00:20:02

Mayberry# show frame-relay map
Serial0/1/1 (up): ip 199.1.1.2 dlci 52(0x34,0xC40), dynamic,
                  broadcast,, status defined, active
Serial0/1/1 (up): ip 199.1.1.3 dlci 53(0x35,0xC50), dynamic,
                  broadcast,, status defined, active
```

В данном примере выделена информация для маршрутизатора Mayberry, относящаяся к отправке пакетов для сети 199.1.11.0/24 от хоста Mount Pilot. Маршрут устройства Mayberry к сети 199.1.11.0 ссылается на выходной интерфейс Serial 0/1/1 и на 199.1.1.2, как на адрес следующего транзитного перехода. В команде `show frame-relay pvc` содержатся два идентификатора DLCI, с номерами 52 и 53, и оба они активны. Как маршрутизатор Mayberry узнает эти идентификаторы DLCI? Сообщения состояния интерфейса LMI информируют устройство о виртуальных каналах, связанных с ними идентификаторах DLCI и о их состоянии (активное).

Какой идентификатор DLCI должен использовать маршрутизатор Mayberry для пересылки пакета? Ответ на этот вопрос содержится в информации, выводимой командой `show frame-relay map`. Следует обратить внимание на выделенную фразу "`ip 199.1.1.2 dlci 52`" в приведенном выводе. Каким-то образом маршрутизатор Mayberry преобразовал адрес 199.1.1.2 (адрес следующего перехода на маршруте) в правильный локальный идентификатор DLCI, который имеет значение 52. Поэтому устройство Mayberry "знает" о том, что для достижения IP-адреса следующего перехода 199.1.1.2 следует использовать локальный идентификатор DLCI с номером 52.

Для создания сопоставления, показанного на рис. 14.7, маршрутизатор Mayberry может использовать два метода. Одним из них является сопоставление, настроенное статически, а во втором используется динамический процесс, называемый протоколом Inverse ARP (обратным ARP). В следующих двух подразделах описаны детали каждого из двух методов.

Протокол Inverse ARP

Протокол Inverse ARP динамически создает сопоставление адреса уровня 3 (например, IP-адреса) с адресом уровня 2 (локальный идентификатор DLCI). Окончательный результат работы протокола Inverse ARP такой же, как и у протокола ARP технологии IP в сети LAN: маршрутизатор создает сопоставление адреса уровня 3 соседнего маршрутизатора с соответствующим адресом уровня 2. Однако процесс, используемый протоколом Inverse ARP, отличается от применяемого в протоколе ARP локальной сети. После того как виртуальный канал установлен, каждый маршрутизатор анонсирует свой адрес сетевого уровня, отправляя сообщение протокола Inverse ARP по этому виртуальному каналу. Принцип работы протокола показан на рис. 14.4.

Как показано на рис. 14.4, протокол Inverse ARP анонсирует адреса уровня 3 сразу после того, как интерфейс LMI сообщает о том, что каналы PVC установлены. Сначала протокол Inverse ARP определяет адрес канального уровня DLCI (при посредничестве сообщений интерфейса LMI), а затем анонсирует собственные адреса уровня 3, которые используют этот виртуальный канал. Протокол Inverse ARP обычно включен в маршрутизаторах компании Cisco.

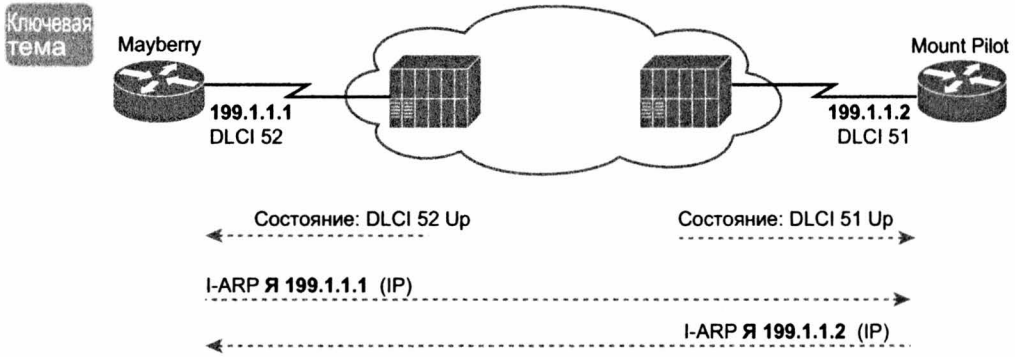


Рис. 14.4. Принцип работы протокола Inverse ARP

В примере 14.6 в выводе команды `show frame-relay map` маршрутизатору Mayberry соответствуют две строки. Маршрутизатор Mayberry использует протокол Inverse ARP для того, чтобы узнать, что идентификатор DLCI 52 сопоставлен с IP-адресом следующего транзитного перехода 199.1.1.2, а идентификатор DLCI 53 сопоставлен с IP-адресом следующего перехода 199.1.1.3. Интересно отметить, что рассматриваемое устройство получает эту информацию с помощью сообщений протокола Inverse ARP от маршрутизаторов Mount Pilot и Raleigh соответственно.

В работе процесса Inverse ARP есть несколько тонкостей. В первую очередь, сообщения Inverse ARP объявляют IP-адрес маршрутизатора во фрейме, передаваемом по каналу PVC. Получающий маршрутизатор узнает IP-адрес из сообщения и выясняет идентификатор DLCI из фрейма InARP. На рис. 14.4 показано:

- маршрутизатор Mayberry посылает сообщение InARP с IP-адресом 199.1.1.1; маршрутизатор Mount Pilot получает сообщение InARP с идентификатором DLCI 51 в заголовке, таким образом маршрутизатор Mount Pilot сопоставляет IP-адрес 199.1.1.1 с идентификатором DLCI 51;
- маршрутизатор Mount Pilot посылает сообщение InARP с IP-адресом 199.1.1.2; маршрутизатор Mayberry получает сообщение InARP с идентификатором DLCI 52 в заголовке, таким образом маршрутизатор Mayberry сопоставляет IP-адрес 199.1.1.2 с идентификатором DLCI 52.

Статическое сопоставление адреса для протокола Frame Relay

Сопоставление адреса можно настроить статически, без использования протокола Inverse ARP. В корпоративной сети инженер, вероятно, сразу перейдет к использованию протокола Inverse ARP, поскольку так много проще. Для сдачи экзамена читателю следует знать, как выглядят команды статического сопоставления. В примере 14.7 осуществляется статическое сопоставление адресов Frame Relay для трех маршрутизаторов, показанных на рис. 14.2, а также конфигурация, используемая для отключения протокола Inverse ARP.

Пример 14.7. Команды `frame-relay map`

```
Mayberry
interface serial 0/1/1
```

```
  no frame-relay inverse-arp
  frame-relay map ip 199.1.1.2 52 broadcast
  frame-relay map ip 199.1.1.3 53 broadcast
! ------------------------------------------------------------------
Mount Pilot
interface serial 0/1/1
  no frame-relay inverse-arp
  frame-relay map ip 199.1.1.1 51 broadcast
  frame-relay map ip 199.1.1.3 53 broadcast
! ------------------------------------------------------------------
Raleigh
interface serial 0/1/1
  no frame-relay inverse-arp
  frame-relay map ip 199.1.1.1 51 broadcast
  frame-relay map ip 199.1.1.2 52 broadcast
```

Чтобы лучше понять значение команды **frame-relay map**, рассмотрим пример ее применения на маршрутизаторе Mayberry, обращающемся по адресу 199.1.1.2. Команда отдается на маршрутизаторе Mayberry, поэтому он добавляет запись сопоставления в свою таблицу. Команда указывает маршрутизатору Mayberry, что когда он посылает пакет по адресу 199.1.1.2 (на Mount Pilot), он должен использовать идентификатор DLCI 52. Оператор **frame-relay map** на маршрутизаторе Mayberry коррелирует IP-адрес маршрутизатора Mount Pilot (199.1.1.2) с локальным идентификатором DLCI, используемым для доступа к маршрутизатору Mount Pilot, а именно идентификатором DLCI 52.

В качестве другого примера рассмотрите команду **frame-relay map ip 199.1.1.1 51 broadcast** на маршрутизаторе Mount Pilot, которая создает запись сопоставления для маршрутизатора Mount Pilot. Когда он посылает пакет по адресу 199.1.1.1 (на маршрутизатор Mayberry), то использует идентификатор DLCI 51.

Необходимо сопоставление каждого адреса уровня 3 следующего перехода с каждым адресом маршрутизируемого протокола уровня 3. Даже если сеть невелика, такой процесс конфигурирования может оказаться весьма трудоемким!

ВНИМАНИЕ!

Ключевое слово `broadcast` в команде `frame-relay map` необходимо в тех случаях, когда маршрутизатору нужно отправить широковещательные сообщения или сообщения многоадресатной рассылки соседнему маршрутизатору, например, для поддержки сообщений протокола маршрутизации, таких как сообщения Hello.

Настройка двухточечных субинтерфейсов

Второй пример сети, на базе схемы согласно рис. 14.5, использует двухточечные субинтерфейсы. Двухточечные субинтерфейсы работают хорошо, когда проект подсетей предполагает по одной подсети для каждого канала PVC. Примеры 14.8–14.11 демонстрируют конфигурацию для этого примера сети со всеми четырьмя маршрутизаторами, использующими только двухточечные субинтерфейсы. Обратите особое внимание на приглашения к вводу команд в примере 14.8, поскольку они изменяются по мере настройки субинтерфейсов.

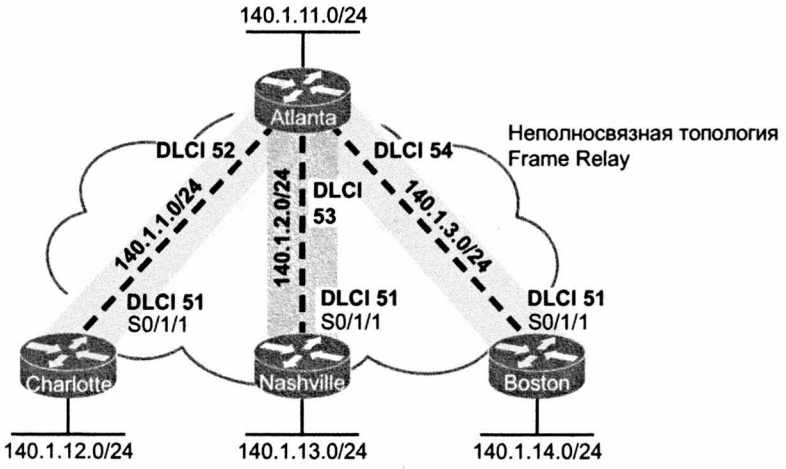


Рис. 14.5. Неполносвязная топология с IP-адресами и глобальными идентификаторами DLCI

Пример 14.8. Конфигурация маршрутизатора Atlanta

```
Atlanta(config)# interface serial0/1/1
Atlanta(config-if)# encapsulation frame-relay

Atlanta(config-if)# interface serial 0/1/1.1 point-to-point
Atlanta(config-subif)# ip address 140.1.1.1 255.255.255.0
Atlanta(config-subif)# frame-relay interface-dlci 52

Atlanta(config-fr-dlci)# interface serial 0/1/1.2 point-to-point
Atlanta(config-subif)# ip address 140.1.2.1 255.255.255.0
Atlanta(config-subif)# frame-relay interface-dlci 53

Atlanta(config-fr-dlci)# interface serial 0/1/1.3 point-to-point
Atlanta(config-subif)# ip address 140.1.3.1 255.255.255.0
Atlanta(config-subif)# frame-relay interface-dlci 54

Atlanta(config-fr-dlci)# interface gigabitethernet 0/0
Atlanta(config-if)# ip address 140.1.11.1 255.255.255.0
```

Пример 14.9. Конфигурация маршрутизатора Charlotte

```
interface serial0/1/1
encapsulation frame-relay
!
interface serial 0/1/1.1 point-to-point
  ip address 140.1.1.2 255.255.255.0
frame-relay interface-dlci 51
!
interface gigabitethernet 0/0
ip address 140.1.12.2 255.255.255.0
```

Пример 14.10. Конфигурация маршрутизатора Nashville

```
interface serial0/1/1
encapsulation frame-relay
!
interface serial 0/1/1.2 point-to-point
  ip address 140.1.2.3 255.255.255.0
frame-relay interface-dlci 51
!
interface gigabitethernet 0/0
  ip address 140.1.13.3 255.255.255.0
```

Пример 14.11. Конфигурация маршрутизатора Boston

```
interface serial0/1/1
encapsulation frame-relay
!
interface serial 0/1/1.3 point-to-point
  ip address 140.1.3.4 255.255.255.0
frame-relay interface-dlci 51
!
interface gigabitethernet 0/0
  ip address 140.1.14.4 255.255.255.0
```

Как и ранее, в этой конфигурации присутствует много стандартных значений, однако некоторые параметры отличаются от тех, которые настраивались на физическом интерфейсе. Тип интерфейса LMI распознается автоматически, используется инкапсуляция Cisco, как и в примерах полносвязной топологии. В двухточечных интерфейсах на самом деле протокол Inverse ARP не нужен, однако он по умолчанию включен, чтобы в том случае, когда маршрутизатору на другом конце виртуального канала необходимо использовать протокол Inverse ARP, он мог с ним работать.

Для создания конфигурации, необходимой двухточечным (point-to-point) субинтерфейсам, используются две новые команды. Первая из них — команда `interface serial 0/1/1.1 point-to-point` — создает логический субинтерфейс с номером 1 на физическом интерфейсе Serial0/1/1.1. Эта команда определяет также субинтерфейс как двухточечный, а не многоточечный. Далее следует ассоциировать с субинтерфейсом один канал PVC; подкоманда субинтерфейса `frame-relay interface-dlci` укажет маршрутизатору один локальный идентификатор DLCI, ассоциируемый с этим субинтерфейсом.

Понять конфигурацию поможет пример выполнения команды `frame-relay interface-dlci`. Рассмотрим маршрутизатор Atlanta на рис. 14.5. Устройство получает сообщения LMI на интерфейсе Serial0/1/1.1, в которых утверждается, что установлены три виртуальных канала с локальными идентификаторами DLCI 52–54. Возникает вопрос: с каким каналом PVC работает каждый субинтерфейс? Операционной системе Cisco IOS нужно связать правильный канал PVC с соответствующим интерфейсом. Это осуществляется с помощью команды `frame-relay interface-dlci`.

Уделите минуту внимания настройке всех субинтерфейсов командой конфигурации `frame-relay interface-dlci` в примерах 14.8–14.11 и сравнению их

с идентификаторами DLCI и IP-адресами подсетей на рис. 14.5. Обратите внимание, что в каждом случае локальный идентификатор DLCI, заданный в команде `framerelay interface-dlci`, соответствует подсети (на основании команд `ip address`).

Прежде чем завершить тему настройки двухточечного соединения, обратим внимание на субинтерфейсы. Номера субинтерфейсов необязательно должны соответствовать номерам идентификаторов маршрутизатора; то же относится и к номерам локальных идентификаторов DLCI. В данном примере субинтерфейсы были пронумерованы так, как показано, лишь для удобства запоминания. На практике в номере субинтерфейса полезно указывать некоторую информацию о схеме нумерации в сети.

Например, возможно, что компания внесет в номер субинтерфейса часть идентификатора ID несущего канала для того, чтобы операционный персонал при поиске ошибок на линии мог найти и сообщить правильные сведения телекоммуникационной компании (telco). На многих площадках в качестве номера субинтерфейса используется идентификатор DLCI. Конечно, полезная для поиска ошибок информация (например, идентификатор DLCI и имя маршрутизатора на другом конце виртуального канала) также может быть задана как текст с помощью команды `description`. В любом случае соответствие номеров субинтерфейсов не требуется. В данном примере номер субинтерфейса просто соответствует третьему октету IP-адреса.

Проверка двухточечного канала Frame Relay

В примере 14.12 показан вывод наиболее популярных команд EXEC технологии Frame Relay в операционной системе Cisco IOS для мониторинга работы протокола Frame Relay на маршрутизаторе Atlanta.

Пример 14.12. Вывод по командам EXEC на маршрутизаторе Atlanta

```
Atlanta# show frame-relay pvc

PVC Statistics for interface Serial0/1/1 (Frame Relay DTE)

            Active   Inactive   Deleted   Static
Local          2          0         0        0
Switched       0          0         0        0
Unused         1          0         0        0

DLCI = 52, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Seri-
al0/1/1

  input pkts 80        output pkts 76    in bytes 5940
  out bytes 5594       dropped pkts 0    in pkts dropped 0
  out pkts dropped 0 out bytes dropped 0
  in FECN pkts 0       in BECN pkts 0    out FECN pkts 0
  out BECN pkts 0      in DE pkts 0      out DE pkts 0
  out bcast pkts 45  out bcast bytes 3030
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
  pvc create time 00:39:49, last time pvc status changed 00:27:29
```

```
DLCI = 53, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial0/1/1

  input pkts 64       output pkts 82    in bytes 4206
  out bytes 6612      dropped pkts 0    in pkts dropped 0
  out pkts dropped 0  out bytes dropped 0
  in FECN pkts 0      in BECN pkts 0    out FECN pkts 0
  out BECN pkts 0     in DE pkts 0      out DE pkts 0
  out bcast pkts 38   out bcast bytes 2532
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
  pvc create time 00:33:49, last time pvc status changed 00:27:19

DLCI = 54, DLCI USAGE = UNUSED, PVC STATUS = ACTIVE, INTERFACE = Serial0/1/1

  input pkts 0        output pkts 0     in bytes 0
  out bytes 0         dropped pkts 0    in pkts dropped 0
  out pkts dropped 0  out bytes dropped 0
  in FECN pkts 0      in BECN pkts 0    out FECN pkts 0
  out BECN pkts 0     in DE pkts 0      out DE pkts 0
  out bcast pkts 0 out bcast bytes 0 5 minute input rate 0 bits/sec, 0
packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
  pvc create time 00:00:59, last time pvc status changed 00:00:59

Atlanta# show frame-relay map
Serial0/0/0.3 (up): point-to-point dlci, dlci 54(0x36,0xC60), broadcast
                    status defined, active
Serial0/0/0.2 (up): point-to-point dlci, dlci 53(0x35,0xC50), broadcast
                    status defined, active
Serial0/0/0.1 (up): point-to-point dlci, dlci 52(0x34,0xC40), broadcast
                    status defined, active

Atlanta# debug frame-relay lmi
Frame Relay LMI debugging is on
Displaying all Frame Relay LMI data

Serial0/0/0(out): StEnq, myseq 163, yourseen 161, DTE up
datagramstart = 0x45AED8, datagramsize = 13
FR encap = 0xFCF10309
00 75 01 01 01 03 02 A3 A1

Serial0/0/0(in): Status, myseq 163
RT IE 1, length 1, type 1
KA IE 3, length 2, yourseq 162, myseq 163
```

По команде `show frame-relay pvc` выводится полезная управляющая информация. В частности, вывод включает множество коэффициентов и счетчиков для пакетов, проходящих через каждый постоянный виртуальный канал (PVC). Кроме того, состояние канала PVC — это хорошая точка для начала поиска ошибок.

Команда `show frame-relay map` выводит информацию о сопоставлении адресов. В приведенном ранее примере полносвязной топологии без использования субинтерфейсов был приведен адрес уровня 3 для каждого идентификатора DLCI. В данном примере идентификатор DLCI приведен для каждой позиции, однако не приводятся ссылки на соответствующие адреса уровня 3. Вся суть сопоставления

состоит в установлении связи между адресами уровня 3 и уровня 2, однако в выводе команды `show frame-relay map` адрес уровня 3 не приводится!

Причина, по который маршрутизаторы с двухточечными субинтерфейсами могут найти правильную информацию сопоставления только в локальной конфигурации, приведены ниже.

- Маршрутизатор соответствует маршруту, передающему пакет через двухточечный субинтерфейс.
- Маршрутизатор ищет одну (и только одну) команду конфигурации `frame-relay interface-dlci` на данном субинтерфейсе и использует ее DLCI при упаковке пакета.

И наконец, в выводе команды `debug frame-relay lmi` приводится информация для отправки и получения запросов к интерфейсам LMI. Коммутатор отправляет сообщения состояния, а устройство типа DTE (маршрутизатор) посылает запрос состояния. В программном обеспечении Cisco включены отправка и прием таких сообщений состояния. Команда `no keepalive` системы Cisco IOS используется для отключения сообщений о состоянии интерфейсов LMI. В отличие от других интерфейсов, тестовые сообщения (keepalive) в устройствах компании Cisco не пересылаются от одного маршрутизатора к другому по протоколу Frame Relay. Вместо этого они просто используются для проверки наличия соединения маршрутизатора с его локальным коммутатором Frame Relay.

Настройка при многоточечных субинтерфейсах

Для конфигурирования сети протокола Frame Relay можно также использовать многоточечные интерфейсы. В последнем варианте топологии, основанном на сети, показанной на рис. 14.6, используются как многоточечные субинтерфейсы, так и двухточечные. В примерах 14.13–14.17 показана конфигурация этой сети. В табл. 14.1 обобщены используемые адреса и субинтерфейсы.

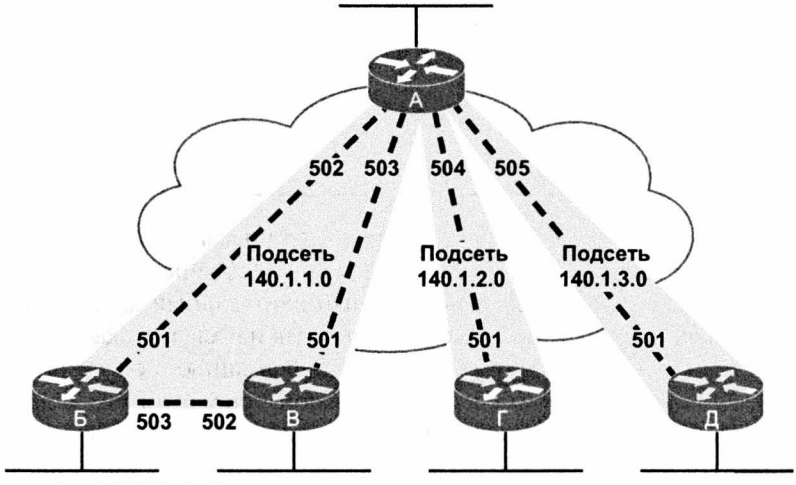


Рис. 14.6. Гибридная сеть: неполносвязная и полносвязная топологии

Пример 14.13. Конфигурация маршрутизатора А

```
interface serial0/1/1
  encapsulation frame-relay
!
interface serial 0/1/1.1 multipoint
  ip address 140.1.1.1 255.255.255.0
  frame-relay interface-dlci 502
  frame-relay interface-dlci 503
!
interface serial 0/0/0.2 point-to-point
  ip address 140.1.2.1 255.255.255.0
  frame-relay interface-dlci 504
!
interface serial 0/1/1.3 point-to-point
  ip address 140.1.3.1 255.255.255.0
  frame-relay interface-dlci 505
```

Пример 14.14. Конфигурация маршрутизатора Б

```
interface serial0/0/0
  encapsulation frame-relay
!
interface serial 0/1/1.1 multipoint
  ip address 140.1.1.2 255.255.255.0
  frame-relay interface-dlci 501
  frame-relay interface-dlci 503
```

Пример 14.15. Конфигурация маршрутизатора В

```
interface serial0/1/1
  encapsulation frame-relay
!
interface serial 0/1/1.1 multipoint
  ip address 140.1.1.3 255.255.255.0
  frame-relay interface-dlci 501
  frame-relay interface-dlci 502
```

Пример 14.16. Конфигурация маршрутизатора Г

```
interface serial0/1/1
  encapsulation frame-relay
!
interface serial 0/1/1.1 point-to-point
  ip address 140.1.2.4 255.255.255.0
  frame-relay interface-dlci 501
```

Пример 14.17. Конфигурация маршрутизатора Д

```
interface serial0/1/1
  encapsulation frame-relay
!
interface serial 0/1/1.1 point-to-point
  ip address 140.1.3.5 255.255.255.0
  frame-relay interface-dlci 501
```

Таблица 14.1. IP-адреса двух- и многоточечных субинтерфейсов

Маршрутизатор	Подсеть	IP-адрес	Тип субинтерфейса
А	140.1.1.0/24	140.1.1.1	Многоточечный
Б	140.1.1.0/24	140.1.1.2	Многоточечный
В	140.1.1.0/24	140.1.1.3	Многоточечный
А	140.1.2.0/24	140.1.2.1	Двухточечный
Г	140.1.2.0/24	140.1.2.4	Двухточечный
А	140.1.3.0/24	140.1.3.1	Двухточечный
Д	140.1.3.0/24	140.1.3.5	Двухточечный

Многоточечные субинтерфейсы наиболее эффективны в тех случаях, когда набор маршрутизаторов образует полносвязную топологию. В маршрутизаторах А, Б и В многоточечный субинтерфейс используется для того, чтобы в конфигурации выполнялись ссылки на два других маршрутизатора, поскольку эти три маршрутизатора можно рассматривать как полносвязную подсеть более обширной сети.

Термин "многоточечный интерфейс" означает, что имеется более одного виртуального канала, благодаря чему отправлять и получать пакеты на субинтерфейсе можно более чем с одного виртуального канала. Как и в двухточечных субинтерфейсах, в многоточечных интерфейсах используется команда `frame-relay interface-dlci`. Необходимо обратить внимание на то, что для каждого многоточечного субинтерфейса в данном случае имеются две команды, поскольку каждый из связанных с ним двух каналов PVC должен быть идентифицирован как используемый этим субинтерфейсом.

Только маршрутизатор А использует как многоточечный, так и двухточечный субинтерфейс. Для маршрутизатора А на многоточечном интерфейсе Serial0/0/0.1 приведены идентификаторы для маршрутизаторов Б и В. На двух других двухточечных субинтерфейсах маршрутизатора А требуется отображения только одного идентификатора DLCI. Фактически на двухточечном субинтерфейсе допускается только одна команда `frame-relay interface-dlci`, так как разрешен лишь один виртуальный канал. В противном случае конфигурации для этих двух типов совпадали бы.

Для конфигураций, показанных в примерах 14.13–14.17, команды сопоставления не нужны, поскольку на многоточечных субинтерфейсах протокол Inverse ARP обычно включен. Не нужны преобразования и для двухточечного субинтерфейса, поскольку единственный идентификатор DLCI, связанный с данным интерфейсом, статически задается командой `frame-relay interface-dlci`.

В примере 14.18 приведена еще одна команда `show frame-relay map`, отображающая информацию о преобразовании, полученную протоколом Inverse ARP для многоточечного субинтерфейса. Следует обратить внимание на то, что теперь вывод содержит адреса уровня 3, в то время как при использовании двухточечного субинтерфейса та же команда этих адресов не выводит. Маршрутизатор должен сопоставить информацию о многоточечных субинтерфейсах, чтобы при перенаправлении пакетов через субинтерфейс маршрутизатор мог выбрать правильный идентификатор DLCI для инкапсуляции пакета.

Пример 14.18. Сопоставления протокола Frame Relay и протокола Inverse ARP в маршрутизаторе B

```
RouterC# show frame-relay map
Serial0/1/1.1 (up): ip 140.1.1.1 dlci 501(0x1F5,0x7C50), dynamic,
                    broadcast,, status defined, active
Serial0/1/1.1 (up): ip 140.1.1.2 dlci 502(0x1F6,0x7C60), dynamic,
                    broadcast,, status defined, active
```

Проблемы протокола OSPF на многоточечных субинтерфейсах и физических интерфейсах Frame Relay

Во многих корпоративных сетях, использующих технологию Frame Relay, инженеры решают использовать только двухточечные субинтерфейсы Frame Relay. Большинство глобальных сетей Frame Relay соединяют дистанционные площадки с центральной площадкой, поэтому двухточечная модель работает хорошо. Кроме того, *открытый протокол поиска первого кратчайшего маршрута* (Open Shortest Path First — OSPF) и *расширенный протокол маршрутизации внутреннего шлюза* (Enhanced Interior Gateway Routing Protocol — EIGRP) хорошо работают со стандартными настройками по двухточечным субинтерфейсам Frame Relay.

Однако протокол OSPF требует немного больше внимания при настройке в конфигурации с использованием многоточечных или физических интерфейсов Frame Relay. В данном разделе кратко описаны эти проблемы.

Использующие протокол OSPF маршрутизаторы не становятся соседями по физическим интерфейсам или многоточечным субинтерфейсам Frame Relay с использованием только конфигурации OSPF, описанной в главе 8. Проблема? Физические и многоточечные субинтерфейсы Frame Relay изначально используют не широковещательный тип сети OSPF. Этот тип сети OSPF означает, что маршрутизатор не будет пытаться динамически обнаруживать соседей OSPF на данном интерфейсе.

Проблема OSPF имеет несколько решений, и простейшее из них подразумевает изменение типа сети OSPF на интерфейсах Frame Relay. (Концепция типов сети OSPF для интерфейсов представлена в главе 8, но перед обсуждением данной проблемы следовало получить представление о технологии Frame Relay.) Конкретное решение: изменение типа сети OSPF на многоточечное соединение позволяет маршрутизаторам динамически обнаруживать друг друга по физическому или многоточечному субинтерфейсу.

В примерах 14.13–14.15 все представленные маршрутизаторы использовали многоточечный субинтерфейс и совместно использовали ту же подсеть. При использовании протокола OSPF все три маршрутизатора должны стать соседями OSPF. Для этого, помимо обычной настройки протокола OSPF, следует разрешить протокол OSPF на многоточечном субинтерфейсе каждого маршрута при помощи команды `ip ospf network point-to-multipoint` на многоточечных субинтерфейсах всех трех маршрутизаторов.

Эта команда изменяет тип сети OSPF на многоточечное соединение, указывающее каждому маршрутизатору динамически обнаруживать соседей (и не использовать выделенный маршрутизатор или резервный выделенный маршрутизатор (DR/BDR)).

ВНИМАНИЕ!

Хороший совет: при первом чтении этой главы сделайте здесь перерыв и отдохните, прежде чем перейти к разделу о поиске и устранении неисправностей. Не торопитесь, попрактикуйтесь в настройке конфигурации Frame Relay, используя любые доступные лабораторной работы по своему выбору (реальные устройства, эмулятор и т.д.).

Поиск и устранение неисправностей в протоколе Frame Relay

Протокол Frame Relay имеет много функций и настраиваемых опциональных параметров. Как в реальной работе, так и в процессе сдачи экзамена поиск проблем в протоколе Frame Relay часто означает, что придется просмотреть конфигурации всех маршрутизаторов и убедиться в том, что эти конфигурации соответствуют определенным требованиям. Типы интерфейсов LMI маршрутизаторов должны соответствовать друг другу или определяться автоматически, *информация сопоставления* (mapping information) должна быть получена через стандартные протоколы или указана статически, с каждым субинтерфейсом должны быть связаны правильные значения идентификаторов DLCI и т.д. Поэтому, чтобы хорошо подготовиться к экзаменам CCNA, нужно запомнить многие опциональные параметры конфигурирования протокола Frame Relay, а также назначение каждого из них.

Однако экзамен может содержать вопросы по протоколу Frame Relay, которые требуют определения причины проблемы без просмотра конфигурации. В этом разделе рассматриваются поиск и устранение ошибок протокола Frame Relay, причем основное внимание уделяется использованию команд `show`, которые вместе с анализом признаков возникшей проблемы применяются для локализации ее основной причины.

Устранение ошибок в протоколе Frame Relay

Чтобы локализовать проблему, возникшую в протоколе Frame Relay, следует начать с выполнения нескольких команд `ping`. В оптимальном случае эта операция, выполненная с хоста конечного пользователя локальной сети в дистанционную сеть LAN, позволяет быстро определить, удовлетворяет ли в настоящее время сеть конечной цели пересылки пакетов между компьютерами. Если такая попытка неудачна, то следующим шагом будет запуск команды `ping` с IP-адресом дистанционного маршрутизатора в качестве аргумента команды. Если такая команда `ping` работает, а команда `ping` от конечного пользователя неудачна, то проблема, вероятно, имеет отношение к вопросам уровня 3 (поиск и устранение таких ошибок были подробно освещены в главах 4 и 11). Однако если результат команды `ping` окажется неудачным, то проблема, вероятнее всего, связана с самой сетью Frame Relay.

В данном разделе основное внимание уделяется задачам поиска и устранения неисправностей в тех случаях, когда результат выполнения команды `ping` для маршрутизатора является отрицательным. На данном этапе сетевой инженер должен выполнить команду `ping` по IP-адресу протокола Frame Relay всех остальных маршрутизаторов на другом конце каждого виртуального канала и ответить на приведенный ниже вопрос.

Для всех ли IP-адресов протокола Frame Relay дистанционных маршрутизаторов проверка `ping` *завершается неудачно, или одни пакеты* `ping` *не проходят, а другие проходят?*

Например, на рис. 14.7 приведен пример сети протокола Frame Relay, которая будет использоваться в оставшейся части данной главы. Если инженер в маршрутизаторе R1 пытался выполнить команду `ping` для IP-адреса протокола Frame Relay маршрутизатора R2 (в данном случае для адреса 10.1.2.2) и она завершилась неудачно, то нужно ответить на следующий вопрос: будут ли работать команды `ping` маршрутизатора R1 для маршрутизаторов R3 (10.1.34.3) и R4 (10.1.34.4)?

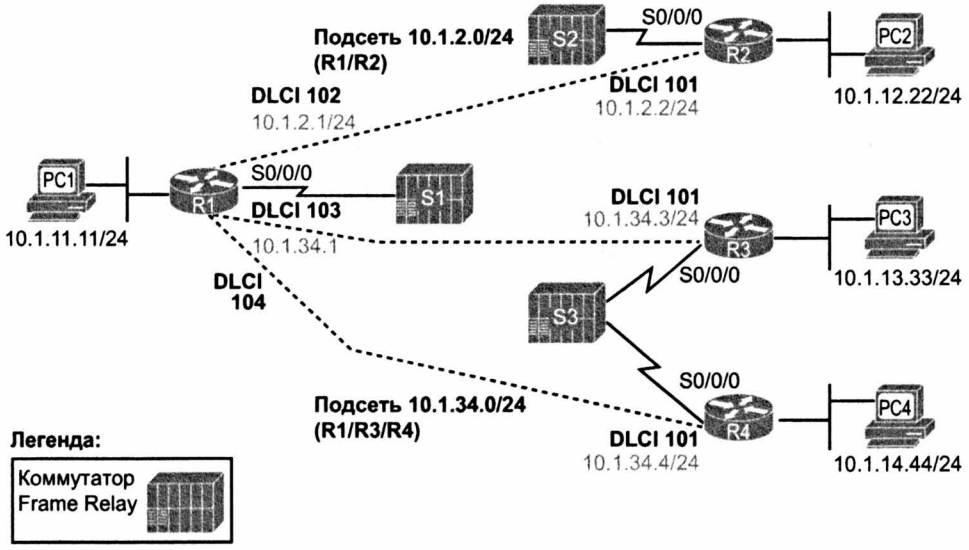


Рис. 14.7. Пример сети протокола Frame Relay для иллюстрации процесса поиска ошибок

В данной главе описание процесса поиска и устранения ошибок протокола Frame Relay опирается на рассмотренный выше этап 1 локализации проблемы. Ниже обобщаются основные действия и подробно рассматривается каждый этап.

Если команды `ping` для маршрутизатора, подключенного к среде Frame Relay, не работают для всех дистанционных маршрутизаторов, виртуальные каналы которых совместно используют один канал доступа, то выполните следующие действия.

Процесс поиска и устранения ошибок протокола Frame Relay, включающий в себя шесть этапов

Ключевая тема

Этап 1 Проверьте наличие проблем уровня 1 в канале доступа между маршрутизатором и локальным коммутатором Frame Relay (для всех маршрутизаторов)

Этап 2 Проверьте наличие проблем уровня 2 в канале доступа, в частности, связанных с инкапсуляцией и интерфейсом LMI

После устранения всех проблем, обнаруженных на этих двух этапах, или после того, как первоначальные тестовые команды `ping` показали, что маршрутизатор Frame Relay может выполнить команды `ping` для некоторых, но не всех маршрути-

заторов Frame Relay, виртуальные каналы которых совместно используют один канал доступа, выполните следующие действия.

Этап 3 Проверьте наличие проблем в виртуальных каналах PVC на основе состояния каналов PVC и субинтерфейса

Этап 4 Проверьте наличие проблем уровня 2 или 3, связанных со статическим или динамическим (протокол Inverse ARP) сопоставлением адресов

Этап 5 Проверьте наличие проблем уровня 2 или 3, связанных с несоответствием типов сквозной инкапсуляции (`cisco` или `ietf`)

Этап 6 Проверьте наличие других проблем уровня 3, включая возможное несоответствие подсетей

В оставшейся части данной главы описаны некоторые подробности каждого этапа предлагаемого процесса поиска и устранения ошибок.

Проблемы уровня 1 в канале доступа (этап 1)

Если физический интерфейс маршрутизатора, используемый для канала доступа, не находится в рабочем состоянии ("`up`" и "`up`", т.е. физический и канальный уровни работают), то маршрутизатор не может пересылать по каналу какие-либо фреймы. Если интерфейс имеет статус физического канала "выключен" ("`down`"), первый код состояния интерфейса, то у данного интерфейса, вероятнее всего, есть проблема уровня 1.

С точки зрения уровня 1 канал доступа Frame Relay представляет собой просто выделенную линию между маршрутизатором и коммутатором Frame Relay. По существу, точно такие же проблемы уровня 1 для данного канала полностью совпадают с проблемами двухточечного канала. Поскольку возможные основные причины и предлагаемые действия по устранению ошибок полностью отражают действия, которые следует выполнить на выделенной линии, читателю рекомендуется обратиться к соответствующему разделу главы 12 за дополнительной информацией об этом этапе.

Проблемы уровня 2 в канале доступа (этап 2)

Если состоянием канала физического интерфейса маршрутизатора является "включен" ("`up`"), а состоянием протокола линии (второй код состояния) — "выключен" ("`down`"), то в этом случае у линии обычно имеется проблема уровня 2 между маршрутизатором и локальным коммутатором Frame Relay. Для интерфейсов Frame Relay проблема обычно связана с командой `encapsulation` или с интерфейсом LMI протокола Frame Relay.

Наличие потенциальной проблемы, связанной с командой `encapsulation`, очень легко проверить. Если в конфигурации последовательного интерфейса маршрутизатора опущена подкоманда интерфейса `encapsulation frame-relay`, но физический канал доступа работает, то физический интерфейс устанавливается в состояние "включен/выключен" ("`up/down`"). Если конфигурация устройства недоступна, то для просмотра типа настроенной инкапсуляции может быть использована команда `show interfaces`; нужные сведения приведены в нескольких первых строках вывода команды.

Другая потенциальная проблема связана с интерфейсом LMI. Маршрутизатор (DTE) и коммутатор Frame Relay LMI (DCE) обмениваются сообщениями о состоянии в обоих направлениях для двух основных целей.

Общее описание двух главных функций LMI



- Чтобы устройства DCE могли сообщить устройствам DTE о каждом идентификаторе DLCI виртуального канала и его состоянии.
- Чтобы выполнить функцию тестовых сообщений, которая легко позволяет устройствам DCE и DTE сообщать о том, что канал доступа не может больше передавать данные.

Маршрутизатор переводит канал в состояние "up/down", когда он физически работает, однако устройство перестает получать сообщения интерфейса LMI от коммутатора. Если интерфейс не находится во включенном состоянии ("up/up"), то маршрутизатор не пытается передавать какие-либо пакеты с интерфейса, поэтому на этом этапе перестанут выполняться все команды `ping`.

Маршрутизатор может перестать получать сообщения интерфейса LMI от коммутатора как по вполне естественным причинам, так и вследствие ошибок. Обычной функцией тестовых пакетов является то, что в случае наличия реальных проблем в канале и невозможности передачи каких-либо данных маршрутизатор может обнаружить потерю тестовых сообщений и отключить канал. Такой механизм позволяет маршрутизатору использовать альтернативный маршрут, если таковой существует. Однако маршрутизатор может перестать получать сообщения LMI и отключить интерфейсы и вследствие описанных ниже ошибок.

- Интерфейс LMI в маршрутизаторе (с помощью команды физического интерфейса `no keepalive`) отключен; при этом он включен в коммутаторе (или наоборот).
- Разные типы LMI включены на маршрутизаторе (с помощью команды физического интерфейса `frame-relay lmi-type` *тип*) и на коммутаторе.

Как инкапсуляцию, так и интерфейс LMI можно легко проверить с помощью команды `show frame-relay lmi`. Она выводит данные только для маршрутизаторов, на которых указана команда `encapsulation frame-relay`, поэтому специалист может быстро убедиться, что команда `encapsulation frame-relay` настроена на правильных последовательных интерфейсах. Эта команда также выводит тип LMI, используемый маршрутизатором, и отображает счетчики сообщений, полученных и отправленных интерфейсом LMI. В примере 14.19 приведены данные от маршрутизатора R1, показанного на рис. 14.7.

Пример 14.19. Выполнение команды `show frame-relay lmi` на маршрутизаторе R1

```
R1# show frame-relay lmi
LMI Statistics for interface Serial0/0/0 (Frame Relay DTE) LMI TYPE =
ANSI
  Invalid Unnumbered info 0      Invalid Prot Disc 0
  Invalid dummy Call Ref 0       Invalid Msg Type 0
  Invalid Status Message 0       Invalid Lock Shift 0
```

```
Invalid Information ID 0      Invalid Report IE Len 0
Invalid Report Request 0      Invalid Keep IE Len 0
Num Status Enq. Sent 122      Num Status msgs Rcvd 34
Num Update Status Rcvd 0      Num Status Timeouts 88
Last Full Status Req 00:00:04 Last Full Status Rcvd 00:13:24
```

В данном примере маршрутизатор R1 был статически настроен с помощью команды интерфейса `frame-relay lmi-type ansi`, при этом коммутатор S1 по-прежнему использует тип `cisco` для интерфейса LMI. После изменения конфигурации LMI статистические данные покажут по 34 посланных и полученных сообщений о состоянии. (При работе эти значения будут расти с той же скоростью.) На настоящий момент маршрутизатор R1 послал 88 сообщений ANSI о состоянии, а в общей сложности послано 122 сообщения о состоянии. Количество полученных сообщений о состоянии все еще 34, поскольку маршрутизатор R1 больше не понимает посланные коммутатором сообщения LMI Cisco. Кроме того, маршрутизатор R1 ожидал сообщения о состоянии ANSI для последних 88 периодов состояния LMI, как отмечено в счетчике периодов состояния.

Если повторное использование команды `show frame-relay lmi` показывает, что количество полученных сообщений состояния остается тем же, то вероятной причиной, не связанной с неработающим каналом, может быть несоответствие типов интерфейсов LMI. Наилучшим решением является включение автоматического обнаружения типа интерфейса LMI в ходе конфигурирования подкоманды физического интерфейса `no frame-relay lmi-type` *тип* или в качестве альтернативы конфигурирования того же типа LMI, который используется коммутатором.

Если специалист занимается поиском и устранением ошибок, описанных на этапах 1 и 2, на всех подключенных маршрутизаторах Frame Relay, то все физические интерфейсы каналов доступа маршрутизаторов должны находиться в полностью рабочем состоянии (“`up/up`”). На последних четырех этапах исследуются проблемы, связанные с индивидуальными каналами PVC и с соседними устройствами в сети.

Проблемы и состояние каналов PVC (этап 3)

Целью данного этапа в процессе поиска и устранения ошибок является обнаружение идентификаторов DLCI каналов PVC, используемых для достижения конкретного соседнего устройства и последующего выяснения, работает ли данный канал PVC.

Чтобы определить правильный канал PVC, особенно если нет конфигурации или документации, придется вновь начать с выполнения команды `ping` для IP-адреса соседнего маршрутизатора в сети Frame Relay. Далее можно следовать такой логической последовательности.

Этап 3 **A.** Определите IP-адрес и маску для всех интерфейсов/субинтерфейсов Frame Relay (команды `show interfaces`, `show ip interface brief`), а также напрямую подключенные подсети.

B. Сравните IP-адрес неудачной команды `ping` и адрес на интерфейсе или субинтерфейсе.

C. Определите канал (каналы) PVC, назначенный этому интерфейсу или субинтерфейсу (команда `show frame-relay pvc`).

D. Если этому интерфейсу или субинтерфейсу назначено более одного канала PVC, определите, какой канал PVC используется для достижения конкретного соседнего устройства (команда `show frame-relay map`)

ВНИМАНИЕ!

Списки, подобные этому, предназначены для удобства изучения темы при чтении главы. При изучении и необходимости вспомнить конкретную часть, относящуюся к решению поставленной проблемы, легко найти и использовать формализованный список. Нет необходимости заучивать этот список или тренироваться в его использовании до того, как вы усвоите всю информацию о рассматриваемой технологии.

На этапах 3 A–D определяется канал PVC, который следует проверить. После его определения на этапе 3 в предлагаемом процессе поиска ошибок интерпретируется состояние этого канала PVC и связанного с ним интерфейса или субинтерфейса для определения причины каких-либо проблем.

В данном разделе более подробно рассматривается пример, где на маршрутизаторе R1 команда `ping` для IP-адреса 10.1.2.2 протокола Frame Relay возвращает отрицательный результат. Перед тем как сосредоточить внимание на определении используемого виртуального канала, полезно узнать окончательный ответ, поэтому на рис. 14.8 приведены некоторые подробности. Например, команда `ping 10.1.2.2` маршрутизатора R1 в данном случае не срабатывает.

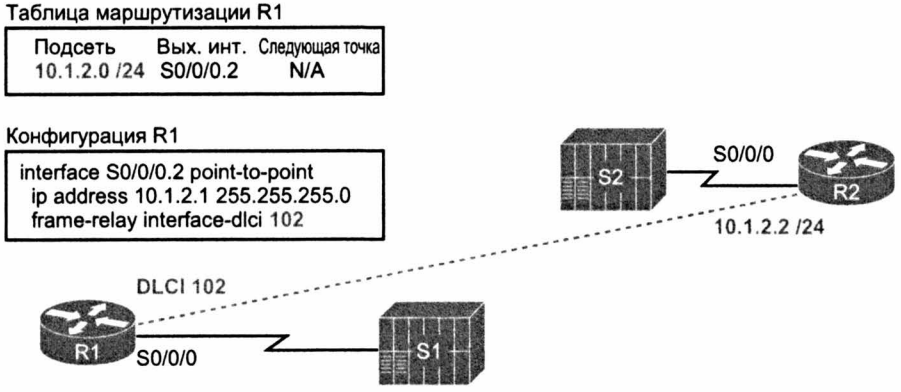


Рис. 14.8. Сведения о конфигурации, относящиеся к неудачной команде `ping 10.1.2.2` маршрутизатора R1

Поиск подключенной подсети и выходного интерфейса (этапы 3 A и B)

Два первых промежуточных этапа для определения канала PVC (DLCI), соединяющего маршрутизатор R1 с маршрутизатором R2 (промежуточные этапы 3 A и B должны быть относительно простыми, учитывая то, что читатель уже прочитал части II и III данной книги). Каждый раз при выполнении команды `ping` для IP-адреса протокола Frame Relay соседнего маршрутизатора этот IP-адрес должен находиться в одной из подсетей, также подключенных к этому локальному маршрутизатору. Для определения интерфейса, используемого в локальном маршрутизато-

ре при пересылке пакетов дистанционному маршрутизатору, нужно просто найти такую совместно используемую подключенную подсеть.

В примере 14.20 показано выполнение на маршрутизаторе R1 команды `ping` для адреса 10.1.2.2. В нем представлено несколько команд, подтверждающих, что субинтерфейс S0/0/0.2 маршрутизатора R1 подключен к подсети 10.1.2.0/24, которая включает в себя IP-адрес 10.1.2.2 маршрутизатора R2.

Пример 14.20. Поиск подсети 10.1.2.0/24 и субинтерфейса S0/0/0.2

```
R1> show ip interface brief
Interface        IP-Address  OK? Method Status Protocol
FastEthernet0/0 10.1.11.1    YES NVRAM    up    up
FastEthernet0/1 unassigned   YES NVRAM administratively down down
Serial0/0/0      unassigned  YES NVRAM    up    up
Serial0/0/0.2    10.1.2.1    YES NVRAM   down   down
Serial0/0/0.5    10.1.5.1    YES manual  down   down
Serial0/0/0.34   10.1.34.1   YES NVRAM    up     up
R1# show interfaces s 0/0/0.2
Serial0/0/0.2 is down, line protocol is down
  Hardware is GT96K Serial
  Internet address is 10.1.2.1/24
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation FRAME-RELAY
  Last clearing of "show interface" counters never
```

Поиск каналов PVC, назначенных данному интерфейсу (этап 3 С)

Команда `show frame-relay pvc` непосредственно отвечает на вопрос о том, какие каналы PVC были назначены указанным интерфейсам и субинтерфейсам. Если эта команда выполняется без параметров, то она выводит около десяти строк для каждого виртуального канала, при этом в конце первой строки выводится связанный с ним интерфейс или субинтерфейс. В примере 14.21 приведена часть вывода этой команды.

Пример 14.21. Установление связи между субинтерфейсом S0/0/0.2 и каналом PVC, имеющим идентификатор DLCI, равный 102

```
R1> show frame-relay pvc

PVC Statistics for interface Serial0/0/0 (Frame Relay DTE)

             Active   Inactive  Deleted   Static
Local         1          2         0         0
Switched      0          0         0         0
Unused        0          0         0         0

DLCI = 102, DLCI USAGE = LOCAL, PVC STATUS = INACTIVE, INTERFACE = Seri-
al0/0/0.2

input pkts 33        output pkts      338 in bytes 1952
out bytes 29018      dropped pkts     0 in pkts dropped 0
      out pkts dropped 0        out bytes dropped 0
in FECN pkts 0 in    BECN pkts 0       out FECN pkts 0
```

```
out BECN pkts 0 in  DE pkts 0          out DE pkts 0
out bcast pkts 332  out bcast bytes 28614
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
pvc create time 00:30:05, last time pvc status changed 00:04:14

DLCI = 103, DLCI USAGE = LOCAL, PVC STATUS = INACTIVE,
INTERFACE = Serial0/0/0.34

input pkts 17          output pkts 24  in bytes 1106
out bytes 2086 dropped pkts 0          in pkts dropped 0
      out pkts dropped 0          out bytes dropped 0
in FECN pkts 0         in BECN pkts 0  out FECN pkts 0
out BECN pkts 0        in DE pkts 0    out DE pkts 0
out bcast pkts 11      out bcast bytes 674
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
pvc create time 00:30:07, last time pvc status changed 00:02:57

DLCI = 104, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE,
INTERFACE = Serial0/0/0.34

input pkts 41          output pkts 42  in bytes 2466
out bytes 3017         dropped pkts 0  in pkts dropped 0
       out pkts dropped 0          out bytes dropped 0
in FECN pkts 0         in BECN pkts 0  out FECN pkts 0
out BECN pkts 0        in DE pkts 0    out DE pkts 0
out bcast pkts 30      out bcast bytes 1929
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
pvc create time 00:30:07, last time pvc status changed 00:26:17
```

Для определения всех каналов PVC, связанных с интерфейсом или субинтерфейсом, нужно лишь просмотреть выделенные фрагменты вывода команды в примере 14.21. В данном случае для интерфейса S0/0/0.2 приведен лишь один канал PVC, имеющий идентификатор DLCI 102, поэтому с интерфейсом S0/0/0.2 связан только один канал PVC.

Определение канала PVC, используемого для достижения конкретного соседнего устройства (этап 3 D)

Если в конфигурации маршрутизатора с интерфейсом или субинтерфейсом связано несколько каналов PVC, то на следующем этапе необходимо определить, какой из каналов PVC применяется для отправки трафика конкретному соседнему устройству. В примере 14.21 показан маршрутизатор R1, который использует многоточечный субинтерфейс S0/0/0.34 с идентификаторами DLCI 103 и 104, при этом идентификатор DLCI 103 применяется для канала PVC к маршрутизатору R3, а идентификатор DLCI 104 — для канала PVC, осуществляющего соединение с маршрутизатором R4. Поэтому если вы решаете проблему, в которой команда `ping 10.1.34.3` не сработала на маршрутизаторе R1, то следующим этапом является определение того, какой из двух идентификаторов DLCI (103 или 104) идентифицирует виртуальный канал, соединяющий маршрутизатор R1 с маршрутизатором R3. К сожалению, не всегда можно найти ответ на этот вопрос, не обращаясь к дополнительной документации. Един-

ственной командой show, которая может помочь, является команда show frame-relay map, которая может установить связь между IP-адресом следующего перехода и идентификатором DLCI. Но если локальный маршрутизатор использует протокол Inverse ARP, то он (маршрутизатор) также не может сразу узнать информацию сопоставления, поэтому таблица сопоставлений может не содержать полезной информации. Но если используется статическое сопоставление, то правильный PVC/DLCI может быть идентифицирован.

В примере не сработавшей для маршрутизатора R1 команды ping для адреса 10.1.2.2 (маршрутизатор R2), в связи с тем, что канал PVC связан только с необходимым интерфейсом (S0/0/0.2), канал PVC уже был идентифицирован, поэтому данный этап можно пропустить.

Состояние канала PVC

В данный момент на этапе 3 поиска ошибок были определены правильный интерфейс/субинтерфейс и правильные значения PVC/DLCI. В заключение можно было исследовать состояние канала PVC, чтобы узнать, есть ли проблема в самом канале PVC.

Маршрутизаторы используют четыре различных кода состояния виртуального канала. Устройство узнает о двух возможных кодах состояния — *активного* или *неактивного* (active и inactive) — с помощью сообщений интерфейса LMI от коммутатора Frame Relay. В сообщении LMI коммутатора приводятся коды DLCI для всех настроенных каналов PVC в канале доступа и сообщается, можно ли в настоящий момент использовать данный канал PVC (активен) или нельзя (неактивен). Сообщение LMI, выводящее эти состояния, означает следующее.

Активен (active). Сети Frame Relay известен канал PVC с соответствующим идентификатором DLCI. Канал PVC сейчас работает правильно

Неактивен (inactive). Сети Frame Relay известен канал PVC с соответствующим идентификатором DLCI. Канал PVC сейчас не работает.

У маршрутизаторов есть еще два состояния канала PVC, требующих немного больше объяснений. Первое состояние называется *статическим* (static) и означает, что на маршрутизаторе настроен идентификатор DLCI для некоего канала PVC, но сообщения LMI отключены. Поскольку сообщения LMI отключены, маршрутизатор не знает, будет ли канал PVC работать, ведь он не получает сообщений LMI о состоянии. Однако маршрутизатор может, по крайней мере, посылать фреймы, используя эти идентификаторы DLCI, и надеяться, что сеть Frame Relay сможет доставить их.

Другое состояние канала PVC, *удаленный* (deleted), означает, что конфигурация маршрутизатора ссылается на идентификатор DLCI, при этом сообщения LMI работают, но не выводят информацию об этом идентификаторе DLCI. Сообщения LMI о состоянии выводят состояние для всех каналов PVC, определенных на канале доступа, поэтому данное состояние означает, что у сети Frame Relay нет определения для канала PVC. Проще говоря, это состояние означает, что на маршрутизаторе идентификатор DLCI настроен, а на коммутаторе — нет.

В табл. 14.2 обобщена информация о четырех кодах состояния каналов PVC в протоколе Frame Relay.

Таблица 14.2. Состояния постоянных виртуальных каналов

Ключевая тема

Состояние	Активный	Неактивный	Удален	Статический
Постоянный виртуальный канал определен в сети Frame Relay	Да	Да	Нет	Неизвестно
Маршрутизатор попытается переслать фреймы через такой канал	Да	Нет	Нет	Да

Как указано в последней строке таблицы, маршрутизаторы пересылают данные по каналам PVC только в активном или статическом состоянии. Кроме того, даже если канал PVC находится в статическом состоянии, нет гарантии, что сеть Frame Relay действительно может пересылать фреймы по этому каналу, поскольку статическое состояние предполагает, что интерфейс LMI отключен и маршрутизатор не получил какой-либо информации о состоянии.

Следующим этапом в процессе поиска ошибок является определение состояния канала PVC, используемого для достижения конкретного соседнего устройства. Продолжая рассмотрение проблемы, возникшей при неудачной попытке выполнить команду `ping` на маршрутизаторе R1 (по адресу 10.1.2.2), в примере 14.22 представлено состояние канала PVC с идентификатором DLCI 102, обнаруженным ранее.

Пример 14.22. Команда `show frame-relay pvc`, выполняемая на маршрутизаторе R1

```
R1> show frame-rellay pvc 102

PVC Statistics for interface Serial0/0/0 (Frame Relay DTE)

DLCI = 102, DLCI USAGE = LOCAL, PVC STATUS = INACTIVE,
INTERFACE = Serial0/0/0.2

input pkts 22          output pkts 193    in bytes 1256
out bytes 16436        dropped pkts 0     in pkts dropped 0
out pkts dropped 0           out bytes dropped 0
in FECN pkts 0         in BECN pkts 0     out FECN pkts 0
out BECN pkts 0        in DE pkts 0       out DE pkts 0
out bcast pkts 187     out bcast bytes 16032
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
pvc create time 01:12:56, last time pvc status changed 00:22:45
```

В данном случае маршрутизатор R1 не может выполнить команду `ping` к маршрутизатору R2, поскольку канал PVC с идентификатором DLCI 102 находится в неактивном состоянии.

Для дальнейшей локализации проблемы и определения ее главной причины необходимо глубже изучить причины, по которым канал PVC может быть неактивным. Как обычно, повторим те же этапы поиска ошибок на другом маршрутизаторе, в данном случае — на маршрутизаторе R2. Если на маршрутизаторе R2 не было выявлено других проблем, кроме неактивного канала PVC, то проблема может в действительности быть связана с сетью провайдера Frame Relay, поэтому следующим этапом может быть обращение к провайдеру. Однако возможны и другие проблемы, связанные с удаленным маршрутизатором. Например, для (искусственного) создания проблемы

и иллюстрации команд show в данном разделе канал доступа маршрутизатора R2 был отключен, однако при быстром выполнении этапа 1 на маршрутизаторе R2 возникшая проблема была бы обнаружена. Если же дальнейший поиск ошибок показывает, что оба маршрутизатора свидетельствуют о том, что оба конца канала PVC находятся в неактивном состоянии, то основная причина проблемы может быть связана с сетью провайдера Frame Relay.

Поиск причины проблем, связанных с каналом PVC в удаленном состоянии, относительно прост. Состояние "удален" может означать, что конфигурация коммутатора Frame Relay и конфигурация маршрутизатора не соответствуют друг другу. В маршрутизаторе настроен идентификатор DLCI, который на коммутаторе не задан. В этом случае либо провайдер сообщил, что канал PVC будет настроен с данным конкретным идентификатором DLCI, но не сделал этого, либо отвечающий за маршрутизатор инженер указал неправильное значение DLCI.

Состояние субинтерфейса

Субинтерфейсы, как и физические интерфейсы, имеют код состояния канала и код состояния протокола. Однако, поскольку субинтерфейсы являются виртуальными, коды состояния и их значения несколько отличаются от значений для физических интерфейсов. В данном разделе кратко анализируются работа субинтерфейсов Frame Relay и то, каким образом операционная система Cisco IOS решает, будет ли субинтерфейс Frame Relay находиться в полностью рабочем состоянии ("up/up") или в нерабочем состоянии ("down/down").

Конфигурация протокола Frame Relay связывает с субинтерфейсом один или более идентификатор DLCI с помощью команд frame-relay interface-dlci и frame-relay map. При работе со всеми идентификаторами DLCI, связанными с данным субинтерфейсом, операционная система IOS использует приведенные ниже правила для определения состояния субинтерфейса.

Ключевая тема

Причины, по которым субинтерфейсы находятся в состоянии "up/up" или "down/down"

- down/down. Все идентификаторы DLCI, связанные с данным субинтерфейсом, являются неактивными или удаленными, т.е. соответствующий физический интерфейс не находится в состоянии "up/up".
- up/up. По меньшей мере один из идентификаторов DLCI, связанных с данным субинтерфейсом, находится в активном или статическом состоянии.

Например, для создания проблем, показанных в примере 14.22, на маршрутизаторах R2 и R3 просто отключены их каналы доступа Frame Relay. На рис. 14.9 представлено следующее сообщение состояния интерфейса LMI, которое коммутатор S1 посылает маршрутизатору R1.

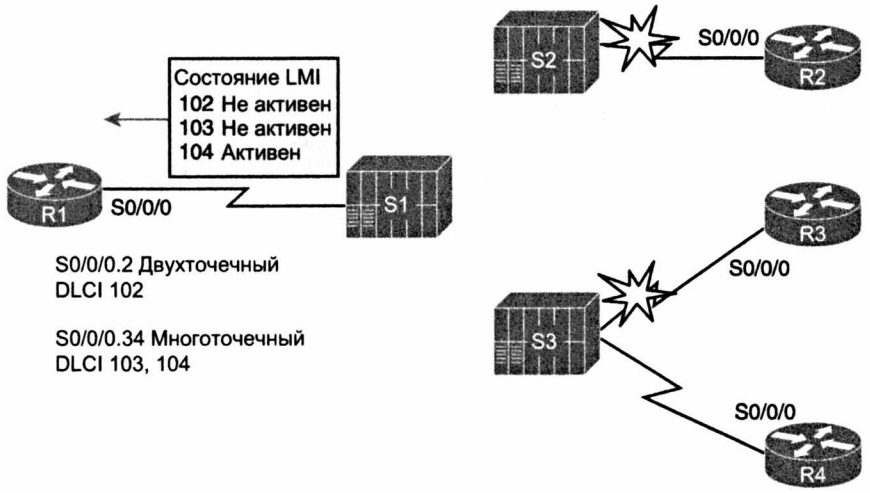


Рис. 14.9. Результат отключения каналов доступа маршрутизаторов R2 и R3

Как показано на данном рисунке, маршрутизатор R1 использует двухточечный субинтерфейс (S0/0/0.2) для виртуального канала, подключенного к маршрутизатору R2, а многоточечный субинтерфейс (S0/0/0.34), связанный с этими виртуальными каналами, — для подключения к маршрутизаторам R3 и R4 (103 и 104 соответственно). В начале примера 14.20 показано, что интерфейс S0/0/0.2 находится в состоянии "`down/down`". Это объясняется тем, что субинтерфейс (102) не активен. Однако интерфейс S0/0/0.34 имеет два идентификатора DLCI, один из которых является активным, поэтому операционная система IOS оставляет интерфейс S0/0/0.34 в состоянии "`up/up`".

При поиске и устранении неисправностей полезно следить за состоянием субинтерфейса, однако следует учитывать, что, поскольку субинтерфейс включен (`up`), если он является многоточечным субинтерфейсом, состояние "`up/up`" не обязательно означает, что все идентификаторы DLCI, связанные с данным субинтерфейсом, находятся в рабочем состоянии.

Проблемы сопоставления адресов в протоколе Frame Relay (этап 4)

Предположим, что первые три этапа предложенного в данной главе процесса поиска и устранения неисправностей пройдены, и проблемы, возникающие на каждом этапе, разрешены. Теперь интерфейсы каналов доступа каждого маршрутизатора должны быть в полностью рабочем состоянии "`up/up`", а все каналы PVC между каждыми двумя маршрутизаторами должны быть в активном (или статическом) состоянии. Если в маршрутизаторах по-прежнему нельзя успешно выполнить команду `ping` для адресов друг друга, то следующим действием является проверка информации сопоставления адресов, устанавливающей соответствие идентификаторов DLCI IP-адресам следующего транзитного перехода.

В данном разделе не повторяется подробное изложение механизма сопоставления адресов, приведенное в настоящей главе и в главе 15. Однако ниже даны некоторые советы и рекомендации в качестве напоминания при выполнении данного этапа поиска неисправностей.

Следует помнить, что для двухточечных субинтерфейсов характерны следующие особенности.

Ключевая тема

Информация о преобразовании адресов, отображаемая в двухточечных субинтерфейсах

- Эти субинтерфейсы не нуждаются в протоколе Inverse ARP или статическом сопоставлении.
- Операционная система IOS автоматически сопоставляет любые другие IP-адреса в той же подсети, что и двухточечный субинтерфейс, как доступные через единственный идентификатор DLCI на субинтерфейсе.
- Команда `show frame-relay map` выводит двухточечные субинтерфейсы, но без IP-адресов следующей транзитной точки перехода и отметки "dynamic" (означающей, что сопоставление изучено по протоколу InARP).

Для физических и многоточечных интерфейсов характерны перечисленные ниже особенности.

Ключевая тема

Информация о сопоставлении адресов, отображаемая в многоточечных субинтерфейсах

- Необходимо использовать протокол Inverse ARP или статическое преобразование.
- В команде `show frame-relay map` должны быть показаны IP-адреса дистанционного маршрутизатора Frame Relay и локальные идентификаторы DLCI для каждого канала PVC, связанного с данным интерфейсом или субинтерфейсом. Пометка "`dynamic`" означает, что сопоставление было изучено по протоколу InARP.
- При использовании статического сопоставления необходимо использовать ключевое слово `broadcast` для обеспечения работы протоколов маршрутизации.

Для полноты картины в примере 14.23 приведен вывод команды `show frame-relay map` для маршрутизатора R1, показанного на рис. 14.7, у которого нет проблем с преобразованием адресов (предполагается, что ранее выявленные проблемы были устранены). В данном случае интерфейс S0/0/0.2 является двухточечным субинтерфейсом, а интерфейс S0/0/0.34 — многоточечным интерфейсом, в котором есть полученное из протокола Inverse ARP сопоставление и одно сопоставление, настроенное статически.

Пример 14.23. Выполнение команды `show frame-relay map` в маршрутизаторе R1

```
R1# show frame-relay map
Serial0/0/0.34 (up): ip 10.1.34.4 dlci 104(0x68,0x1880), static,
            broadcast,
            CISCO, status defined, active
Serial0/0/0.34 (up): ip 10.1.34.3 dlci 103(0x67,0x1870), dynamic,
            broadcast,, status defined, active
Serial0/0/0.2 (up): point-to-point dlci, dlci 102(0x66,0x1860), broadcast
            status defined, active
```

Сквозная инкапсуляция (этап 5)

Понятие сквозной инкапсуляции на каналах PVC относится к заголовку протокола Frame Relay с двумя опциональными возможностями: собственный заголовок Cisco и стандартный заголовок IETF. Подробности конфигурирования были описаны ранее в данной главе, в разделе "Настройка инкапсуляции и типа LMI".

Оказывается, что несовпадающие установки типов инкапсуляции на маршрутизаторах, расположенных на обоих концах канала, могут вызвать проблему в одном конкретном случае. Если одним из маршрутизаторов является маршрутизатор Cisco, использующий инкапсуляцию Cisco, а другой маршрутизатор не является маршрутизатором Cisco и использует инкапсуляцию IETF, то команды `ping` могут не выполняться из-за несоответствия типов инкапсуляции. Однако два маршрутизатора Cisco понимают оба типа инкапсуляции, поэтому такая настройка не может вызвать проблем в сетях, в которых работают только устройства компании Cisco.

Несовпадение номеров подсетей (этап 6)

Если проблемы, обнаруженные на первых шести этапах поиска и устранения неисправностей, были разрешены, то на данном этапе в протоколе Frame Relay больше не должно быть ошибок. Однако если для двух маршрутизаторов на каком-либо канале PVC оказались ошибочно настроенными IP-адреса в различных подсетях, то маршрутизаторы не смогут обмениваться пакетами команды `ping` друг с другом и протоколы маршрутизации не установят отношения смежности (adjacent). Поэтому в качестве последнего этапа специалист должен проверить на каждом маршрутизаторе IP-адреса и маски и убедиться в том, что они подключены к той же подсети. Для этого следует выполнить команды `show ip interface brief` и `show interfaces` на этих двух маршрутизаторах.

Обзор

Резюме

- При планировании конфигурации Frame Relay определите, для каких физических площадок необходимо установить каналы доступа Frame Relay, определите частоту синхронизации (физическую скорость доступа), используемую на каждом канале связи, определите каждый виртуальный канал за счет идентификации конечных точек и согласованную скорость CIR для каждого канала и согласуйте тип интерфейса LMI (обычно задаваемого провайдером).
- Протокол Inverse ARP динамически создает сопоставление адреса уровня 3 (например, IP-адреса) с адресом уровня 2 (локальный идентификатор DLCI).
- Используя протокол Inverse ARP, маршрутизатор создает сопоставление адреса уровня 3 соседнего маршрутизатора с соответствующим адресом уровня 2.
- Информацию сопоставления можно задать и статически, не используя протокол Inverse ARP.
- Термин "многоточечный интерфейс" означает, что имеется более одного виртуального канала, благодаря чему отправлять и получать пакеты на субинтерфейсе можно более чем с одного виртуального канала.
- Использующие протокол OSPF маршрутизаторы не становятся соседями по физическому интерфейсу Frame Relay или многоточечному субинтерфейсу без дополнительной настройки, которая не затрагивается на экзамене CCNA.

Контрольные вопросы

Ответьте на эти вопросы. Ответы можно найти на последней странице главы. Полное объяснение ответов приведено в приложении B на веб-сайте.

1. Предположим, два маршрутизатора Cisco, R1 и R2, соединены через среду Frame Relay. Маршрутизатор R1 подсоединяется к коммутатору, который использует интерфейс LMI типа ANSI T1.617, а маршрутизатор R2 подсоединяется к коммутатору, который использует интерфейс ITU Q.933a. Какие ключевые слова могли бы использоваться в конфигурациях маршрутизаторов R1 и R2 для того, чтобы интерфейсы LMI работали без ошибок?

   А) `ansi` и `itu`.

   Б) `T1617` и `q933a`.

   В) `ansi` и `q933a`.

   Г) `T1617` и `itu`.

   Д) Маршрутизаторы не будут работать с двумя различными типами интерфейсов.

2. Сеть компании BettyCo состоит из пяти хостов, при этом все маршрутизаторы подсоединены к одной и той же сети Frame Relay. Виртуальные каналы (VC) были заданы для каждой пары маршрутизаторов. Господин Бетти (Betty), президент компании, сказал, что уволит любого, кто настроит что-то, что проще

было бы оставить со стандартными настройками. Какая из приведенных ниже команд конфигурирования, выполненная для данной сети Frame Relay, приведет к увольнению инженера? (Выберите три ответа.)

А) `ip address`.

Б) `encapsulation`.

В) `lmi-type`.

Г) `frame-relay map`.

Д) `frame-relay inverse-arp`.

3. Несколько маршрутизаторов компании подсоединены к сети Frame Relay. Маршрутизатор R1 расположен на дистанционной площадке сети и имеет лишь один виртуальный канал к штаб-квартире компании. В настоящее время конфигурация маршрутизатора R1 выглядит следующим образом.

```
interface serial 0/0
ip address 10.1.1.1 255.255.255.0
encapsulation frame-relay
```

Госпожа Вилма (Wilma), президент компании, слышала о том, что двухточечные субинтерфейсы превосходно работают, и хочет изменить конфигурацию так, чтобы использовался двухточечный субинтерфейс. Какую из приведенных ниже команд необходимо использовать для перехода к такой конфигурации? (Выберите два ответа.)

А) `no ip address`.

Б) `interface-dlci`.

В) `no encapsulation`.

Г) `encapsulation frame-relay`.

Д) `frame-relay interface-dlci`.

4. У компании есть другая сеть, в которой главный маршрутизатор имеет десять виртуальных каналов (VC), подсоединенных к десяти дистанционным площадкам. Теперь у президента компании сложилось мнение, что многоточечные субинтерфейсы эффективнее двухточечных. В настоящее время конфигурация главного маршрутизатора выглядит следующим образом.

```
interface serial 0/0
 ip address 172.16.1.1 255.255.255.0
 encapsulation frame-relay
```

Госпожа Вилма хочет, чтобы вы изменили конфигурацию для использования многоточечного субинтерфейса. Какую из приведенных ниже команд нужно использовать для перехода к этой конфигурации? (**Примечание**. Идентификаторы DLCI 101-110 используются для десяти виртуальных каналов.)

А) `interface-dlci 101 110`.

Б) `interface dlci 101-110`.

В) Десять различных команд `interface-dlci`.

Г) `frame-relay interface-dlci 101 110`.

Д) `frame-relay interface dlci 101-110`.

Е) Десять различных команд `frame-relay interface-dlci`.

5. Какая из приведенных ниже команд выводит информацию, полученную протоколом Inverse ARP (обратный ARP)?

   А) `show ip arp`.

   Б) `show arp`.

   В) `show inverse arp`.

   Г) `show frame-relay inverse-arp`.

   Д) `show map`.

   Е) `show frame-relay map`.

6. Какие из приведенных ниже ключевых слов являются кодами состояния канала PVC Frame Relay, для которых маршрутизатор посылает фреймы по связанным с ним каналам PVC?

   А) Up (включен).

   Б) Down (выключен).

   В) Active (активен).

   Г) Inactive (неактивен).

   Д) Static (статический).

   Е) Deleted (удален).

7. Маршрутизатор RC центральной площадки имеет виртуальный канал, подключенный к десяти дистанционным маршрутизаторам (R1–R10) с локальными идентификаторами DLCI с номерами 101–110 соответственно. В маршрутизаторе RC идентификаторы 107–109 сгруппированы в один многоточечный субинтерфейс S0/0.789, текущим состоянием которого является "`up`" и "`up`" (корректно работает на уровнях 1 и 2). Какое из приведенных ниже утверждений верно? (Выберите два ответа.)

   А) Последовательный интерфейс Serial 0/0 может быть в состоянии "`up/down`" (уровень 1 работает, уровень 2 — нет).

   Б) Виртуальный канал PVC с идентификатором DLCI 108 может быть в неактивном состоянии.

   В) Команда `show frame-relay map` выводит информацию о привязке адресов для этих трех виртуальных каналов.

   Г) Как минимум один из данных трех каналов PVC находится в активном или статическом состоянии.

8. Маршрутизатор R1 в сети Frame Relay подключен к каналу доступа по интерфейсу S0/0. Физический интерфейс находится в состоянии "`up/down`". Какова причина этой проблемы? (Выберите два ответа.)

   А) В канале доступа есть физическая проблема, и он не может пересылать биты между маршрутизатором и коммутатором.

   Б) Коммутатор и маршрутизатор используют различные типы интерфейса LMI.

   В) В конфигурации маршрутизатора отсутствует команда `encapsulation frame-relay` для интерфейса S0/0.

   Г) Маршрутизатор получил сообщения состояния интерфейса LMI, в которых указано, что некоторые идентификаторы DLCI являются неактивными.

Ключевые темы

Повторите все ключевые темы данной главы, отмеченные пиктограммой "Ключевая тема". Ключевые темы и соответствующие им страницы перечислены в табл. 14.3.

Таблица 14.3. Ключевые темы главы 14

Элемент	Описание	Страница
Список	Последовательность настройки протокола Frame Relay	462
Определение	Основные понятия и определения сопоставления адресов протокола Frame Relay	467
Рис. 14.4	Принцип работы протокола Inverse ARP	470
Список	Процесс поиска и устранения ошибок протокола Frame Relay, включающий в себя шесть этапов	481
Список	Общее описание двух главных функций LMI	483
Табл. 14.2	Состояния постоянных виртуальных каналов	489
Список	Причины, по которым субинтерфейсы находятся в состоянии "up/up" или "down/down"	490
Список	Информация о преобразовании адресов, отображаемая в двухточечных субинтерфейсах	492
Список	Информация о сопоставлении адресов, отображаемая в многоточечных субинтерфейсах	492

Заполните таблицы и списки по памяти

Распечатайте приложение Г с веб-сайта или его раздел, относящийся к этой главе, и заполните таблицы и списки по памяти. В приложении Д приведены заполненные таблицы и списки для самоконтроля.

Таблицы команд

Хоть и не обязательно заучивать информацию из таблиц данного раздела, ниже приведен список команд конфигурации и пользовательских команд главы. Фактически команды стоит запомнить, чтобы лучше понять содержимое главы и выполнить задания по подготовке к экзамену. Чтобы проверить, насколько хорошо вы запомнили команды, закройте левую сторону таблицы листом бумаги, читайте описания с правой стороны и пытайтесь вспомнить команду.

Таблица 14.4. Конфигурационные команды главы 14

Команда	Описание
`encapsulation frame-relay [ietf]`	Команда режима конфигурирования интерфейса, задающая тип инкапсуляции Frame Relay в отличие от HDLC, PPP и т.д.
`frame-relay lmi-type {ansi | q933a | cisco}`	Команда режима конфигурирования интерфейса, которая определяет тип сообщений интерфейса LMI, посылаемых коммутатору

Окончание табл. 14.4

Команда	Описание
`no frame-relay lmi-type`	Команда режима конфигурации интерфейса, возвращающая интерфейс к стандартным параметрам LMI для автоматического считывания типа LMI
`bandwidth` *число*	Подкоманда интерфейса, устанавливающая воспринимаемую маршрутизатором скорость интерфейса
`frame-relay map {`*протокол протокольный-адрес идентификатор-dlci*`}[broadcast] [ietf | cisco]`	Команда режима конфигурирования интерфейса, статически определяющая преобразование между адресом сетевого уровня и идентификатором DLCI
`frame-relay interface-dlci` *dlci* `[ietf | cisco]`	Команда режима конфигурации субинтерфейса, связывающая DLCI с субинтерфейсом
`keepalive` *сек*	Команда режима конфигурирования интерфейса, статически определяющая отправку и ожидание сообщений запросов состояния интерфейса LMI и их частоту
`interface serial` *номер_субинтерфейса* `[point-to-point | point-to-multipoint]`	Глобальная команда конфигурации, создающая субинтерфейс или ссылающаяся на ранее созданный субинтерфейс
`[no] frame-relay inverse-arp`	Физическая и многоточечная подкоманда, включающая или отключающая (команда `no inverse-arp`) протокол Inverse ARP Frame Relay

Таблица 14.5. Команды EXEC главы 14

Команда	Описание
`show interfaces [`*тип номер*`]`	Отображает состояние физического интерфейса
`show frame-relay pvc [interface` *интерфейс*`] [`*идентификатор-dlci*`]`	Выводит информацию о состоянии канала PVC
`show frame-relay lmi [`*тип номер*`]`	Выводит информацию о состоянии интерфейса LMI
`show frame-relay map [`*тип номер*`]`	Выводит информацию сопоставления Frame Relay, соответствующую IP-адресу следующей транзитной точки перехода к локальному DLCI
`show interfaces [`*тип номер*`]`	Выводит статистику и подробности конфигурации интерфейса, включая тип инкапсуляции
`show ip interface brief`	Выводит по одной строке вывода на интерфейс, включая состояние интерфейса и IP-адрес
`debug frame-relay lmi`	Отображает содержание сообщений интерфейса LMI

Ответы на контрольные вопросы:

1 В. 2 В, Г, и Д. 3 А и Д. 4 Е. 5 Е. 6 В. 7 Б и Г. 8 Б и В.

Глава 15

Другие типы глобальных сетей

В большинстве глав этой книги сначала следует вводная часть, а затем более подробное рассмотрение темы, поскольку экзамен требует глубоких знаний. В отличие от большинства других глав, данная глава кратко знакомит с каждой темой, а затем переходит к следующей, поскольку читатели должны ознакомиться с общими концепциями множества других протоколов WAN.

Только чтобы придать технологиям некий контекст, эта глава разделена на два главных раздела. В первом рассматриваются технологии WAN, обычно применяемые для создания частных служб WAN, как правило, для предприятий. Второй раздел посвящен технологиям WAN, используемым для доступа к Интернету предприятиями или отдельными потребителями.

В этой главе рассматриваются следующие экзаменационные темы
Технологии WAN
Различные технологии WAN
Metro Ethernet
VSAT
Сотовый 3G / 4G
MPLS
T1/E1
ISDN
DSL
Кабель
Реализация и устранение проблем PPPoE

Основные темы

Частные глобальные сети, соединяющие предприятия

Службы WAN обычно используются для создания либо частной, либо открытой службы WAN. В частной службе один клиент подключается к провайдеру служб WAN, соединенному со многими площадками. Провайдер обеспечивает перенаправление данных между этими площадками. Позже, когда к той же службе WAN подключится второй клиент, служба WAN обеспечивает приватность данных трафика двух клиентов. Хотя данные могут передаваться через те же устройства в сети провайдера, провайдер никогда не перенаправляют данные, посланные клиентом 1 клиенту 2, и наоборот, что делает сеть частной с точки зрения клиента.

Соединение с Интернетом, напротив, полагается на тот факт, что каждый клиент *провайдера служб Интернета* (Internet Service Provider — ISP) вполне может передавать и получать пакеты от других клиентов. Добавление соединения с Интернетом через провайдера ISP объявляет о готовности посылать и получать пакеты по этому соединению. Чтобы защитить это соединение, следует обратить внимание на защиту, позволив передавать по каналам доступа к Интернету только допустимые виды трафика.

Большую часть технологий WAN, упомянутых в этой главе, можно использовать для построения и частных глобальных сетей, и открытых сетей Интернета. Но некоторые технологии лучшее подходят в одном месте, а другие в другом, поэтому в данной главе каждая технология WAN обсуждается по месту их наиболее вероятного использования.

Первый раздел главы посвящен следующим технологиям частных служб WAN.

- Выделенные линии.
- Технология Frame Relay.
- Глобальные сети Ethernet.
- MPLS.
- VSAT.

Выделенные линии

Из всех тем по глобальным сетям, упомянутых в этой книге, основное внимание уделяется выделенным линиям и линиям Frame Relay. В главе 12 уже обсуждались выделенные линии и связанные с ними наиболее популярные протоколы канала связи, но не очень подробно. Почему о них упоминается в этой главе? Чтобы подготовить почву для сравнения с другими технологиями WAN, описанными в этой главе.

Экзамен ICND2 (и CCNA) требует быть готовым идентифицировать разные технологии WAN. Так как же выявить выделенные линии, встретив их на экзамене? Рассмотрим следующий список.

- Выделенные линии имеют много названий (см. табл. 12.2 в главе 12).
- На рисунках выделенные линии обычно изображают зигзагообразной линией, похожей на молнию. На других рисунках, более похожих на рис. 15.1,

демонстрируют модуль обслуживания канала и данных (CSU/DSU), необходимый для каждого маршрутизатора; обратите внимание, на рисунке приведен внешний модуль CSU/DSU.

- Другими словами, для создания канала используется такая технология, как T-канал или мультиплексирование с разделением времени (TDM). По скоростям передачи каналы бывают DS1, T1, E1, T3 и E3.
- Что касается протоколов, то выделенные линии предоставляют службы уровня 1, в которых провайдер обещает доставлять биты на другой конец канала. Провайдер служб позволяет клиенту использовать любой канал связи и протоколы более высокого уровня, которые клиент хочет использовать.

На рис. 15.1 приведена типичная схема выделенной линии, причем основное внимание уделяется кабельной проводке между внешними блоками CSU/DSU.



Рис. 15.1. Двухточечная выделенная линия

И наконец, одна из задач этой главы заключается в том, чтобы помочь выявлять технологии WAN, обращая внимание на их различия. Для этого в табл. 15.1 отмечено несколько ключевых фактов о выделенных линиях, а в следующих таблицах будут описаны новые технологии для сравнения.

Таблица 15.1. Ключевые идентификаторы выделенных линий

	Выделенная линия
Типичные физические каналы доступа	TDM (T1, E1 и т.д.)
Интерфейс маршрутизатора	Serial
Протоколы	HDLC, PPP[1]
Предлагаемые услуги WAN	Доставить биты на другой конец линии

[1] Служба выделенной линии не требует и не использует протокол канала связи. Однако маршрутизаторы обычно используют *высокоуровневый протокол управления каналом* (High-Level Data Link Control — HDLC) или *протокол двухточечного соединения* (Point-to-Point Protocol — PPP).

Технология Frame Relay

Концепции и терминология Frame Relay должны быть еще свежи в памяти после глав 13 и 14. На что же следует обращать внимание на экзамене в контексте отличия глобальных сетей Frame Relay от других технологий WAN?

- В качестве канала доступа (канал связи между клиентским маршрутизатором и сетью Frame Relay) обычно используется выделенная линия.

- Клиентские маршрутизаторы (в среде Frame Relay это *терминальное оборудование* (Data Terminal Equipment — DTE)) используют протоколы канала связи Frame Relay.
- Провайдер служб Frame Relay обязуется доставлять фреймы Frame Relay другому клиентскому маршрутизатору (на основании *идентификатора канального подключения* (Data-Link Connection Identifier — DLCI) его *постоянного виртуального канала* (Permanent Virtual Circuit — PVC)).
- Служба является частной. Посланные клиентом А фреймы не попадут на маршрутизаторы, принадлежавшие клиенту В.
- В своей сети провайдер Frame Relay может использовать любую технологию по своему желанию, поэтому на рисунках внутренняя сеть провайдера изображается в виде облака.

Некоторые из этих элементов представлены на рис. 15.2.



Рис. 15.2. Общие элементы, используемые для идентификации глобальных сетей Frame Relay

Глобальные сети Ethernet

Технология Ethernet появилась как технология только локальных сетей, главным образом из-за ограничения дистанции, делавшей непрактичным создание достаточно длинных каналов связи служб WAN. Со временем, благодаря усовершенствованию стандарта оптоволоконных каналов Ethernet уровня 1, увеличилась и скорость, и дистанция. В результате провайдеры служб WAN могут и используют каналы связи Ethernet для предоставления услуг WAN как на клиентском канале доступа, так и в ядре сети провайдера.

Некоторые службы WAN на базе Ethernet используют модель, подобную частным службам WAN на базе Frame Relay. Каналы доступа используют стандарты Ethernet, а не выделенных линий, маршрутизаторы также используют протоколы канала связи Ethernet, а не Frame Relay. Маршрутизаторы могут передавать фреймы Ethernet друг другу по сети WAN. Однако служба WAN Ethernet не поддерживает концепцию PVC. Общее представление дано на рис. 15.3.

Представленная на рис. 15.3 служба WAN Ethernet имеет много названий. В этой книге используются те же названия, что и на курсах Cisco, а именно *Ethernet поверх MPLS* (Ethernet over MPLS — EoMPLS) и более общее — Ethernet WAN. К другим терминам, описывающим различные виды служб Ethernet WAN, относятся *Metropolitan Ethernet* (MetroE) и *виртуальная закрытая служба LAN* (Virtual Private LAN Service — VPLS). И наконец, термин *эмуляция Ethernet* (Ethernet emulation)

подчеркивает тот факт, что провайдер подражает (действует как) большой сети Ethernet, но для создания службы может использовать любую технологию.

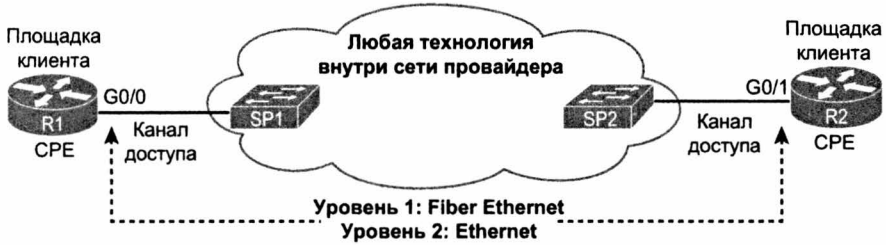


Рис. 15.3. Служба WAN Ethernet по сравнению со службой Frame Relay

Служба WAN Ethernet показана на рисунке подобной Frame Relay. Но она, безусловно, обеспечивает более быстрые скорости, технология Frame Relay обычно не быстрее 44 Мбит/с или такая, как у канала связи T3, тогда как службы WAN Ethernet обеспечивают и 100 Мбит/с и 1 Гбит/с. Ключевые сходства и различия между службами WAN Ethernet и Frame Relay приведены ниже.

Основные сходства и отличия глобальных сетей Ethernet и Frame Relay

- Каналы доступа используют любой стандарт физического уровня *Ethernet*, но для более длинных кабельных соединений обычно используют некий оптоволоконный стандарт.
- Клиентские маршрутизаторы (или коммутаторы LAN) будут использовать некий интерфейс Ethernet, а не последовательный интерфейс.
- Клиентские маршрутизаторы (или коммутаторы LAN) используют протоколы *канала связи Ethernet*.
- На рисунке не будут представлены идентификаторы DLCI, но могут быть представлены MAC-адреса в сети WAN.
- На рисунке в облаке провайдера могут быть представлены коммутаторы Ethernet.
- Частный, по тем же причинам, что и выделенные линии, и Frame Relay.
- В своей сети провайдер WAN Ethernet может использовать любую технологию, которую пожелает, поэтому в центре рисунка она представлена как облако.

Ключевые пункты сравнения трех обсуждавшихся в этой главе технологий WAN приведены в табл. 15.2.

Таблица 15.2. Сравнение технологий Ethernet WAN, Frame Relay и выделенных линий

	Выделенная линия	Frame Relay	Ethernet WAN
Типичные физические каналы доступа	TDM (T1, E1 и т.д.)	TDM (T1, E1 и т.д.)	Ethernet (оптоволоконный)
Интерфейс маршрутизатора	Serial	Serial	Ethernet

Окончание табл. 15.2

	Выделенная линия	Frame Relay	Ethernet WAN
Протоколы	HDLC, PPP[1]	Frame Relay	Ethernet
Обязательство службы WAN	Доставлять биты на другой конец канала	Доставлять фреймы FR на другой конец каждого канала PVC	Доставлять фреймы Ethernet определенным конечным точкам

[1] Служба выделенной линии не требует и не использует протокол канала связи. Однако маршрутизаторы обычно используют протоколы HDLC или PPP.

MPLS

Мультипротокольная коммутация по меткам (Multiprotocol Label Switching — MPLS) использует концепции, подобные глобальным сетям Frame Relay и Ethernet. Но поскольку, подобно глобальным сетям Ethernet, существует множество типов служб WAN MPLS, только для общего представления в этом разделе рассматривается один конкретный случай использования MPLS — сети VPN MPLS.

Службы VPN MPLS используют уже знакомую модель частной сети WAN, где клиентские площадки соединяются с облаком MPLS, перенаправляющим данные между всеми подключенными к нему клиентскими площадками. Как обычно, для сохранения приватности двух несвязанных клиентов A и B, служба MPLS обязуется не перенаправлять данные клиента A на маршрутизаторы клиента B, и наоборот.

Многие факты отличают службы VPN MPLS от других служб WAN, но самое большое различие в том, что служба обязуется передавать между площадками клиентов пакеты IP, а не отдельные биты (как выделенные линии) или фреймы канала связи (как Frame Relay и Ethernet WAN). С точки зрения клиента, сеть MPLS очень похожа на сеть IP, передающую пакеты IP клиентов между площадками.

Идея представлена на рис. 15.4. Клиент B подключен к четырем маршрутизаторам, от B1 до B4, и к службе MPLS. Маршрутизатор B3 перенаправляет пакет IP службе MPLS (этап 1). Служба MPLS так или иначе (детали пока не важны) перенаправляет этот пакет IP на другую сторону службы MPLS. Затем служба перенаправляет пакет IP через канал доступа соответствующему клиентскому маршрутизатору, в данном случае маршрутизатору B4 (этап 3).

Технология MPLS обладает большей гибкостью, чем некоторые другие службы WAN, — это побочный эффект перенаправления пакетов IP. Служба MPLS способна поддерживать практически любой вид каналов доступа, обеспечивающих передачу пакетов IP, как каналы связи, представленные на рис. 15.4. Хотя технология Frame Relay стала менее популярной в этом столетии, ее все еще можно найти во многих сетях, используемой на канале доступа к службе MPLS, как показано на рис. 15.4.

Из всех служб WAN, обсуждавшихся до сих пор в этой главе, у службы MPLS больше всего подобий с глобальными сетями Ethernet и Frame Relay. Эти три технологии сравниваются в табл. 15.3.

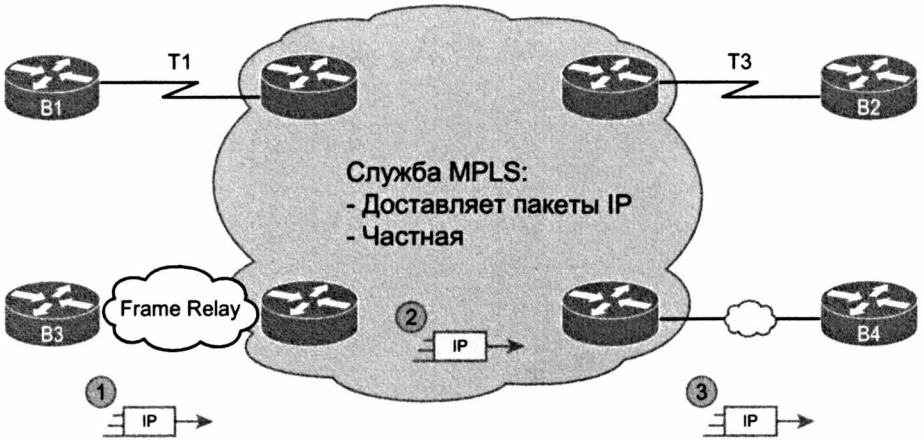


Рис. 15.4. Служба WAN MPLS (VPN MPLS) перенаправляет пакеты IP

Таблица 15.3. Сравнение технологий Ethernet WAN, Frame Relay и MPLS

Ключевая тема

	MPLS	Frame Relay	Ethernet WAN
Физические каналы доступа	Любой поддерживающий IP	TDM (T1, E1 и т.д.)	Ethernet (оптоволоконный)
Интерфейс маршрутизатора	Любой поддерживающий IP	Serial	Ethernet
Протоколы	Любой поддерживающий IP	Frame Relay	Ethernet
Обязательство службы WAN	Доставлять пакеты IP	Доставлять фреймы FR	Доставлять фреймы Ethernet

VSAT

И наконец, обратите внимание, что все частные службы WAN, обсуждавшиеся до сих пор в этой главе, используют некий вид кабельной проводки. Но иногда к сети WAN необходимо подключить пользователей, находящихся в месте, где никакой провайдер не предоставляет таких услуг. Возможно, площадки находятся очень далеко географически, например, на мало населенных островах, куда нет смысла прокладывать дорогой подводный кабель, или, возможно, рельеф местности не позволяет проложить кабели.

В этих случаях компания может создать частную сеть WAN, используя спутниковую связь и терминалы VSAT. *Очень маленький спутниковый терминал* (Very Small Aperture Terminal — VSAT) оснащен спутниковой антенной примерно 1 метр диаметром, как для спутникового телевидения. Антенна VSAT, расположенная снаружи здания, направлена на определенный спутник и подключена к специальному интерфейсу маршрутизатора, расположенного в здании. На рис. 15.5 приведен пример, где антенны VSAT расположены на крышах зданий.

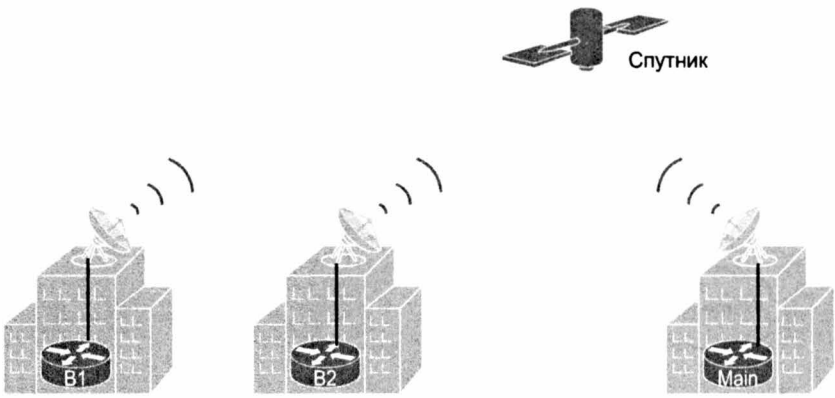


Рис. 15.5. VSAT

Терминалы VSAT позволяют создать частную сеть WAN, как и с использованием выделенных линий, но с одним важным отличием: подключение осуществляется в месте, где другие подключения затруднительны.

Открытые глобальные сети и доступ к Интернету

Для подключения к Интернету *провайдер служб Интернета* (Internet Service Provider — ISP) нуждается в каналах связи с другими провайдерами служб Интернета и каналах связи с клиентами ISP. Ядро Интернета объединяет всех провайдеров служб Интернета, используя множество высокоскоростных технологий. Каналы доступа к Интернету, соединяющие провайдеров ISP с каждым клиентом, также используют широкое разнообразие технологий. Для клиентских каналов доступа технологии должны быть недорогими, чтобы рядовой потребитель мог позволить себе заплатить за службу.

Некоторые технологии WAN работают настолько хорошо, насколько хороша технология доступа к Интернету. Фактически одни используют телефонные линии, поскольку телефонные компании провели их в большинство домов, а провайдеры служб Интернета еще не проложили дополнительную кабельную проводку. Другие используют проводку кабельного телевидения, а третьи — беспроводное подключение.

В данном разделе кратко рассматриваются некоторые из технологий WAN и их использование для доступа к Интернету. Раздел завершается небольшим обсуждением настройки одного из взаимосвязанных протоколов, а именно *PPP поверх Ethernet* (PPP over Ethernet — PPPoE).

Каналы доступа к Интернету (WAN)

Каждая технология WAN может использоваться для построения как открытых, так и частных глобальных сетей; просто одни лучше подходят для первого, а другие для второго. Кстати, только для полноты картины обратите внимание, что все обсуждаемые в первой половине главы технологии WAN прекрасно работают как технологии доступа к Интернету, особенно корпоративного. Для доступа к Интернету компании зачастую используют последовательные каналы TDM, Frame Relay, службы WAN Ethernet или даже службы MPLS. Некоторые из них, а также их условные изображения приведены на рис. 15.6.

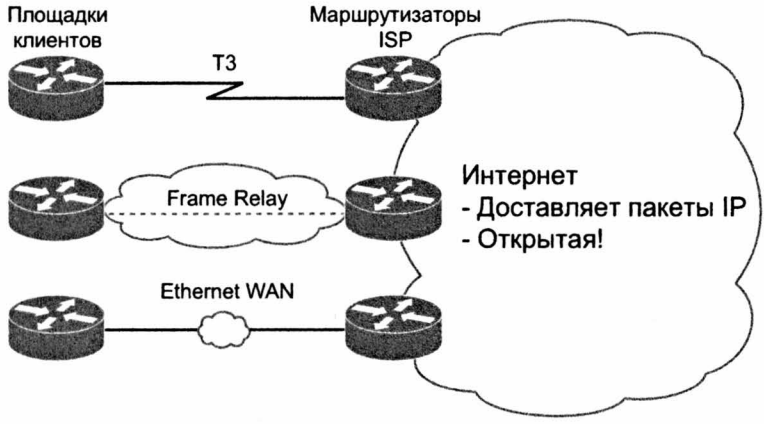


Рис. 15.6. Три примера каналов корпоративного доступа к Интернету

Доступ по телефонным модемам и ISDN

Для обсуждения двух следующих технологий доступа к Интернету следует вспомнить ранние дни Интернета. У Интернета было много периодов быстрого роста, один из них пришелся на начало 1990-х годов, когда появление коммерческого трафика обусловило существенный рост всемирной сети.

На ранних этапах большинство потребителей подключались к Интернету, используя модемную связь, т.е. они использовали свою аналоговую телефонную линию и аналоговый модем для обычного телефонного звонка провайдеру ISP.

Кстати, для общей информации: при использовании домашней телефонной линии вызов создает электрический канал, использующий аналоговый сигнал. Компьютеры используют цифровые сигналы; чтобы передать их по аналоговому каналу, как-то нужно преобразовать цифровой сигнал в аналоговый. Для этого и применяется аналоговый модем.

На каждом конце вызова находились аналоговые модемы — один на площадке клиента и один у провайдера ISP. Для передачи цифровых данных с компьютера или маршрутизатора клиента модем модулирует (или преобразует) цифровой сигнал в аналоговый. Передающий модем посылает аналоговые сигналы принимающему модему, который демодулирует аналоговый сигнал в цифровой. (Термин *модем* образован из начальных букв двух терминов: модуляция и демодуляция.)

Рис. 15.7 дает общее представление на двух примерах. В одном случае компьютер оснащен внешним модемом, а значит, компьютер соединен с модемом кабелем. Во втором случае представлен внутренний модем. У провайдера ISP установлен целый набор модемов, называемый *модемным пулом* (modem bank). Звонок по номеру телефона провайдера ISP примет любой доступный модем, позволяя клиенту подключиться к Интернету.

ВНИМАНИЕ!

Телефонные компании называют телефонный кабель, проложенный к дому или офису клиента, *абонентским каналом* (local loop).



Рис. 15.7. Доступ к Интернету с использованием внешних и внутренних модемов

Сегодня большинство провайдеров служб Интернета называют эту возможность *доступом по телефону* (dial access), или просто *dial*. Несмотря на то что эта возможность использовалась десятилетия назад, большинство провайдеров служб Интернета все еще предоставляют службу dial-app. Она не дорога и применима для удаленных мест, где более быстрые возможности подключения к Интернету недоступны.

Доступ по телефону дешевле по сравнению с другими потребительскими способами доступа к Интернету. Провайдеры ISP имеют *представительства* (Point of Presence — PoP) в большинстве телефонных сетей, поэтому телефонный вызов для подключения к Интернету бесплатный, в отличие от удаленной связи. Кроме того, цена на оборудование со временем существенно упала, поэтому начальная стоимость этого способа относительно низка. Домашняя телефонная линия есть почти в каждом доме, поэтому нет никакой необходимости платить за прокладку физического канала доступа. В результате единственная дополнительная затрата — это плата провайдеру ISP за подключение к Интернету.

Конечно, есть и недостатки. Можно выходить в Интернет, можно разговаривать по телефону, но только не одновременно. Чтобы использовать Интернет, необходим телефонный звонок, поэтому Интернет не может быть подключен постоянно. Но самая большая проблема — скорость; при самом быстром модеме скорость передачи информации по линии составит только 56 Кбит/с — невероятно медленно по сегодняшним стандартам.

Со временем телефонные компании мира намереваются улучшать параметры аналогового модема. Одним из первых усовершенствований было использование новой технологии — *цифровой сети с комплексным обслуживанием* (Integrated Services Digital Network — ISDN). Сеть ISDN обладала преимуществом стоимости аналоговых модемов и более быстрыми скоростями. Ее особенности приведены ниже.

- Сеть ISDN использует тот же абонентский канал (телефонную линию), уже имеющийся у большинства людей.
- Сеть ISDN требует некого эквивалента телефонного звонка провайдеру ISP, как и аналоговый модем.
- Провайдеры служб Интернета уже имеют представительства в телефонных компаниях, чтобы поддерживать аналоговые модемы, поэтому вызовы ISDN не потребуют дополнительной платы за удаленную связь.

Наибольшим преимуществом технологии ISDN была скорость. Она передавала по абонентскому каналу цифровой сигнал вместо аналогового. Кроме того, это поддерживает два одновременных вызова по той же телефонной линии по 64 Кбит/с

каждый. Оба вызова (канала) могли быть объединены в один со скоростью 128 Кбит/с, или пользователь мог звонить по телефону и одновременно иметь подключение к Интернету со скоростью 64 Кбит/с. Служба ISDN действительно стоила немного больше (за модернизированную службу ISDN нужно было платить телефонной компании), но пользователи получали параллельные Интернет и телефон, а также скорость, большую, чем у аналоговых модемов.

Некоторые из подробностей ISDN приведены на рис. 15.8. Потребительская сторона ISDN использует для пользовательского трафика канал *интерфейса базового уровня* (Basic Rate Interface — BRI), обладающий двумя каналами по 64 Кбит/с. Физически соединение использует некое поддерживающее технологию ISDN устройство, зачастую упоминаемое как *модем ISDN* (ISDN modem), занимающий место аналогового модема.



Рис. 15.8. Типичное соединение ISDN

На канале связи со стороны провайдера ISP также может использоваться много разных технологий, включая такую технологию ISDN, как *интерфейс основного уровня* (Primary Rate Interface — PRI). Эта технология превратила физическую линию T1 в 23 канала ISDN, готовых принимать вызовы ISDN (см. рис. 15.8, *справа*).

В первое время существования Интернета аналоговые модемы и технология ISDN удовлетворяли большую часть потребности в доступе к Интернету. Использование существующих телефонных линий, за которые уже заплачено так или иначе, было прекрасным деловым подходом. Но их относительно медленные скорости привели к возникновению новых, более быстрых технологий доступа к Интернету, предоставляемых как телефонными компаниями, так и конкурирующими с ними компаниями кабельного телевидения. Некоторые из ключевых параметров рассмотренных на настоящий момент технологий представлены для сравнения в табл. 15.4.

Таблица 15.4. Сравнение технологий доступа к Интернету

	Аналоговый модем	ISDN
Физические каналы доступа	Телефонная линия (абонентский канал)	Телефонная линия (абонентский канал)
Интернет включен всегда?	Нет	Нет
Обязательство службы данных	Передавать биты с любой вызывающей стороны	Передавать биты с любой вызывающей стороны
Скорость (общая)	56 Кбит/с	128 Кбит/с
Асимметрична?	Нет	Нет

Цифровой абонентский канал

В секторе потребительского доступа к Интернету большой прорыв по скорости произошел с появлением *цифрового абонентского канала* (Digital Subscriber Line — DSL). Это был большой технологический прорыв и с точки зрения скорости. Такое увеличение скорости изменило сам способ использования Интернета, поэтому большинство современных приложений не будет работать на скоростях аналоговых модемов и ISDN.

Как и в случае с технологией ISDN, телефонные компании существенно повлияли на создание технологии DSL. Технология DSL позволила телефонным компаниям предоставлять намного более высокие скорости доступа к Интернету. С деловой точки зрения технология DSL позволила телефонным компаниям предоставлять довольно дорогую услугу высокоскоростного доступа к Интернету множеству уже существующих телефонных клиентов, что позволило им зарабатывать хорошие деньги.

Технически технология DSL работает совсем не так, как аналоговый модем и ISDN. Для начала остановимся на домашней стороне соединения DSL, представленной на рис. 15.9, *слева*. Телефон может делать то, что он делал всегда: передавать аналоговый сигнал, будучи подключенным к телефонной розетке. Для передачи данных модем DSL подключается к параллельной телефонной розетке. Модем DSL передает и получает данные в цифровом виде на более высоких частотах по тому же абонентскому каналу, причем одновременно с телефонным звонком.

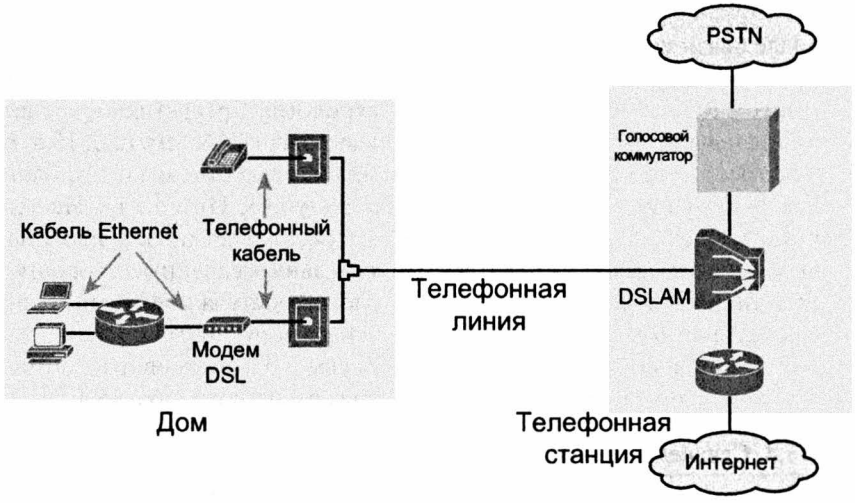


Рис. 15.9. Кабели и устройства домашнего канала связи DSL

Поскольку технология DSL использует на той же линии аналоговые (голосовые) и цифровые (данные) сигналы, телефонная компания должна разделить эти сигналы на своей стороне соединения. Для этого абонентский канал должен быть подключен к *мультиплексору доступа цифровой абонентской линии* (DSL Access Multiplexer — DSLAM), расположенному на ближайшей телефонной станции (CO). Мультиплексор DSLAM отделяет цифровые данные и направляет их на маршрутизатор (внизу справа), устанавливая соединение с Интернетом. Аналоговый (голосовой) сигнал мульти-

плексор DSLAM также отделяет и передает в голосовую телефонную сеть (см. рис. 15.9, *вверху справа*).

Технология DSL имеет много преимуществ, особенно по сравнению с аналоговым модемом и ISDN. Например, *ассиметричная цифровая абонентская линия* (Asymmetric DSL — ADSL), использовавшаяся большинством потребителей DSL, обычно обеспечивает скорость от 5 до 24 Мбит/с (в идеальных условиях). Кроме того, линия ADSL поддерживает асимметричные скорости, лучше всего подходящие для потребительского трафика. Асимметричность означает, что скорость передачи от провайдера к дому (входящая) намного выше, чем скорость передачи из дома к провайдеру ISP (исходящая). Асимметричные скорости лучше для потребительского доступа потому, что щелчок на веб-странице передает в Интернет лишь несколько сот байтов данных, но может вызвать передачу в ответ множества мегабайтов данных.

Конечно, у каждой технологии, включая DSL, есть некоторые недостатки. Канал DSL дороже, чем dial-up, и деньги конечно важны, но такой канал действительно стоит дороже. Кроме того, у технологии DSL есть ограничения. Она хорошо работает только до определенной дистанции между домом и телефонной станцией, а при ее превышении скорость ухудшается. Таким образом, расстояние от дома до телефонной станции может существенно повлиять на качество службы и даже сделать ее недоступной вообще.

Кабельный Интернет

Аналоговые модемы, ISDN и DSL использовали локальный канал связи (телефонную линию) с районной телефонной станцией. Следующая рассматриваемая возможность использует вместо него другой кабель, обычно телевизионный, что создало телефонным компаниям серьезного конкурента на большинстве рынков: кабельные компании.

В общем, но не в деталях, служба доступа кабельного Интернета имеет много общего со службой DSL. Как и DSL, кабельный Интернет использует для передачи данных уже существующую кабельную проводку, в данном случае кабельного телевидения (CATV). Как и DSL, кабельный Интернет использует асимметричные скорости (входящие данные передаются быстрее исходящих), что очень удобно для большинства потребителей. И как DSL, кабельный Интернет позволяет одновременно использовать кабель и по прямому назначению (для телевидения), и для доступа к Интернету.

Общая архитектура кабельного Интернета практически та же, что и у DSL, только вместо телефонного кабеля используется кабель CATV. На рис. 15.10, *слева*, представлен телевизор, подключенный к розетке кабельного телевидения, как и обычно. К другой розетке того же кабеля подключен кабельный модем. Служба доступа к Интернету передает данные на частоте еще одного телевизионного канала, специально зарезервированного для Интернета.

Подобно DSL, на стороне кабельной компании (справа на рисунке) необходимо отделить данные от видео. Данные передаются через маршрутизатор в Интернет (см. рис. 15.10, *внизу справа*). Видеосигнал поступает с телевизионной антенны и распределяется по домам потребителей.

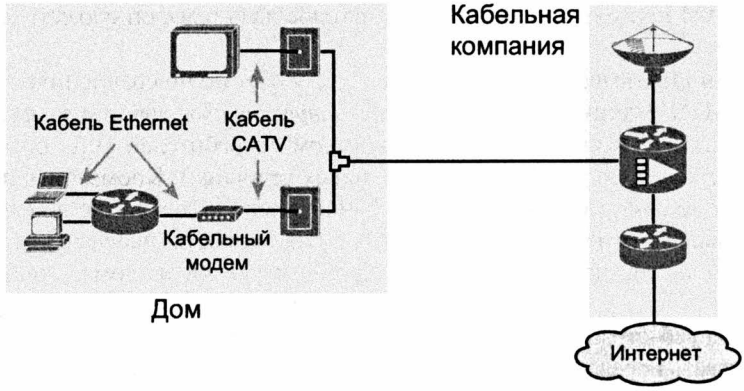


Рис. 15.10. Кабели и устройства домашнего кабельного Интернета

Службы кабельного Интернета и DSL конкурируют на потребительском рынке. По правде говоря, хотя обе технологии предоставляют высокие скорости, кабельный Интернет обычно быстрее, чем DSL, поэтому провайдеры DSL в целях конкуренции предлагают цены немного ниже. Обе службы поддерживают асимметричные скорости и обеспечивают постоянное подключение, позволяя общаться по Интернету без предварительной установки соединения.

Сравнительная характеристика технологий доступа к Интернету приведена в табл. 15.5.

Ключевая тема **Таблица 15.5. Сравнение технологий доступа к Интернету**

	Аналоговый модем	ISDN	DSL	Кабель
Физические каналы доступа	Телефонная линия (абонентский канал)	Телефонная линия (абонентский канал)	Телефонная линия (абонентский канал)	Кабель CATV
Интернет включен всегда?	Нет	Нет	Да	Да
Обязательство службы данных	Передавать биты с любой вызывающей стороны	Передавать биты с любой вызывающей стороны	Передавать все данные провайдеру ISP	Передавать все данные провайдеру ISP
Скорость (общая)	56 Кбит/с	128 Кбит/с	Десятки Мбит/с	Десятки Мбит/с
Асимметрична?	Нет	Нет	Да	Да

Доступ по мобильному телефону

У большинства читателей есть мобильные телефоны, позволяющие подключиться к Интернету и проверить электронную почту, просматривать веб, загружать приложения и смотреть видеофильмы. Среди множества предлагаемых мобильными телефонами возможностей есть и доступ к Интернету. В данном разделе рассматриваются концепции технологии доступа к Интернету по мобильному телефону.

Для связи с ближайшей вышкой сотовой связи мобильные телефоны используют радиоволны. В телефоне есть небольшая радиоантенна, а у провайдера имеется множество больших антенн на вышках в пределах нескольких километров друг от друга. Телефоны, планшетные компьютеры, портативные компьютеры и даже маршрутизаторы (с соответствующими интерфейсными платами) могут подключаться к Интернету с помощью технологии, представленной на рис. 15.11.



Рис. 15.11. Беспроводной доступ к Интернету с использованием технологий 3G/4G

Радиомачты мобильной связи оснащены кабельной проводкой и разным оборудованием, включая маршрутизаторы. Провайдеры мобильной связи создают собственные сети IP, как и провайдеры ISP. Клиентские пакеты IP поступают через маршрутизатор IP на вышки в сеть IP мобильного провайдера, а затем в Интернет.

Рынок мобильных телефонов и других устройств беспроводного доступа к Интернету обширен и разнообразен. В результате провайдеры мобильных служб тратят много денег на рекламу своих услуг с большим количеством разных названий. Откровенно говоря, зачастую трудно сказать, что означает весь этот коммерческий жаргон, но некоторые из терминов используются в отрасли повсеместно.

Названия служб беспроводного доступа к Интернету

Ключевая тема

Беспроводной Интернет (Wireless Internet). Общий термин для служб Интернета — от мобильного телефона до любого устройства, использующего ту же технологию.

Беспроводной 3G/4G (3G/4G Wireless). Сокращение от *третьего* (third generation) и *четвертого поколений* (fourth generation). Эти термины означают главные этапы развития беспроводных сетей и провайдеров мобильной связи.

Технология LTE (Long-Term Evolution — *долгосрочное развитие*). Самая новая и самая быстрая технология в составе технологий четвертого поколения.

Если отбросить коммерческий жаргон, то суть сводится к тому, что когда вы слышите о службах беспроводного Интернета, на логотипе которых изображены вышки мобильной связи (для телефона, планшета или компьютера), то речь, вероятно, идет о таком беспроводном подключении к Интернету, как 3G, 4G или LTE.

PPP поверх Ethernet

В этом разделе мы отступим от перечня технологий WAN и рассмотрим технологию, работающую поверх некоторых соединений DSL: *PPP поверх Ethernet* (PPP over Ethernet — PPPoE).

Концепции PPP поверх Ethernet

Сначала вкратце вспомним обсуждение протоколов PPP и CHAP из главы 12. Протокол PPP — это один из протоколов двухточечных каналов связи, а *протокол аутентификации с предварительным согласованием* (Challenge Handshake Authentication Protocol — CHAP) — это его часть, обеспечивающая аутентификацию. Протокол PPP применяется на последовательных каналах, включая каналы связи, созданные с использованием аналоговых модемов и модемов ISDN. Например, канал связи между пользователем и провайдером ISP, установленный через аналоговые модемы, сейчас, вероятнее всего, использует протокол PPP. На рис. 15.12 дано общее представление об аналоговом соединении dial-up с использованием протокола PPP.

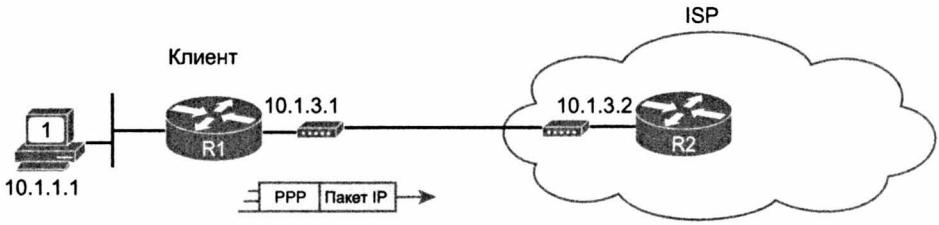


Рис. 15.12. Передача фреймов PPP между маршрутизаторами по соединению dial-up с провайдером ISP

Провайдеры служб Интернета использовали PPP как протокол канала связи по нескольким причинам. В первую очередь, протокол PPP позволяет присваивать IP-адреса устройствам на концах канала связи PPP. Провайдеры служб Интернета могут использовать протокол PPP для присвоения всем клиентам одного открытого IPv4-адреса. Но самое главное, что протокол PPP поддерживает протокол CHAP, используемый провайдерами служб Интернета для аутентификации клиентов. Кроме аутентификации, протокол CHAP позволяет провайдерам служб Интернета проверять учетные записи и определять, оплачен ли счет клиента, прежде чем предоставлять ему доступ к Интернету.

Теперь вспомним немного из истории некоторых технологий доступа к Интернету. Ниже приведены технологии с различной степенью поддержки протокола PPP в порядке их появления на рынке.

1. Аналоговые модемы для связи dial-up, способной использовать протоколы PPP и CHAP.
2. Модемы ISDN для связи dial-up, способной использовать протоколы PPP и CHAP.
3. Модемы DSL не создают двухточечный канал связи и не могут использовать протоколы PPP и CHAP.

Таким образом, и телефонным компаниям, и провайдерам служб Интернета понравилась технология DSL, но некоторым провайдерам все еще хотелось использовать протокол PPP! Однако клиенты все чаще использовали каналы Ethernet между своим компьютером или маршрутизатором и модемом DSL (см. рис. 15.9). Этот канал поддерживает только протоколы канала связи Ethernet, но не PPP.

Таким провайдерам ISP нужен был способ создания эквивалента соединения PPP между маршрутизатором клиента и маршрутизатором ISP с использованием различных технологий, применимых на соединениях DSL. Как уже можно догадаться, для этого было создано несколько новых протоколов, включая протокол PPP поверх Ethernet (PPPoE), позволяющий передачу фреймов PPP, инкапсулируемых во фреймах Ethernet.

Протокол PPPoE просто создает на соединении DSL туннель для передачи фреймов PPP между маршрутизатором клиента и маршрутизатором ISP, как показано на рис. 15.13. Модем DSL не создает единый двухточечный канал связи между этими маршрутизаторами. Используя протокол PPPoE (и протоколы связанные с ним), маршрутизаторы создают такой туннель логически. С одной стороны, маршрутизаторы создают и посылают фреймы PPP, как будто между ними создан канал связи dial-up. Но перед передачей фреймов по любому физическому каналу связи маршрутизаторы инкапсулируют их в различные заголовки, представленные в общем на рисунке как туннельный заголовок.

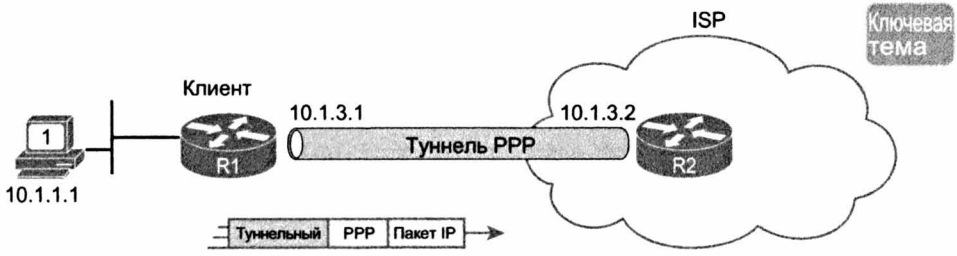


Рис. 15.13. Концепция создания туннеля в канале связи PPP поверх Ethernet

ВНИМАНИЕ!

В этой главе конкретные особенности туннельного заголовка не имеют значения. Но в данном конкретном случае, буквально, туннельный заголовок PPPoE имеет типичный заголовок Ethernet, короткий заголовок для использования протоколом PPPOE, а затем следует фрейм PPP (заключающий пакет IP).

Настройка протокола PPP поверх Ethernet

Получив возможность передавать фреймы PPP между маршрутизаторами, провайдер ISP может продолжить использовать ту же аутентификационную модель, что и при аналоговой связи через набор номера и ISDN. Чтобы все это заработало, маршрутизаторы клиента и ISP нуждаются в некой новой конфигурации, включая конфигурацию протокола PPP. Оставшийся материал этого раздела посвящен общему представлению о конфигурации клиентской стороны.

Для этой конфигурации применяется несколько иной подход. Предположим, имеется типичная конфигурация, как в примере на рис. 15.14. Необходимо решить, какие параметры должны подойти. (Не волнуйтесь о создании этих настроек с самого начала.) Чтобы понимать конфигурацию, учитывайте следующие факты.

- Конфигурация использует интерфейс программы набора номера — виртуальный интерфейс, используемый для создания туннеля PPP. Конфигурация протокола PPP осуществляется на интерфейсе программы набора номера.
- У физического интерфейса Ethernet, подключенного к модему DSL, должны быть команды, разрешающие протокол PPPoE и связывающие интерфейс с интерфейсом программы набора.
- Конфигурация протокола PPP CHAP обычно определяет одностороннюю аутентификацию; т.е. провайдер ISP аутентифицирует клиента, как показано в следующем примере. (Примеры двухсторонней аутентификации см. в главе 12.)
- Клиент может настроить статический IP-адрес, но, вероятнее всего, он попросит у провайдера ISP присвоить открытый IP-адрес (как показано далее).

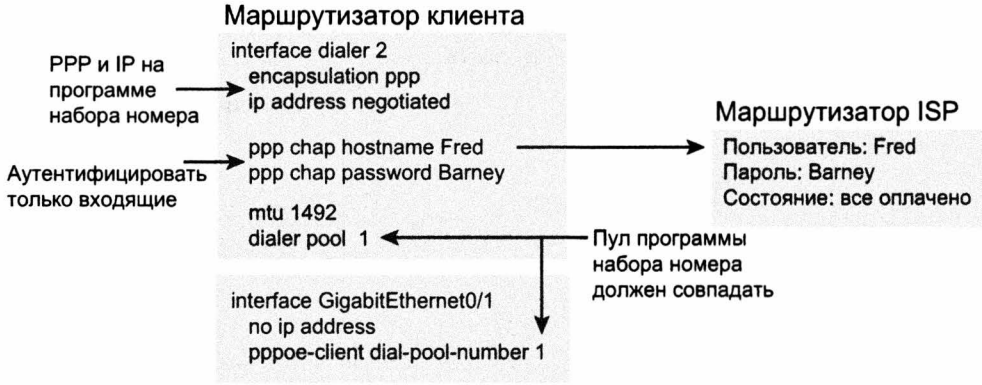


Рис. 15.14. Конфигурация клиента для протокола PPPoE

Встретившись с типовой конфигурацией, внимательно рассмотрите ее основные элементы. Например, конфигурация протокола PPP находится на интерфейсе программы набора номера, а не на интерфейсе Ethernet. Проверьте имя пользователя и пароль CHAP — они должны соответствовать таковым у провайдера ISP. Убедитесь, что команда `dialer interface` связана с интерфейсом Ethernet, а команды `dialer pool` и `pppoeclient` используют то же число, что и на рис. 15.4. (Номер интерфейса программы набора номера не обязательно должен совпадать.) Размер максимального блока передачи (MTU) должен быть снижен до 1492 (стандартное значение 1500), чтобы использоваться в заголовках PPPoE.

Обзор

Резюме

- Большую часть технологий WAN, упомянутых в этой главе, можно использовать для создания и частных глобальных сетей, и открытой сети Интернет.
- В своей сети провайдер Frame Relay может использовать любую технологию по своему желанию, поэтому на рисунках внутренняя сеть провайдера изображается в виде облака.
- Провайдеры служб WAN могут и используют каналы связи Ethernet для предоставления услуг WAN как на клиентском канале доступа, так и в ядре сети провайдера.
- Каналы доступа используют стандарты Ethernet, а не выделенных линий, маршрутизаторы также используют протоколы канала связи Ethernet, а не Frame Relay.
- Каналы доступа используют любой стандарт физического уровня Ethernet, но для более длинных кабельных соединений обычно используют некий оптоволоконный стандарт.
- Мультипротокольная коммутация по меткам (MPLS) использует концепции, подобные глобальным сетям Frame Relay и Ethernet.
- Службы VPN MPLS используют уже знакомую модель частной сети WAN, где клиентские площадки соединяются с облаком MPLS, перенаправляющим данные между всеми подключенными к нему клиентскими площадками.
- Терминалы VSAT позволяют создать частную сеть WAN, как и с использованием выделенных линий, но с одним важным отличием: подключение осуществляется в месте, где другие подключения затруднительны.
- Наибольшим преимуществом технологии ISDN была скорость. Она передавала по абонентскому каналу цифровой сигнал вместо аналогового.
- Модем DSL передает и получает данные в цифровом виде на более высоких частотах по тому же абонентскому каналу.
- В общем, но не в деталях служба доступа кабельного Интернета имеет много общего со службой DSL.
- Для связи с ближайшей вышкой сотовой связи мобильные телефоны используют радиоволны.
- Протокол PPP применяется на последовательных каналах, включая каналы связи, созданные с использованием аналоговых модемов и модемов ISDN.
- Протокол PPPoE просто создает на соединении DSL туннель для передачи фреймов PPP между маршрутизатором клиента и маршрутизатором ISP.

Контрольные вопросы

Ответьте на эти вопросы. Ответы можно найти на последней странице главы. Полное объяснение ответов приведено в приложении B на веб-сайте.

1. Какая из следующих частных служб WAN работает как служба уровня 3, передавая между двумя клиентскими площадками пакеты IP?

   А) Выделенная линия.

   Б) MPLS.

   В) Ethernet WAN.

   Г) Frame Relay.

2. Какая из следующих частных служб WAN предоставляет канал доступа Ethernet на 100 Мбит/с? (Выберите два ответа.)

   А) Выделенная линия.

   Б) MPLS.

   В) Ethernet WAN.

   Г) Frame Relay.

3. Какая из следующих частных служб WAN использовала бы на маршрутизаторе клиента последовательный интерфейс? (Выберите два ответа.)

   А) Выделенная линия.

   Б) VSAT.

   В) Ethernet WAN.

   Г) Frame Relay.

4. Какая из следующих технологий доступа к Интернету обеспечивает постоянное подключение и не требует от пользователя предварительных действий перед отправкой пакетов в Интернет? (Выберите два ответа.)

   А) DSL.

   Б) Аналоговый dial-up.

   В) Кабельный Интернет.

   Г) ISDN.

5. Какая из следующих технологий доступа к Интернету обеспечивает использование симметричных скоростей, т.е. одинаковой скорости приема и передачи данных провайдеру ISP?

   А) DSL.

   Б) ISDN.

   В) Кабельный Интернет.

   Г) Ни одна из вышеупомянутых.

6. В типовой конфигурации PPPoE клиентского маршрутизатора есть четыре команды с параметром 2. У каких двух команд это значение должно совпадать в конфигурации, чтобы все работало правильно? (Выберите два ответа.)

```
interface dialer 2
 dialer pool 2
 encapsulation ppp
 ppp chap hostname Fred
 ppp chap password 2
```

```
 ip address negotiated
 mtu 1492

interface gigabitethernet 0/1
 pppoe-client dial-pool-number 2
```

А) `interface dialer 2`.

Б) `dialer pool 2`.

В) `ppp chap password 2`.

Г) `pppoe-client dial-pool-number 2`.

Ключевые темы

Повторите все ключевые темы данной главы, отмеченные пиктограммой "Ключевая тема". Ключевые темы и соответствующие им страницы перечислены в табл. 15.6.

Таблица 15.6. Ключевые темы главы 15

Элемент	Описание	Страница
Рис. 15.3	Служба WAN Ethernet по сравнению со службой Frame Relay	503
Список	Основные сходства и отличия глобальных сетей Ethernet и Frame Relay	503
Табл. 15.2	Сравнение технологий Ethernet WAN, Frame Relay и выделенных линий	503
Табл. 15.3	Сравнение технологий Ethernet WAN, Frame Relay и MPLS	505
Табл. 15.5	Сравнение технологий доступа к Интернету	512
Список	Названия служб беспроводного доступа к Интернету	513
Рис. 15.13	Концепция создания туннеля в канале связи PPP поверх Ethernet	515

Заполните таблицы и списки по памяти

Распечатайте приложение Г с веб-сайта или его раздел, относящийся к этой главе, и заполните таблицы и списки по памяти. В приложении Д приведены заполненные таблицы и списки для самоконтроля.

Ключевые термины

После первого прочтения главы попытайтесь дать определения следующим ключевым терминам. Но не расстраивайтесь, если не все получится сразу, в главе 22 описано, как использовать эти термины на завершающем этапе подготовки к экзамену.

мультипротокольная коммутация по меткам (Multiprotocol Label Switching — MPLS), Ethernet WAN, очень маленький спутниковый терминал (Very Small Aperture Terminal — VSAT), аналоговый модем (analog modem), цифровая сеть с комплексным обслуживанием (Integrated Services Digital Network — ISDN), доступ по телефону (dial access), модем DSL (DSL modem), кабельный Интернет (cable Internet), 3G/4G Интернет (3G/4G Internet), протокол PPPoE (PPP over Ethernet — PPP по Ethernet)

Ответы на контрольные вопросы:

1 Б. 2 Б и В. 3 А и Г. 4 А и В. 5 Б. 6 Б и Г.

Обзор части IV

Проследите свой прогресс изучения материала части по контрольному списку в следующей таблице. Подробно задачи описаны ниже.

Контрольный список обзора части IV

Задача	Первая дата завершения	Вторая дата завершения
Повторите вопросы из обзоров глав		
Ответьте на вопросы обзора части		
Повторите ключевые темы		
Создайте диаграмму связей первопричин проблем и их изоляции		
Создайте диаграмму связей конфигурации Frame Relay		

Повторите вопросы из обзоров глав

Ответьте снова на вопросы обзоров глав этой части книги, используя программное обеспечение PCPT. Инструкция по запуску программного обеспечения PCPT с вопросами обзоров глав только этой части приведена в разделе "Как просмотреть вопросы только обзоров глав конкретной части" введения к книге.

Ответьте на вопросы обзора части

Ответьте на вопросы обзора этой части книги, используя программное обеспечение PCPT. Инструкция по запуску программного обеспечения PCPT с вопросами обзоров только этой части приведена в разделе "Как просмотреть вопросы только обзоров частей" введения к книге.

Повторите ключевые темы

Снова просмотрите темы прочитанных глав, отмеченные пиктограммой "Ключевая тема". Если понятны не все их подробности, уделите время повторному изучению.

Создайте диаграмму связей первопричин проблем и их изоляции

При создании первой диаграммы связей обзора этой части подумайте о поиске и устранении неисправностей последовательных каналов и каналов Frame Relay. Вспомните все признаки неисправностей, являются ли они первопричиной, помогают ли изолировать проблему или приблизиться к первопричине. Затем объедините их в диаграмму связей. Например, если маршрутизаторы R1 и R2 соединены одним последовательным каналом или постоянным виртуальным каналом Frame Relay (PVC), то что может воспрепятствовать успеху команды `ping` с IP-адресами этих маршрутизаторов? Затем организуйте ответы в диаграмму связей.

Начинайте создание диаграммы связей с того, что пришло на ум. Затем сгруппируйте признаки неисправностей и первопричины. Одной из главных задач является организация этих идей в систему взглядов, поэтому организация информации не менее важна, чем индивидуальные факты. Таким образом, сгруппируйте причины последовательного канала в один набор, а причины канала Frame Relay — в другой.

ВНИМАНИЕ!

Более подробная информация по этой теме приведена в разделе "О диаграммах связей" введения к данной книге.

Создайте диаграмму связей конфигурации Frame Relay

У технологии Frame Relay есть две большие сложности с конфигурацией. Во-первых, это три основных стиля конфигурации: с использованием физического интерфейса, многоточечных и двухточечных субинтерфейсов. Во-вторых, у нее много полезных стандартных настроек.

Для этой диаграммы связей разделите конфигурацию Frame Relay на три раздела. В первом подразумевается, что IP-адреса и идентификаторы канального подключения (DLCI) используются на физическом интерфейсе. Затем запишите все команды конфигурации и их стандартные значения. Для команд, стандартное значение которых применимо для этой ветви, используйте другой цвет.

Затем проделайте то же самое для второй ветви: конфигурации многоточечного субинтерфейса. И наконец, повторите упражнение для ветви двухточечного субинтерфейса. Включите в набор команды создания субинтерфейса.

В завершенной диаграмме связей большинство команд повторится три раза. Но это должно также помочь вам увидеть различия в командах, используемых при каждом стиле конфигурации.

Ответы приведены в приложении E на веб-сайте, но ваши диаграммы связей могут выглядеть иначе.

Как и с протоколом IPv4, компания Cisco распределила темы по протоколу IP версии 6 (IPv6) между экзаменами ICND1 и ICND2. В экзамен ICND1 включены основы: адресация, создание подсетей, маршрутизация, адреса маршрутизатора, настройка статического маршрута и базовая конфигурация протокола OSPF. Экзамен ICND2 включает немного более глубокие темы по протоколу маршрутизации, больше подробностей о протоколах OSPF и EIGRP, поиску и устранению неисправностей процесса маршрутизации и протоколов маршрутизации.

В данной части для протокола IPv6 используется тот же общий подход, что и в частях II и III для протокола IPv4. Глава 16 содержит обзор IPv6 адресации и маршрутизации на уровне экзамена ICND1, включая обсуждение поиска и устранения неисправностей по тем же темам. В главе 17 протокол OSPF версии 3 (OSPFv3) рассмотрен более подробно, а также приведены советы по отладке. И наконец, в главе 18 детально рассматривается второй протокол маршрутизации IPv6 — EIGRP для IPv6 (EIGRPv6).

Часть V. Протокол IP версии 6

Глава 16. “Поиск и устранение неисправностей маршрутизации IPv6”

Глава 17. “Реализация протокола OSPF для IPv6”

Глава 18. “Реализация протокола EIGRP для IPv6”

Обзор части V

Глава 16

Поиск и устранение неисправностей маршрутизации IPv6

Первый этап поиска и устранения неисправностей любой сетевой технологии заключается в том, чтобы понять, как все должно работать в нормальных условиях. Затем следует сравнить текущее поведение сети с должным и сначала найти отличия, а затем первопричины этих отличий.

Глава начинается с обзора тем книги по ICND1 о нормальной работе протокола IPv6. К счастью, у протокола IPv6 много сходств с протоколом IPv4, кроме очевидных различий в адресации. Данный раздел построен на этих подобиях, и в нем рассматриваются основные средства протокола IPv6, чтобы подготовить почву для обсуждения поиска и устранения неисправностей протокола IPv6.

Второй главный раздел главы посвящен множеству проблем, которые могут возникнуть в сети IPv6. Все эти проблемы препятствуют нормальной работе протокола IPv6.

В этой главе рассматриваются следующие экзаменационные темы
Поиск и устранение неисправностей
Поиск и устранение наиболее распространенных проблем сети
Поиск и устранение проблем маршрутизации
Разрешение маршрутизации
Правильность таблицы маршрутизации
Выбор правильного пути

Основные темы

Нормальная работа протокола IPv6

Чтобы быть готовым к поиску и устранению проблем протокола IPv6, необходимо помнить много фактов о его работе. К счастью, большинство концепций протокола IPv6 совпадает с таковыми у протокола IPv4, но есть и достаточно много различий, чтобы уделить время обзору самого протокола IPv6. Данный раздел содержит краткий обзор подробностей протокола IPv6, описанных в пяти главах книги по ICND1.

В данном разделе, вплоть до подраздела "Поиск и устранение неисправностей IPv6", повторно рассматриваются концепции из книги по ICND1. Если вы используете обе книги, то, возможно, должны вернуться к первому тому или можете пропустить этот раздел и продолжить со следующего, как описано далее.

Пропустите все до раздела "Поиск и устранение неисправностей IPv6". Если темы по протоколу IPv6 свежи в памяти, пропустите этот раздел. Возможно, вы только что закончили читать главы по протоколу IPv6 из книги ICND1 и материал еще свеж в памяти. Знайте, что в этом разделе не вводятся новые концепции, не описанные в главах об IPv6 из книги по ICND1.

Прочитайте этот раздел. Если вы помните часть информации по протоколу IPv6, но не все, то этот раздел именно для вас. Продолжайте читать!

Вернитесь к книге по ICND1. Если вы не занимались протоколом IPv6 довольно долго и действительно многого не помните вообще, то сначала имеет смысл вернуться к главам о протоколе IPv6 из книги по ICND1.

Так о чем же пойдет речь в этом разделе? Здесь изложены основные факты о протоколе IPv6, одноадресатной адресации IPv6 и создании подсетей. Обсуждается также конфигурация хоста IPv6, включая *автоматическую настройку адреса без фиксации состояния* (Stateless Address Autoconfiguration — SLAAC) и *протокол динамического конфигурирования хоста* (Dynamic Host Configuration Protocol — DHCP) с фиксацией состояния. Он также содержит обзор базовых протоколов, таких как *протокол обнаружения соседних устройств* (Neighbor Discovery Protocol — NDP), и таких команд, как `ping` и `traceroute`. Раздел завершается обзором конфигурации адресации и статических маршрутов маршрутизатора (обзор конфигурации протокола OSPFv3 приведен в главе 17).

Одноадресатные IPv6-адреса и подсети IPv6

Протокол IPv6 определяет два главных типа одноадресатных IPv6-адресов. *Глобальные одноадресатные* адреса подобны открытым IPv4-адресам, т.е., получив уникальный префикс, предприятие начинает все свои адреса с этого префикса. Все компании используют уникальные префиксы, и все IPv6-адреса в Интернете остаются уникальными.

Уникальные локальные одноадресатные адреса больше похожи на частные адреса. Компания может создать произвольный префикс и присваивать начинающиеся с него адреса. Уникальные локальные адреса позволяют компаниям избежать необходимости регистрации префикса, при хорошем статистическом шансе не использовать тот же диапазон адресов, что и другие компании.

Создание подсетей с глобальными одноадресатными адресами компании начинают с глобального префикса маршрутизации, присвоенного компании, разделяя структуру адреса на три части. Почти во всех случаях, включая большинство случаев, описанных в этой книге и книге по ICND1, комбинация глобального префикса маршрутизации и части подсети адреса составляют первую половину (64 бита) структуры адреса. Часть подсети позволяет инженеру корпоративной сети нумеровать все подсети уникальным значением, однозначно определяя каждую подсеть. Остальная часть структуры оставляет место для 64-битового идентификатора интерфейса (или поля хоста). Эти правила приведены на рис. 16.1.

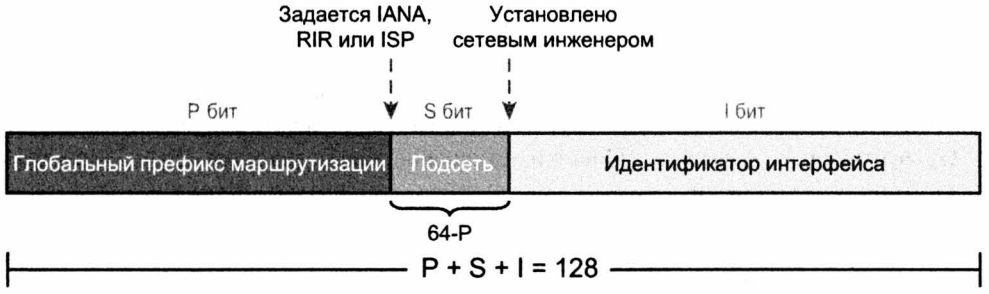


Рис. 16.1. Структура глобального одноадресатного IPv6-адреса в подсети

Предположим, компания получила глобальный префикс маршрутизации 2001:DB8:1111::/48. Таким образом, все адреса компании должны начинаться с этих 12 шестнадцатеричных цифр. Весь четвертый квартет адреса занимает часть подсети. Это может быть шестнадцатеричное значение 0000, 0001, 0002 и т.д. до FFFF, т.е. в данном примере возможно 65 536 подсетей. В результате компания могла бы получить проект подсети, представленный на рис. 16.2.

Внимание! Формально при обсуждении адресации IPv6 следует использовать термин *префикс*, а не *подсеть*, но многие используют их как синонимы.

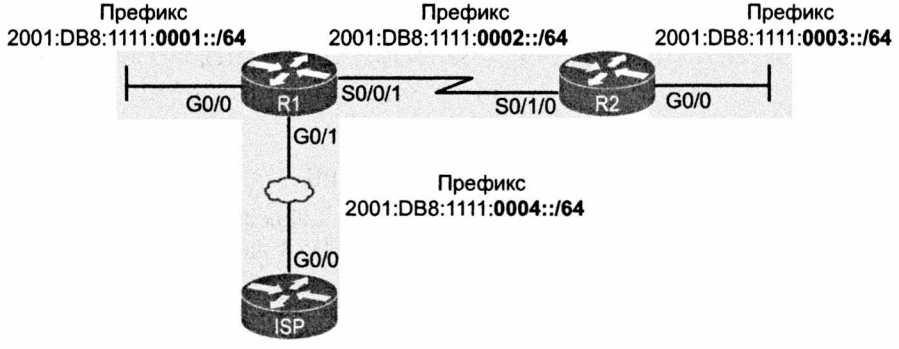


Рис. 16.2. Проект подсети с глобальным префиксом маршрутизации 2001:0DB8:1111

Хотя рис. 16.2 полезен при планировании подсети, на нем показаны конкретные IPv6-адреса. Как и IPv4, протокол IPv6 следует тем же общим правилам. Например, хосты и маршрутизаторы, подключенные к тем же сетям VLAN Ethernet, должны

располагаться в той же подсети IPv6. На рис. 16.3 приведен пример с IPv6-адресами в подсетях, соответствующих рис. 16.2.

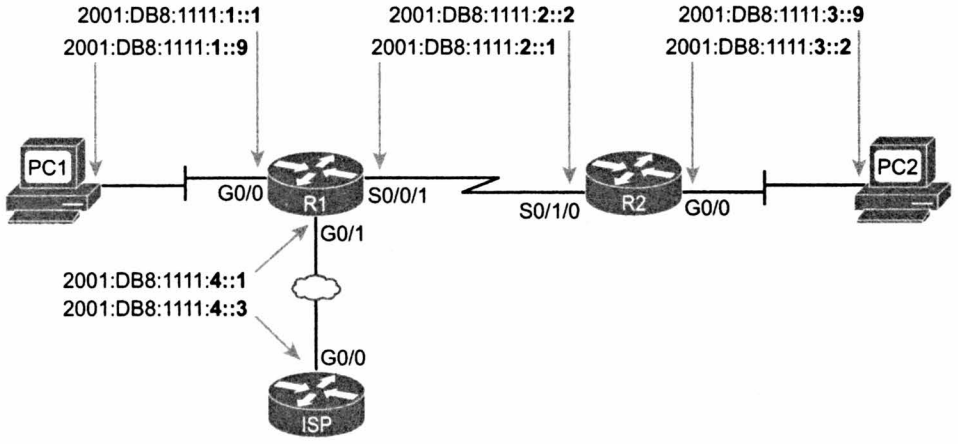


Рис. 16.3. Пример статических IPv6-адресов на основании проекта подсети на рис. 16.2

Для обмена пакетами IPv6 с другими хостами хосты могут использовать глобальные одноадресатные и уникальные локальные одноадресатные адреса, но для пакетов, которые остаются на том же канале связи, протокол IPv6 определяет специальный тип одноадресатного адреса: *адрес, локальный в пределах канала связи* (link-local address). Многие протоколы должны передавать пакеты IPv6 только в локальной подсети, им не нужны маршрутизаторы для перенаправления пакетов в любые другие подсети. Для этих протоколов протокол IPv6 использует адреса, локальные в пределах канала связи. Обратите внимание, что хосты могут создать собственный адрес, локальный в пределах канала связи, даже прежде, чем у хоста появится допустимый глобальный одноадресатный или уникальный локальный адрес.

Хосты и маршрутизаторы IPv6 создают для каждого интерфейса собственный локальный в пределах канала связи адрес согласно неким простым правилам. Все локальные в пределах канала связи адреса начинаются с того же префикса из 16 цифр (FE80:0000:0000:0000), как показано на рис. 16.4, *слева*. Маршрутизатор или хост самостоятельно формирует заключительные 16 шестнадцатеричных цифр, используя правила EUI-64 (подробнее об этом — в следующем разделе).

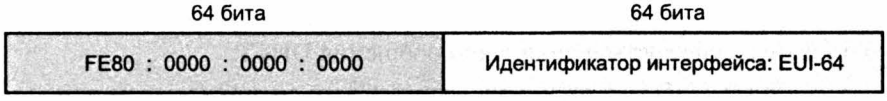


Рис. 16.4. Формат адреса, локального в пределах канала связи

Несколько фактов о глобальных одноадресатных, уникальных локальных одноадресатных и локальных для канала связи адресах приведены в табл. 16.1.

Ключевая тема **Таблица 16.1. Типы одноадресатных IPv6 адресов**

Type	Первые цифры	Подобен открытому или частному IPv4-адресу?
Глобальный одноадресатный	2 или 3[1]	Открытому
Уникальный локальный одноадресатный	FD	Частному
Локальный для канала связи	FE80	Никакому

[1] IANA фактически определяет диапазон глобальных одноадресатных адресов как любой адрес, не зарезервированный для других целей. Однако обычно адреса присваиваются начиная с 2000::/3, поскольку это был первоначальный диапазон, используемый для этих адресов. Большинство справочников по протоколу IPv6 просто указывает префикс как 2000::/3, упоминая, что первой шестнадцатеричной цифрой должна быть 2 или 3.

Присвоение адресов хостам

Как только будут обсуждены, зарегистрированы и задокументированы все подробности адресации, адреса следует настроить на всех хостах и маршрутизаторах. Данный подраздел посвящен настройке хостов IPv6 (включая адресацию).

С точки зрения обучения конфигурация хоста IPv6 немного сложней, чем IPv4. Протокол IPv6 добавляет в набор еще один протокол, *протокол обнаружения соседних устройств* (Neighbor Discovery Protocol — NDP), и предоставляет две возможности получения хостами своих параметров IPv6. Изучение способов динамического получения хостами IPv6 своих параметров IPv6 потребует немного больше усилий, чем в случае IPv4.

У хостов IPv6 есть три основных возможности установки параметров IPv6: статическая конфигурация, протокол DHCP с фиксацией состояния и SLAAC. При статической конфигурации некто просто вводит параметры в соответствующей части пользовательского интерфейса, поэтому в этом разделе не обсуждается статическая настройка параметров, а рассматриваются способы динамической настройки.

Протокол DHCPv6 с фиксацией состояния

Протокол DHCPv6 с фиксацией состояния следует тем же общим принципам, что и протокол DHCP для IPv4 (DHCPv4).

1. Где-нибудь в объединенной сети есть один или несколько серверов DHCP.
2. Для запроса резервируемого IP-адреса и информации о других параметрах пользовательские хосты используют сообщения DHCP.
3. В ответ сервер сообщает хосту присвоенный адрес и другие параметры.

Одно из существенных отличий между протоколами DHCPv4 и DHCPv6 с фиксацией состояния в том, что последний не предоставляет информацию о стандартном маршрутизаторе. Для этого используется встроенный протокол NDP, позволяющий хосту попросить локальные маршрутизаторы идентифицировать себя. В противном случае хосты используют тот же общий процесс, что и DHCPv4. На рис. 16.5 сравнивается то, что хост изучает по протоколу DHCPv4, а что по протоколу DHCPv6 с фиксацией состояния.

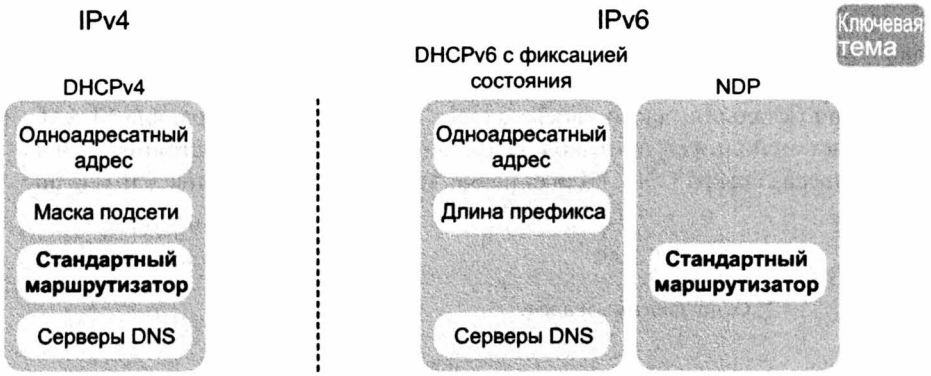


Рис. 16.5. Источники параметров IPv6 при использовании протокола DHCP с фиксацией состояния

Если сервер DHCPv6 с фиксацией состояния находится в подсети, отличной от хоста, протокол DHCPv6 полагается на функцию *агента пересылки DHCP* (DHCP Relay Agent), как показано на рис. 16.6. Предположим, например, что расположенный слева хост A начинает попытку получения адреса для передачи сообщения DHCPv6 Solicit. Это сообщение передается на многоадресатный адрес IPv6 FF02::1:2, и маршрутизаторы, такие как R1, обычно не перенаправляют пакеты, посланные на этот многоадресатный адрес в локальной области видимости. Но при настройке на интерфейсе G0/0 маршрутизатора R1 агента пересылки DHCPv6, как показано на рисунке, маршрутизатор R1 перенаправит сообщение DHCPv6 хоста A на сервер DHCP.

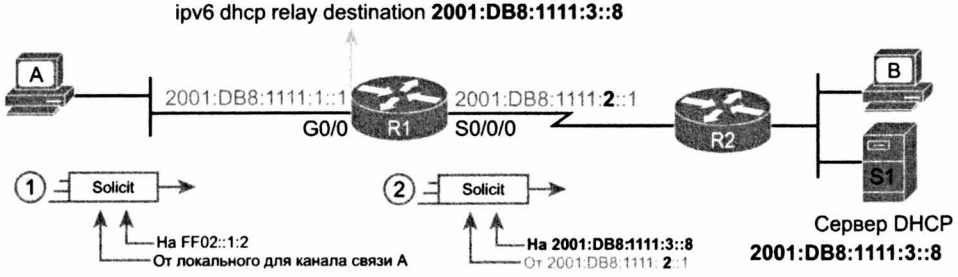


Рис. 16.6. Агент пересылки DHCPv6 и IPv6-адреса DHCP

Автоматическая настройка адреса без фиксации состояния

Автоматическая настройка адресов без фиксации состояния (Stateless Address Autoconfiguration — SLAAC) IPv6 является альтернативным методом динамического присвоения IPv6-адресов, не нуждающихся в сервере с фиксацией состояния. Другими словами, технология SLAAC не требует, чтобы предоставляющий IPv6-адреса сервер записывал (сохранял информацию о состоянии), какому хосту какой IPv6-адрес присвоен, в отличие от службы DHCPv6 с фиксацией состояния.

Общий процесс SLAAC также использует протокол NDP и службу DHCPv6 без фиксации состояния, т.е. сервер не хранит информацию о состоянии. В первую

очередь процесс использует протокол NDP, позволяющий хосту узнавать у любого маршрутизатора на канале связи префикс IPv6 (идентификатор подсети), длину префикса (эквивалент маски) и IPv6-адрес стандартного маршрутизатора. Для построения остальной части своего адреса хост использует правила SLAAC. И наконец, хост использует протокол DHCPv6 без фиксации состояния для выяснения IPv6-адреса сервера DNS. (Для справки эти подробности приведены на рис. 16.7.)

Ключевая тема

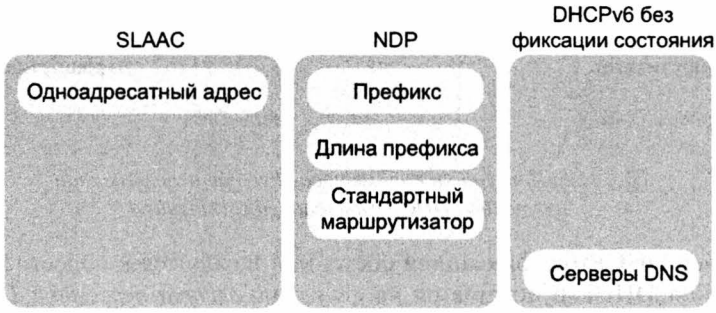


Рис. 16.7. Источники параметров IPv6 при использовании SLAAC

Технология SLAAC позволяет хосту получить значения трех параметров (длину префикса, адрес маршрутизатора и серверов DNS), а чтобы создать значение адреса, хост использует следующие этапы.

1. Используя сообщения NDP Router Solicitation (RS) и Router Advertisement (RA), хост получает от любого маршрутизатора префикс IPv6, используемый на канале связи.
2. Чтобы выбрать значение идентификатора интерфейса, хост либо использует только что полученный префикс IPv6, либо случайное число, либо MAC-адрес хоста в соответствии с правилами EUI-64.

Если хост использует правила EUI-64, то созданный хостом адрес может быть предсказан. Префиксная часть адреса — это префикс, определенный на локальном маршрутизаторе IPv6. Далее, согласно правилам EUI-64, 48-битовый MAC-адрес хоста преобразуется в 64-битовый идентификатор интерфейса следующим образом.

Ключевая тема

Этапы создания адреса с использованием SLAAC и EUI-64

1. 6-байтовый (12 шестнадцатеричных цифр) MAC-адрес разделяется на две половины (по 6 шестнадцатеричных цифр каждая).
2. Между этими двумя половинами вставляется часть FFFE, чтобы идентификатор интерфейса имел теперь в общей сложности 16 шестнадцатеричных цифр (64 бита).
3. Седьмой бит идентификатора интерфейса инвертируется.

Основные элементы такого адреса приведены на рис. 16.8.



Рис. 16.8. Формат IPv6-адреса с идентификатором интерфейса и частью EUI-64

Адрес маршрутизатора и статическая настройка маршрута

На настоящий момент в этом разделе рассмотрены IPv6-адреса, подсети IPv6 и присвоение адресов хостам. Далее речь пойдет о присвоении адреса маршрутизатору, разрешении маршрутизации IPv6 и настройке статических маршрутов IPv6.

Настройка маршрутизации IPv6 и адресов на маршрутизаторах

Для разрешения маршрутизации IPv6 на маршрутизаторе необходимо решить две простых задачи.

Ключевая тема **Этапы настройки IPv6 адресации и маршрутизации**

Этап 1 Разрешить маршрутизацию IPv6 глобальной командой `ipv6 unicast-routing`

Этап 2 Разрешить маршрутизацию IPv6 на каждом необходимом интерфейсе, задать IPv6-адрес интерфейса и длину префикса подкомандой `ipv6 address` *`адреса/длина`* в режиме конфигурации интерфейса

Во многих случаях реализации плана IPv6 адресации внутри предприятия используют стратегию *двойного стека* (dual-stack), по крайней мере на маршрутизаторах и, возможно, хостах. Таким образом, маршрутизаторы все еще перенаправляют пакеты IPv4, а на их интерфейсах остаются IPv4-адреса. Затем маршрутизация IPv6 добавляется в конфигурацию как второй протокол уровня 3, откуда и происходит название *двойной стек*.

Пример 16.1 демонстрирует конфигурацию, где маршрутизация IPv6 добавляется к существующей конфигурации на маршрутизаторе R1, согласно рис. 16.3. Маршрутизатор R1 использует три интерфейса, адреса которых известны и представлены на этом рисунке. В результате в примере 16.1 все адреса вводятся в конфигурацию статически. Обратите также внимание, что длина префикса, в данном случае /64, указана сразу после адреса без пробела. (При использовании подхода двойного стека конфигурация IPv4, не представленная здесь, обычно уже существует.)

Пример 16.1. Настройка маршрутизации IPv6 на маршрутизаторе R1 согласно рис. 16.3

```
ipv6 unicast-routing
!
interface serial0/0/1
    ipv6 address 2001:db8:1111:2::1/64
!
interface gigabitethernet0/0
```

```
    ipv6 address 2001:db8:1111:1::1/64
!
interface gigabitethernet0/1
    ipv6 address 2001:db8:1111:4::1/64
```

В качестве альтернативы при формировании адресов маршрутизаторы могут также использовать правила EUI-64. Для этого в команды `ipv6 address` настройки маршрутизатора следует внести два изменения. Во-первых, команды используют только префикс, а не весь адрес, поскольку маршрутизатор сам создаст часть идентификатора интерфейса в адресе. Во-вторых, в конце команды используется ключевое слово `eui-64`. Таким образом, для использования правил EUI-64 на интерфейсе G0/0 маршрутизатора R1 можно использовать команду `ipv6 address 2001:db8:1111:1::/64 eui-64`.

Статические маршруты IPv6 на маршрутизаторах

Что касается маршрутов IPv6, то большинство предприятий использует динамический протокол маршрутизации IPv6, такой как *открытый протокол поиска первого кратчайшего маршрута версии 3* (Open Shortest Path First Version 3 — OSPFv3; см. главу 17) или *расширенный протокол маршрутизации внутреннего шлюза* (Enhanced Interior Gateway Routing Protocol — EIGRP; см. главу 18). Но маршрутизаторы поддерживают, конечно, и статические маршруты.

Статические маршруты IPv6 предоставляют маршрутизаторам три основные возможности указания направления дальнейшей передачи пакетов. Все они перечислены ниже и представлены на рис. 16.9.

1. Направить пакеты на локальный интерфейс маршрутизатора.
2. Направить пакеты на одноадресатный адрес соседнего маршрутизатора.
3. Направить пакеты на адрес, локальный в пределах канала связи соседнего маршрутизатора (требуется также исходящий интерфейс).

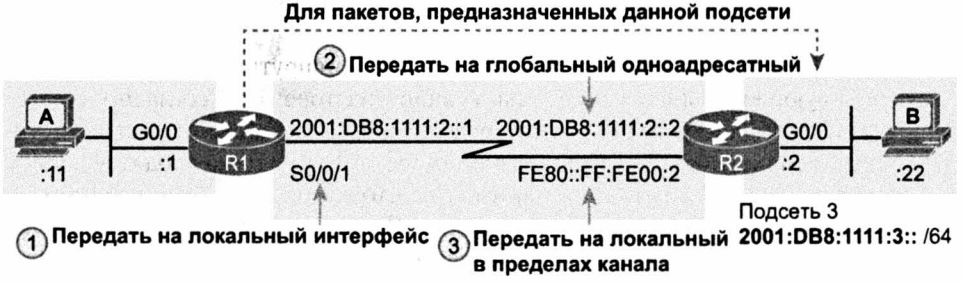


Рис. 16.9. Три возможности статических маршрутов в конфигурации IPv6

В примере 16.2 приведены статические маршруты в каждом из трех стилей в соответствии с рисунком. Один маршрутизатор не использовал бы три статических маршрута для того же префикса IPv6 получателя; все три случая приведены только в качестве примера синтаксиса каждой команды.

Пример 16.2. Три возможности задания статических маршрутов IPv6

```
! Следующая команда использует интерфейс S0/0/1 маршрутизатора R1 как
! исходящий
ipv6 route 2001:db8:1111:3::/64 S0/0/1

! Следующая команда использует адрес маршрутизатора R2's как
! одноадресатный адрес следующего транзитного маршрутизатора
ipv6 route 2001:db8:1111:3::/64 2001:DB8:1111:2::2

! Следующая команда использует интерфейс S0/0/1 маршрутизатора R1 как
! исходящий и локальный в пределах канала связи адрес маршрутизатора R2
! как адрес следующего транзитного маршрутизатора
ipv6 route 2001:db8:1111:3::/64 S0/0/1 FE80::FF:FE00:2
```

Проверка соединения IPv6

Большинство задач поиска и устранения неисправностей, а также экзаменационных задач начинается с частично работающей сети. Для поиска имеющихся проблем инженер должен ввести различные команды, чтобы проверить, какие элементы сети работают правильно, а какие нет. В следующем разделе содержится обзор нескольких команд, используемых для проверки подключения IPv6 и на хостах, и на маршрутизаторах.

Проверка подключения IPv6 с хостов

В первую очередь на любом хосте IPv6 следует проверить четыре ключевых параметра IPv6, показанных на рис. 16.10, *слева*. На этом этапе следует не только проверить параметры на самом хосте, но и сравнить их с таковыми на других устройствах в сети. Например, параметр стандартного маршрутизатора хоста (стандартный шлюз) должен соответствовать адресу, заданному на локальном маршрутизаторе.

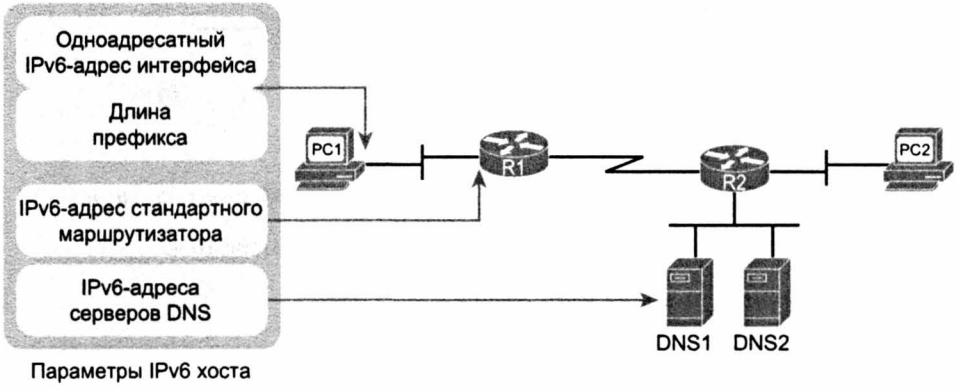


Рис. 16.10. Параметры IPv6, необходимые на хостах

Операционная система хоста обычно предоставляет некий способ просмотра параметров IPv6 в графическом интерфейсе пользователя (GUI), а также соответствующие команды. Четыре главных параметра IPv6, а также некоторые другие параметры обычно представляют команды `ipconfig` (операционные системы Windows) и

`ifconfig` (Linux и Mac OS). Пример 16.3 демонстрирует вывод команды `ifconfig` на хосте Linux, где выделены адрес и длина префикса для глобального одноадресатного и локального в пределах канала связи адресов.

Пример 16.3. Команда `ifconfig` в операционной системе Linux

```
WOair$ ifconfig en0
eth0: Link encap:Ethernet Hwaddr 02:00:11:11:11:11
      inet addr:10.1.1.99 Bcast:10.1.1.255 Mask:255.255.255.0
      inet6 addr: fe80::11ff:fe11:1111/64 Scope:Link
      inet6 2001:db8:1111:1::11/64 Scope:Global
      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
      RX packets: 45 errors:0 droppped:0 overruns:0 frame:0
      TX packets: 804 errors:0 droppped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:5110 (5.1 KB) TX bytes:140120 (140.1 KB)
```

Конечно, наилучшими командами проверки подключения являются `ping` и `traceroute`. Некоторые хосты используют те же команды `ping` и `traceroute` как для IPv4, так и для IPv6, тогда как другие (особенно под Mac OS и Linux) используют для IPv6 другие команды (например, `ping6` и `traceroute6`).

При использовании команды `ping6` для поиска и устранения неисправностей проверяют ближайший IPv6-адрес, затем адрес маршрутизатора и так далее, пока одна из команд не потерпит неудачи, что поможет изолировать проблему. Например, пользователь компьютера PC1 на рис. 16.11 может проверить ближайший интерфейс маршрутизатора R1, затем IPv6-адрес его последовательного интерфейса, затем IPv6-адрес интерфейса S0/1/0 маршрутизатора R2 и т.д.

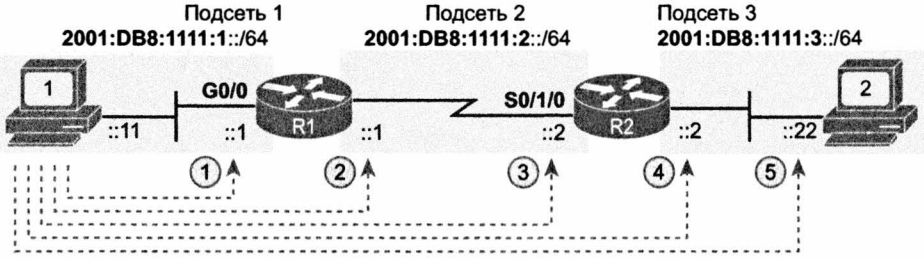


Рис. 16.11. Последовательность проверки при изоляции проблемы маршрутизации IPv6

Этапы 1 и 5, показанные на рис. 16.11, приведены в примере 16.4.

Пример 16.4. Команды `ping6` на компьютере для ближайшего интерфейса R1 и компьютера PC2

```
Master@PC1:~$ ping6 2001:db8:1111:1::1
PING 2001:db8:1111:1::1 (2001:db8:1111:1::1) 56 data bytes
64 bytes from 2001:db8:1111:1::11: icmp_seq=1 ttl=64 time=1.26 ms
64 bytes from 2001:db8:1111:1::11: icmp_seq=2 ttl=64 time=1.15 ms
^C
--- 2001:db8:1111:1::1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001 ms
rtt min/avg/max/mdev = 1.156/1.210/1.263/0.062 ms
```

```
Master@PC1:~$ ping6 2001:db8:1111:3::22
PING 2001:db8:1111:3::22 ( 2001:db8:1111:3::22) 56 data bytes
64 bytes from 2001:db8:1111:3::22: icmp_seq=1 ttl=64 time=2.33 ms
64 bytes from 2001:db8:1111:3::22: icmp_seq=2 ttl=64 time=2.59 ms
64 bytes from 2001:db8:1111:3::22: icmp_seq=3 ttl=64 time=2.03 ms
^C
--- 2001:db8:1111:3::22 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003 ms
rtt min/avg/max/mdev = 2.039/2.321/2.591/0.225 ms
```

Проверка подключения IPv6 на маршрутизаторах

Маршрутизаторы Cisco поддерживают команды `ping` и `traceroute` для протокола IPv6. Обе команды воспринимают IPv4- и IPv6-адреса, имена хостов, а также имеют как стандартные, так и расширенные версии.

Расширенные команды `ping` и `traceroute` предоставляют большие возможности, позволяя, находясь в CLI маршрутизатора, проверять обратный маршрут, используемый хостами в подключенных локальных сетях. В главе 4 обсуждались концепции протокола IPv4, те же концепции применимы и к протоколу IPv6. Напомним, что расширенные версии команд IPv6 `ping` и `traceroute` позволяют проверять с маршрутизатора обратные маршруты к исходной подсети. На рис. 16.12, например, расширенная команда `ping` на маршрутизаторе R1 с IPv6-адресом компьютера PC2 позволяет проверить прямой маршрут к компьютеру PC2. Но если в расширенной команде `ping` используется как источник интерфейс G0/0 маршрутизатора R1, то эта команда проверяет также обратный маршрут к компьютеру PC1 из подсети IPv6.

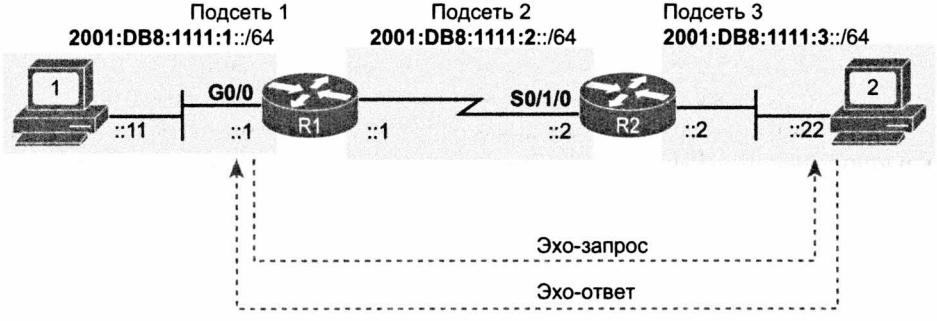


Рис. 16.12. Адреса отправителя и получателя расширенной команды `ping` в примере 16.5

В примере 16.5 приведена расширенная команда `ping` IPv6 с маршрутизатора R1 на компьютер PC2 с использованием интерфейса G0/0 маршрутизатора R1 в качестве отправителя пакетов. Вторая команда — это стандартная команда IPv6 `traceroute` с маршрутизатора R1 на компьютер PC2.

Пример 16.5. Расширенная команда `ping` и стандартная команда `traceroute` на маршрутизаторе R1

```
R1# ping
Protocol [ip]: ipv6
Target IPv6 address: 2001:db8:1111:3::22
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands? [no]: yes
Source address or interface: GigabitEthernet0/0
UDP protocol? [no]:
Verbose? [no]:
Precedence [0]:
DSCP [0]:
Include hop by hop option? [no]:
Include destination option? [no]:
Sweep range of sizes? [no]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:1111:3::22, timeout is 2 se-
conds:
Packet sent with a source address of 2001:DB8:1111:1::1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/1/4 ms
R1# traceroute 2001:db8:1111:3::22
Type escape sequence to abort.
Tracing the route to 2001:DB8:1111:3::22

1 2001:DB8:1111:2::2 4 msec 0 msec 0 msec
2 2001:DB8:1111:3::22 0 msec 4 msec 0 msec
```

Когда команда IPv6 `ping` или `traceroute` указывает на некоторую проблему маршрутизации, для изоляции проблемы и поиска первопричины может понадобиться больше этапов. Большая часть проблем маршрутизации IPv6 обсуждается в главах 17 и 18. Там же рассматриваются конкретные причины, по которым протоколы OSPFv3 и EIGRPv6 могут оказаться не в состоянии поместить маршрут в таблицу маршрутизации IPv6.

Для отображения конкретного маршрута IPv6 маршрутизатору достаточно послать пакеты на определенный адрес получателя, используя команду `show ipv6 route` *адрес*. Команда выводит несколько строк с подробностями о маршруте, используемом маршрутизатором. Если у маршрутизатора нет соответствующего маршрута, маршрутизатор выводит сообщение "`Route not found`" (Маршрут не найден). Приведенный в примере 16.6 соответствующий маршрут является статическим маршрутом для перенаправления пакетов через интерфейс S0/0/1. Здесь также приведен пример, когда маршрут не был найден.

Пример 16.6. Отображение маршрута, используемого маршрутизатором R1 для перенаправления пакетов по адресу 2001:DB8:1111:3:: 22

```
R1# show ipv6 route 2001:db8:1111:3::22
Routing entry for 2001:DB8:1111:3::/64
  Known via "static", distance 1, metric 0
  Route count is 1/1, share count 0
```

```
  Routing paths:
    directly connected via Serial0/0/1
      Last updated 00:01:29 ago

R1# show ipv6 route 2001:1:1:1::1
% Route not found
```

Кроме того, команда `show ipv6 neighbors` выводит замену IPv6 для таблиц *протокола преобразования адресов* (Address Resolution Protocol — ARP) IPv4. Если команда `ping` терпит неудачу и ожидаемая запись в этой таблице отсутствует, то этот факт может указывать на проблему, препятствующую обнаружению протоколом NDP MAC-адреса соседа. В примере 16.7 показана эта команда на маршрутизаторе R2, согласно рис. 16.12. Она выводит IPv6-адрес и соответствующий MAC-адрес компьютера PC2.

Пример 16.7. Команда `show ipv6 neighbors` на маршрутизаторе R2

```
R2# show ipv6 neighbors
IPv6 Address                 Age Link-layer Addr State Interface
FE80::11FF:FE11:1111           0 0200.1111.1111 STALE Gi0/0
FE80::22FF:FE22:2222           1 0200.2222.2222 STALE Gi0/0
2001:DB8:1111:3::22            0 0200.2222.2222 REACH Gi0/0
FE80::D68C:B5FF:FE7D:8200      1 d48c.b57d.8200 DELAY Gi0/0
2001:DB8:1111:3::33            0 0200.1111.1111 REACH Gi0/0
2001:DB8:1111:3::3             0 d48c.b57d.8200 REACH Gi0/0
```

Поиск и устранение неисправностей IPv6

Предположим, что вы работаете с корпоративной сетью среднего размера, использующей протокол IPv6. Все работает нормально, вы каждый день возвращаетесь домой вовремя, и жизнь хороша. Но вот в один прекрасный день вы приходите на работу и получаете сообщение о проблеме с сетью. Что же вы делаете? Вы вводите несколько команд, пытаетесь изолировать проблему и в конечном счете находите первопричину неисправности. Возможно, у пользователя возникла проблема, и сотрудник "помог", задав на его компьютере статические параметры IPv6, допустив опечатку в IPv6-адресе стандартного маршрутизатора.

Далее в этой главе представлено семь случаев поиска и устранения неисправностей IPv6, в которых инженер только что приступил к решению проблемы. В каждом случае подразумевается, что инженер установил наличие проблемы в конкретной части сети или определенный набор первопричин.

Ниже в каждом случае обсуждаются потенциальные первопричины, выявляемые по определенным наборам признаков, а также приведено их краткое описание.

Прежде чем переходить к конкретным случаям, рассмотрим следующие три списка нескольких важных фактов, которые должны иметь место в рабочей сети IPv6. Первопричиной большинства рассматриваемых в этом разделе неисправностей является нарушение одного из этих правил.

Проблемы на хосте



1. Хосты должны располагаться в той же подсети IPv6, что и их стандартный маршрутизатор.

2. Хосты должны использовать такую же длину префикса, как и их стандартный маршрутизатор.
3. Параметр стандартного маршрутизатора на хостах должен содержать адрес реального маршрутизатора.
4. На хосте должен быть задан правильный адрес сервера DNS (службы доменных имен).

Ключевая тема **Проблемы на маршрутизаторе**

1. Используемые интерфейсы маршрутизатора должны быть в состоянии up/up.
2. Два маршрутизатора, соединенных с тем же каналом связи, должны иметь адреса из той же подсети IPv6.
3. Маршрутизаторы должны иметь маршруты IPv6 ко всем подсетям IPv6 согласно проекту подсетей IPv6.

Ключевая тема **Проблемы фильтрации**

1. Контроль фильтрации MAC-адресов на коммутаторах LAN.
2. Контроль пропущенных VLAN на коммутаторах.
3. Контроль списков управления доступом IPv6 (ACL) на маршрутизаторах.

Прежде чем мы перейдем к конкретным случаям, обдумайте все элементы этих списков. Как можно заметить, эти концепции применимы и к IPv4, и к IPv6. Таким образом, концептуально процесс поиска неисправностей IPv6, до некоторой степени, совпадает с таковым у IPv4. Конечно, в деталях они отличаются, и следующие сценарии упоминают эти различия.

Теперь перейдем к разнообразным признакам проблем IPv6!

Команда `ping` на хосте срабатывает лишь в некоторых случаях

Реагируя на новое сообщение о проблеме, наш сетевой инженер звонит пользователю и просит его ввести несколько команд IPv6 `ping` на своем компьютере. Одни команды завершатся успешно, другие — нет. Что делать дальше?

Откровенно говоря, если на настоящий момент задать этот вопрос десяти опытным сетевым инженерам, то, вероятно, будет предложено пять или шесть разных советов о последующих действиях. Когда одни команды `ping` на хосте срабатывают, а другие нет, одним из наиболее эффективных следующих шагов является проверка параметров хоста IPv6.

Статические параметры IPv6 на хосте являются одним из мест наиболее вероятного нахождения проблем, результатом некоторых из которых и является признак "одни команды `ping` срабатывают, а другие нет". Во-первых, числа очень длинные, и в них очень просто допустить опечатку. Во-вторых, следует знать правильные значения адресов стандартного маршрутизатора и сервера DNS. И наконец, когда отвечаете на экзаменационный вопрос, помните, что для создания нового вопроса можно варьировать не так много параметров, поэтому приходится только изменять рисунок и несколько чисел. Таким образом, как и в случае IPv4, необходимо быть готовым проверить параметры хоста IPv6.

Все элементы, которые должны иметь правильные значения, приведены на рис. 16.13. Эти концепции практически совпадают с таковыми у протокола IPv4.

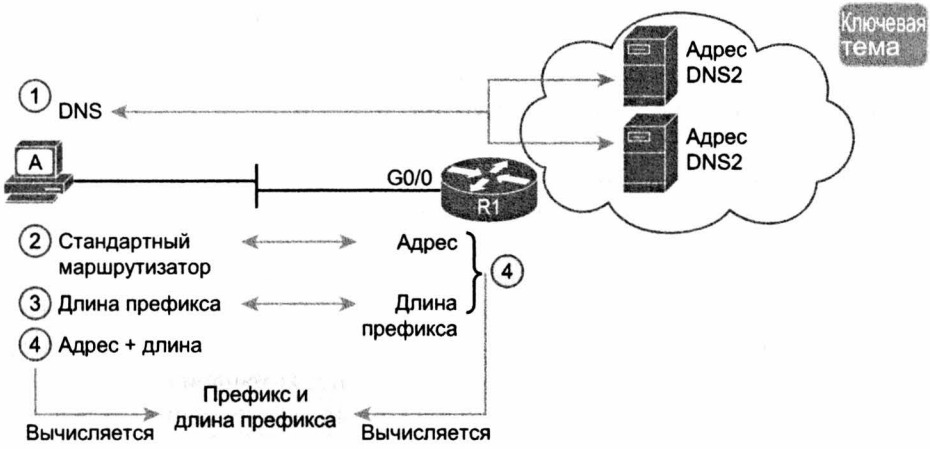


Рис. 16.13. Параметры IPv6 хоста по сравнению со значениями, которым они должны соответствовать

Затем обдумайте результаты команд `ping`, подразумевая, что неправилен только один из параметров. (Если неправильны несколько параметров, то признаки неисправности окажутся существенно сложнее, чем можно описать здесь.) Вот список параметров, указанных на рисунке.

1. При единственном неправильном параметре адреса DNS неудачу будут терпеть команды `ping`, обращающиеся к хосту по имени, а обращающиеся по IPv6-адресу окажутся успешны (имеется в виду, что никаких других проблем нет).
2. При единственном неправильном параметре стандартного маршрутизатора успешны команды `ping` для IPv6-адресов в локальной сети, а запросы к адресам вне подсети (через стандартный маршрутизатор) отказывают. Кроме того, поскольку откажет преобразование имен, неудачу потерпят все запросы с использованием имен.
3. Если не совпадают длины префикса, хост и маршрутизатор не согласуют подсети в локальной сети (см. следующий пункт).
4. Если хост и маршрутизатор не согласуют подсети IPv6 в сетях VLAN, маршрутизаторы не смогут перенаправлять пакеты назад хосту. В результате появятся те же признаки неисправностей, что и во втором пункте.

На экзамене эти признаки следует распознавать максимально быстро. Таким образом, если в вопросе даны параметры хоста, проверьте адрес интерфейса маршрутизатора, длину префикса и адрес сервера DNS, поскольку это должно занять минимум времени.

С точки зрения поиска и устранения неисправностей все эти признаки можно сократить до двух основных наборов.

- Неудачны команды `ping`, использующие имена.

- Неудачны команды `ping` к адресам вне подсети.

Первый из этих двух наборов признаков указывает на некую проблему DNS, а второй — на проблему стандартного маршрутизатора или несогласованности подсетей.

Неудачны команды `ping` от хоста к его стандартному маршрутизатору

Теперь второй случай. Инженер проверил командами хост и его стандартный маршрутизатор. Все параметры IPv6 на хосте и стандартном маршрутизаторе выглядят правильно. Но когда пользователь вводит команды `ping` с хоста на дальние серверы, и по имени, и по IPv6-адресу, они заканчиваются отказом.

На следующем этапе сетевой инженер пытается сузить область вероятной проблемы несколькими локальными командами `ping`. Инженер просит пользователя ввести на хосте команду `ping` с IPv6-адресом стандартного маршрутизатора. Команда терпит неудачу. Инженер пытается проверить командой `ping` со стандартного маршрутизатора хост пользователя, и эта команда также терпит неудачу.

Таким образом, команде `ping` с хоста недоступен его стандартный маршрутизатор, или наоборот. При таких начальных признаках проблемы возникает вопрос: что могло привести к этим признакам? Что, например, мешает команде `ping` с хоста B на рис. 16.14 получить доступ к маршрутизатору R3 даже при правильных параметрах IPv6 на хосте и маршрутизаторе?

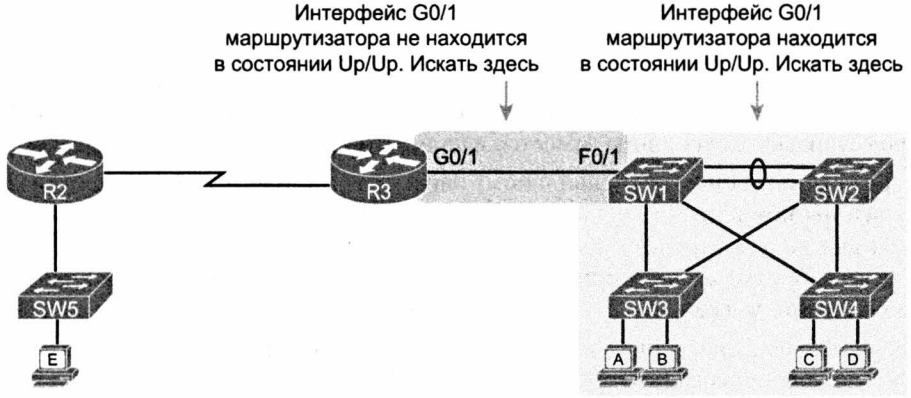


Рис. 16.14. Где искать источник неисправности на основании состояния интерфейса LAN маршрутизатора

Для поиска причины этой неисправности инженеру стоит оставить в покое IPv6 и обдумать сеть LAN между хостом и маршрутизатором. В частности, вероятные первопричины можно разделить на следующие категории.

Ключевая тема

Категории проблем, препятствующих успеху команды `ping` с хоста IPv6 на его стандартный маршрутизатор

1. Интерфейс LAN маршрутизатора или хоста административно отключен.
2. В сети LAN есть некая проблема, препятствующая передаче фреймов Ethernet.

3. В сети LAN есть фильтрация (например, защита порта), отфильтровывающая фреймы Ethernet.

В первом случае маршрутизатору и хосту можно приказать прекратить использовать интерфейс. На маршрутизаторе, конечно, можно использовать подкоманду интерфейса `shutdown`; если бы интерфейс G0/1 маршрутизатора R3 был в настоящий момент отключен, результат команды `ping` был бы именно таким, как описано здесь. У хостов также есть способы отключать и включать их интерфейсы, что также привело бы к тому же набору признаков. Каково же решение? Использовать на маршрутизаторе команду `no shutdown` или включить интерфейс на хосте.

Проблемы LAN во втором случае подробно обсуждались в первой части этой книги. Но вот совет по поиску и устранению неисправностей: если интерфейс G0/1 маршрутизатора R3 находится в состоянии down/down, проблема LAN, вероятно, кроется в канале связи Ethernet, непосредственно подключенном к интерфейсу G0/1 маршрутизатора R3. Но если интерфейс G0/1 маршрутизатора R3 находится в состоянии up/up, то проблема, вероятно, кроется в другом месте, а не в самой LAN. Если команда `ping` все еще не срабатывает, вернитесь к главе 3.

Что касается третьего случая, то вполне может статься так, что некий механизм фильтрации (например, защита порта) целенаправленно фильтрует фреймы, посланные хостом (B) или маршрутизатором (R3 G0/1). Кроме того, на интерфейсе G0/1 маршрутизатора R3 может быть установлен входящий список ACL IPv6, который, к сожалению, фильтрует входящие пакеты ICMPv6 и отбрасывает входящие пакеты, посланные командой `ping`.

Проблемы использования любых функций, требующих преобразования DNS

В третьем случае поиска и устранения неисправностей инженер исследует проблему хоста C. Команда `ping` с хоста C на Server1 терпит неудачу с именем хоста, но команда `ping` с IPv6-адресом сервера Server1 вполне успешна. Инженер повторяет команды `ping` для другого сервера (Server2) и получает те же результаты: с именем хоста — отказ, с IPv6-адресом — успех.

Эти признаки вполне однозначно указывают на некую проблему преобразования имен. Но это не определяет конкретную первопричину, которую инженер может исправить и восстановить работоспособность хоста пользователя. В данном случае первопричины могут относиться к следующим категориям.

Категории проблем, препятствующих использованию хостами IPv6 функций сервера DNS

Ключевая тема

1. На хосте статически задан неправильный параметр сервера DNS.
2. По протоколу DHCPv6 (с фиксацией состояния или без) хост получил неправильный параметр сервера DNS.
3. Между хостом пользователя и сервером DNS есть проблема соединения IPv6.

Что касается первой указанной здесь первопричины, то, если на хосте неправильно задан параметр сервера DNS, хост посылает запросы DNS по неправильному адресу. В результате хост не получает ответа от сервера DNS и не может узнать

IPv6-адрес хоста получателя. Первопричина? Кто-то ввел неправильную информацию в параметры конфигурации IPv6 хоста.

Вторая первопричина в списке подобна первой, но отличается от нее достаточно, чтобы стать отдельной категорией. На компьютере пользователя неправильный параметр сервера DNS, но получил он его значение, используя протокол DHCPv6. Признаки в основном те же, но первопричины разные. Напомним, что при использовании на хосте и протокола DHCPv6 с фиксацией состояния, и технологии SLAAC адрес сервера DNS изучается по протоколу DHCPv6.

Третья первопричина требует более подробного обсуждения и примера. Пример на рис. 16.15 демонстрирует двухэтапный процесс проверки хостом C сервера Server1 командой `ping Server1`. На первом этапе пакеты IPv6 должны поступить с хоста C на сервер DNS и вернуться назад с преобразованным в IPv6-адрес именем Server1. На втором этапе пакеты IPv6 могут передаваться на IPv6-адрес сервера Server1.

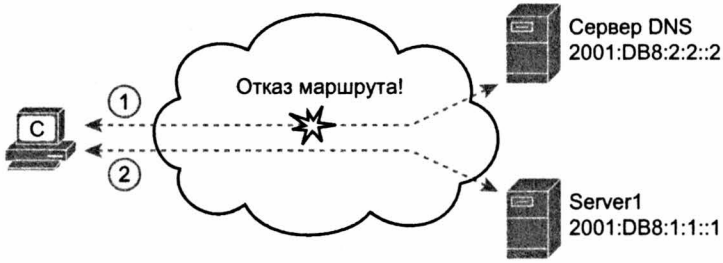


Рис. 16.15. Преобразование имен перед передачей пакетов на сервер

В зависимости от топологии сети внутри облака может существовать проблема подключения между хостом C и сервером DNS, а между хостом C и сервером Server1 никакой такой проблемы может и не быть. Таким образом, при симптоме "не работает преобразование имен" и правильном адресе сервера DNS на хосте начните с проверки подключения IPv6 между хостом и сервером DNS.

На хосте отсутствуют параметры IPv6: проблемы протокола DHCP с фиксацией состояния

В следующем случае наш сетевой инженер решает проблему пользователя хоста D. Инженер позвонил и попросил пользователя ввести несколько команд и установил, что хост пытается динамически изучать свои параметры IPv6 и что у хоста еще нет одноадресатного IPv6-адреса.

Предположим, что в данной сети используется стратегия назначения IPv6-адресов по протоколу DHCPv6. Инженеру известно об этой стратегии, поэтому он задается вопросом: почему процесс потерпел неудачу? Данный случай рассматривает некоторые потенциальные первопричины простых ошибок.

ВНИМАНИЕ!

В этой книге не учитываются некоторые подробности процесса использования хостом технологии SLAAC и протокола DHCPv6 с фиксацией состояния. Для простоты обсуждения данной темы подразумевается, что используется только протокол DHCP с фиксацией состояния.

Поиск и устранение неисправностей протокола DHCP с фиксацией состояния следует той же базовой логике, что и у протокола DHCP IPv4, обсуждавшегося в главе 5. Таким образом, чтобы успешно использовать протокол DHCPv6 (как с фиксацией состояния, так и без нее) для получения хостом информации с сервера DHCPv6, подходят те же правила, что и изложенные в главе 5.

Требования для правильной работы протокола DHCPv6

Ключевая тема

1. Сервер находится в той же подсети, что и клиент.
   Или
2. Сервер может находиться в другой подсети.
   A. Маршрутизатор, находящийся в той же подсети, что и хост клиента, реализует ретранслятор DHCP.
   B. Подключение IPv6 между этим локальным маршрутизатором (маршрутизатор возле клиентского хоста) и сервером DHCPv6 вполне работоспособно.

Двумя наиболее вероятными первопричинами, препятствующими динамическому изучению хостом своих параметров IPv6 по протоколу DHCPv6 с фиксацией состояния, являются пункты 2A и 2B списка. В случае 2A для решения требуется ввести команды конфигурации на соответствующих интерфейсах в каждой сети LAN, подключенной к серверу DHCPv6. Например, на рис. 16.16 хост D находится в подсети LAN слева, и интерфейс G0/0 маршрутизатора R1 подключен к той же подсети. Для включения функции ретранслятора DHCP IPv6, указывающего на сервер DHCPv6 справа, на маршрутизаторе R1 нужно ввести команду, показанную на рис. 16.16, *снизу*.

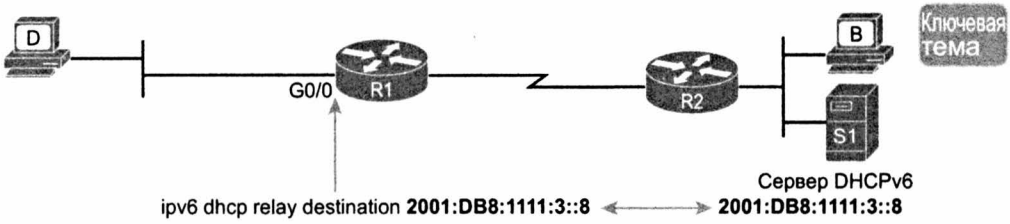


Рис. 16.16. Ретранслятор DHCP IPv6

Если пропустить команду `ipv6 dhcp relay` на маршрутизаторе R1 или указать неправильный IPv6-адрес, то попытки хоста D использовать сервер DHCPv6 окажутся неудачными.

Пункт 2B не является фактически первопричиной. Это только другой признак проблемы, нуждающийся в дальнейшем исследовании. Для передачи сообщений DHCPv6 между маршрутизатором R1 и сервером DHCPv6 должно существовать подключение. (Отправителем запросов DHCPv6 маршрутизатор R1 указывает исходящий интерфейс посланного сообщения, а не обязательно тот же интерфейс, где введена команда `ipv6 dhcp relay`; в данном случае маршрутизатор R1 использовал бы IPv6-адрес своего последовательного интерфейса.) Команда `ping` с маршрутизатора R1 по IPv6-адресу сервера DHCPv6 — наилучший способ проверки этой проблемы.

На хосте отсутствуют параметры IPv6: проблемы SLAAC

В пятом случае поиска и устранения неисправностей симптомы те же, что и в предыдущем случае, но для присвоения IPv6-адреса предприятие использует технологию SLAAC, а не протокол DHCPv6 с фиксацией состояния. Проведя обследование, инженер обнаружил, что хост D не изучил свой IPv6-адрес. Так что же могло помешать технологии SLAAC? Итак, рассмотрим потенциальные первопричины.

Чтобы понять некоторые из первопричин этой проблемы, рассмотрим сначала три этапа получения хостом параметров IPv6 при использовании технологии SLAAC.

1. Для получения от маршрутизатора в той же подсети префикса, его длины и адреса стандартного маршрутизатора используется протокол NDP.
2. Для формирования собственного IPv6-адреса хост использует правила SLAAC локально (никаких сетевых сообщений ненужно).
3. Для получения адресов серверов DNS от сервера DHCPv6 используется протокол DHCPv6 без фиксации состояния.

На первом из этих этапов используется *запрос на получение информации о наличии маршрутизатора* (Router Solicitation — RS) протокола NDP, на который маршрутизатор отвечает *анонсом маршрутизатора* (Router Advertisement — RA) протокола NDP, как показано на рис. 16.17. Сообщение RS, посланное на многоадресатный IPv6-адрес маршрутизатора FF02::2, должно попасть на все маршрутизаторы IPv6 в той же сети VLAN на рисунке, что и хост D. В данном случае маршрутизатор R1 отвечает сообщением, содержащим его IPv6-адрес (чтобы хост D использовал его как адрес стандартного маршрутизатора), а также префикс и его длину для использования хостом D.

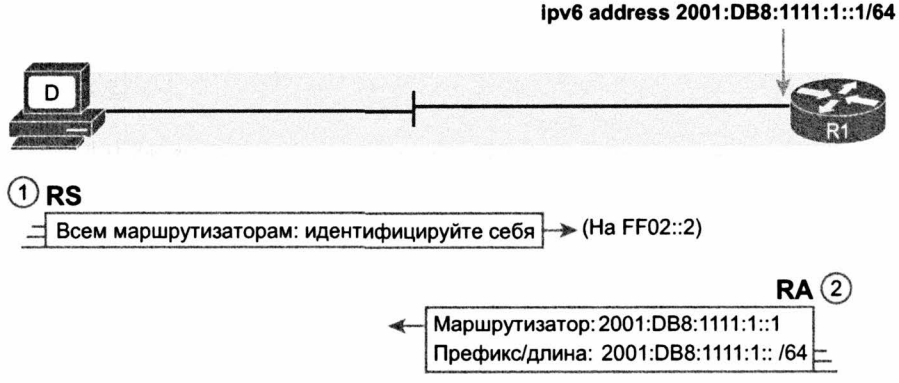


Рис. 16.17. Процесс NDP RS и RA

Хосты, использующие технологию SLAAC, полагаются на информацию в сообщении RA. Таким образом, когда при использовании технологии SLAAC хост не в состоянии получить эти три параметра, включая IPv6-адреса, возникает вполне резонный вопрос: что могло помешать процессу RS/RA протокола NDP? Ниже приведен список потенциальных первопричин.

Причины отказа процесса RS/RA протокола NDP между хостом и маршрутизатором



1. Нет подключения LAN между хостом и любым маршрутизатором в подсети.
2. На маршрутизаторе отсутствует подкоманда интерфейса `ipv6 address`.
3. На маршрутизаторе отсутствует глобальная команда конфигурации `ipv6 unicast-routing`.

Первая причина вполне очевидна. Если локальная сеть не может перенаправлять фреймы Ethernet с хоста на маршрутизатор (или наоборот), то сообщения RS и RA протокола NDP не могут быть доставлены.

Что касается второй причины, то для ответа на сообщение RS у маршрутизатора должна быть команда `ipv6 address`, которая не только разрешает протокол IPv6 на интерфейсе, но и определяет информацию, передаваемую маршрутизатором в сообщении RA. Например, на рис. 16.17 маршрутизатор R1 был настроен командой `ipv6 address 2001:db8:1111:1::1/64`. Эта команда непосредственно вводит две части информации, предоставляемой маршрутизатором R1 в сообщении RA, а для вычисления префикса IPv6 маршрутизатор R1 использует адрес и длину префикса.

Третья первопричина в списке может быть самой удивительной: маршрутизатор должен разрешить маршрутизацию IPv6 глобальной командой `ipv6 unicast-routing`. Почему? Без этой команды маршрутизаторы Cisco даже не будут пытаться маршрутизировать пакеты IPv6. Без нее маршрутизатор не считает себя маршрутизатором IPv6 и не отвечает на сообщения RS с RA протокола NDP.

Команда `traceroute` демонстрирует несколько транзитных участков, а затем отказ

Шестой случай поиска и устранения неисправностей переходит от проблем хоста к проблемам маршрутизации IPv6 на маршрутизаторе.

В данном случае инженеру сообщили, что хост не может соединиться с сервером. Понятно, что команда `ping` с хоста на сервер неудачна, поэтому инженер уже выполнил несколько действий, обсуждавшихся ранее в этой главе.

- Параметры IPv6 хоста выглядят нормально.
- Параметры стандартного маршрутизатора и сервера DNS на хосте соответствуют действительности.
- Команда `ping` с хоста на его стандартный маршрутизатор успешна.

Инженер еще раз звонит пользователю и просит его ввести команду `traceroute` с IPv6-адресом сервера. Команда `traceroute` выводит некий набор маршрутизаторов, а затем приостанавливается, пока пользователь не прервет ее выполнение. Каковы первопричины такого поведения? Обычно, но не всегда, эти признаки указывают на некую проблему маршрутизации IPv6. Ниже обсуждаются некоторые из потенциальных первопричин этих проблем маршрутизации.

Проблемы маршрутизации имеют много причин. Одни связаны с отсутствием маршрутов на маршрутизаторе (возможно много конкретных первопричин), другие — с наличием у маршрутизатора неправильного маршрута. Ниже приведен спи-

сок лишь некоторых из причин, по которым у маршрутизатора может отсутствовать необходимый маршрут или быть неправильный маршрут.

Ключевая тема

Возможные причины проблем маршрутизации IPv6

- Нарушены каналы связи между маршрутизаторами.
- Проблемы с протоколом маршрутизации у соседа.
- Фильтрация пакетов протокола маршрутизации препятствует добавлению маршрута в таблицу маршрутизации IPv6.
- Из-за неправильно заданных статически маршрутов пакеты поступают не на тот следующий маршрутизатор.
- Из-за плохого проекта подсети сдублированы в разных областях сети, что ведет к ложному анонсированию подсети.

Рассмотрим рис. 16.18. Команда `ping` на хосте A терпит неудачу при попытке обращения к хосту C, находящемуся в подсети 33 (2001:DB8:1:33::/64). Команда `traceroute` с хоста A для хоста C выводит IPv6-адреса маршрутизатора R1 и R2, но затем приостанавливается и не завершает работу самостоятельно.

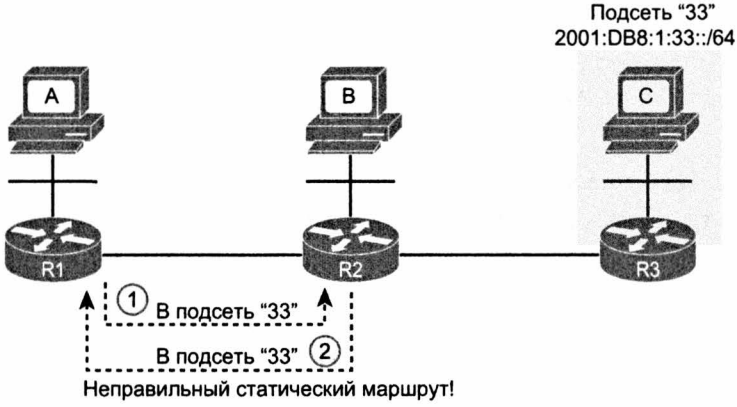


Рис. 16.18. Неправильный статический маршрут создает петлю

Как можно заметить по надписям на рисунке, проблема маршрутизации связана с неправильным статическим маршрутом к маршрутизатору R2. Хост A вполне может перенаправить пакеты IPv6 своему стандартному маршрутизатору R1. Маршрутизатор R1 вполне может правильно перенаправить пакеты, посланные с хоста C на маршрутизатор R2. Но у маршрутизатора R2 неправильный статический маршрут к подсети 33, указывающий назад на маршрутизатор R1.

Что касается других первопричин проблем маршрутизации, то возьмите список и проверьте их также. Проверьте на маршрутизаторах интерфейсы, которые должны быть в состоянии up, и удостоверьтесь в их работоспособности. Проведите поиск и устранение неисправностей для своего протокола маршрутизации. (Поиск и устранение неисправностей для протоколов OSPFv3 и EIGRPv6 обсуждаются в главах 17 и 18 соответственно.) Учтите также возможность неправильной настройки интерфейса маршрутизатора, в результате чего протоколы маршрутизации анонсируют тот же

номер подсети как существующий в двух местах, что нарушает правила проекта на бумаге и вызывает ошибки маршрутизации пакетов к хостам в этой подсети IPv6.

Маршрутизация выглядит хорошо, но команда `traceroute` все еще терпит неудачу

Последний случай сосредоточивается на одной конкретной первопричине: списке управления доступом IPv6 (ACL).

Как уже известно, команды `ping` и `traceroute` могут засвидетельствовать наличие проблемы маршрутизации. Когда они демонстрируют, что хост может перенаправить пакет по крайней мере на стандартный маршрутизатор, но не конечному получателю, то проблема, вероятно, относится к одной из следующих двух категорий:

- проблема в маршрутизации;
- маршрутизация работает, но некий фильтр (например, список ACL IPv6) отбрасывает пакеты.

Хотя списки ACL IPv6 не рассматриваются ни в этой книге, ни в книге по ICND1, в первом томе обсуждались списки ACL IPv4. Списки ACL IPv6 работают почти так же, но фильтруют они, конечно, пакеты IPv6, а не пакеты IPv4. Конфигурация ACL IPv6 содержит список операторов, каждый из которых соответствует диапазону IPv6-адресов отправителя, получателя, номера порта и т.д. Список ACL может фильтровать пакеты IPv6, поступающие на интерфейс или покидающие его.

Например, на рис. 16.19 представлена одна строка списка ACL IPv6 (с правильным синтаксисом). Строка списка ACL IPv6 определяет диапазон адресов отправителя и получателя как пару адрес/префикс, подобно подкоманде интерфейса `ipv6 address`. Чтобы фильтровать трафик Telnet, следующий из подсети 1 в подсеть 3 этой сети, следует добавить список ACL в одну из четырех областей, отмеченных стрелками на рисунке. (Обратите внимание, что для разрешения другого трафика список ACL нуждается в некоторых других операторах.)

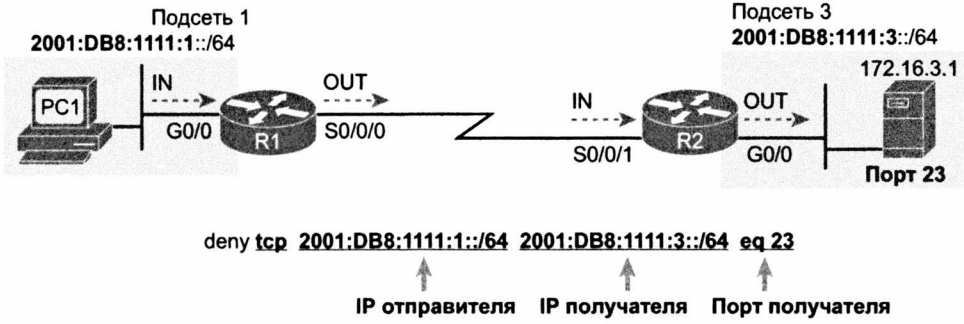


Рис. 16.19. Фильтрация пакетов IPv6 на основании порта получателя

Перед дальнейшим изучением поиска и устранения неисправностей обратите более пристальное внимание на однострочный пример списка ACL. Диапазон адресов основан на префиксе IPv6 (подсети), вычисляемом на основании адреса и длины префикса. В результате этот список ACL определяет диапазон всех адресов в подсети 1 (2001:DB8:1111:1::/64), т.е. подсети отправителя, и диапазон всех адре-

сов в подсети 3 (2001:DB8:1111:3::/64), т.е. подсети получателя. В строке указан также порт получателя 23 (Telnet). Таким образом, при действии deny (запрет) эта команда ACL отбросит трафик Telnet IPv6.

Теперь вернемся к поиску и устранению неисправностей. Короче говоря, когда есть признаки, напоминающие проблему маршрутизации, выясните, были ли применены какие-нибудь списки ACL IPv6. Проверить наличие любых списков ACL на маршрутизаторах IPv4 можно командой `show ip interface`, а на маршрутизаторах IPv6 — командой `show ipv6 interface`. Пример 16.8 демонстрирует эту команду на маршрутизаторе, а выделенная строка свидетельствует об отсутствии списков ACL IPv6.

Пример 16.8. Команда `show ipv6 interface` на маршрутизаторе R2

```
R2# show ipv6 interface
Serial0/0/0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::FF:FE00:1
  No Virtual link-local address(es):
  Global unicast address(es):
    2001:DB8:1:12::1, subnet is 2001:DB8:1:12::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::5
    FF02::1:FF00:1
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
  Output features: Access List
  Outgoing access list book
! Строки опущены для краткости
```

Обзор

Резюме

- Протокол IPv6 определяет два главных типа одноадресатных IPv6-адресов.
- Глобальные одноадресатные адреса подобны открытым IPv4-адресам. Получив уникальный префикс, предприятие начинает все свои адреса с этого префикса.
- Уникальные локальные одноадресатные адреса больше похожи на частные адреса.
- Префикс, присвоенный предприятию провайдером ISP, должен быть использован во всех IPv6-адресах этого предприятии, как часть сети в IPv4-адресе.
- Для обмена пакетами IPv6 с другими хостами хосты могут использовать глобальные одноадресатные и уникальные локальные одноадресатные адреса.
- У хостов IPv6 есть три основные возможности установки параметров IPv6: статическая конфигурация, протокол DHCP с фиксацией состояния и SLAAC.
- Протокол DHCPv6 с фиксацией состояния следует тем же общим принципам, что и протокол DHCP для IPv4 (DHCPv4).
- Автоматическая настройка адреса без фиксации состояния — это один из способов получения хостом своего префикса /64.
- Если хост использует правила EUI-64, созданный хостом адрес может быть предсказан. Префиксная часть адреса — это префикс определенный на локальном маршрутизаторе IPv6. Далее, согласно правилам EUI-64, 48-битовый MAC-адрес хоста преобразуется в 64-битовый идентификатор интерфейса.
- Статические маршруты IPv6 предоставляют маршрутизаторам три основные возможности указания направления дальнейшей передачи пакетов.
- Для отображения конкретного маршрута IPv6 маршрутизатору достаточно послать пакеты на определенный адрес получателя, используя команду `show ipv6 route` *адрес*.
- При поиске и устранении неисправностей сети инженер ищет проблемы на хосте и на маршрутизаторе.
- Первопричины проблем DNS могут относиться к следующим категориям: на хосте статически задан неправильный параметр сервера DNS, по протоколу DHCPv6 (с фиксацией состояния или без нее) получен неправильный параметр сервера DNS, между хостом и сервером DNS есть проблема соединения.
- Строка списка ACL IPv6 определяет диапазон адресов отправителя и получателя как пару адрес/префикс.

Ключевые темы

Повторите все ключевые темы данной главы, отмеченные пиктограммой "Ключевая тема". Ключевые темы и соответствующие им страницы перечислены в табл. 16.2.

Таблица 16.2. Ключевые темы главы 16

Элемент	Описание	Страница
Табл. 16.1	Типы одноадресатных IPv6 адресов	528
Рис. 16.5	Источники параметров IPv6 при использовании протокола DHCP с фиксацией состояния	529
Рис. 16.7	Источники параметров IPv6 при использовании SLAAC	530
Список	Этапы создания адреса с использованием SLAAC и EUI-64	530
Рис. 16.8	Формат IPv6-адреса с идентификатором интерфейса и частью EUI-64	531
Список	Этапы настройки IPv6 адресации и маршрутизации	531
Список	Проблемы на хосте	537
Список	Проблемы на маршрутизаторе	538
Список	Проблемы фильтрации	538
Рис. 16.13	Параметры IPv6 хоста по сравнению со значениями, которым они должны соответствовать	539
Список	Категории проблем, препятствующих успеху команды ping с хоста IPv6 на его стандартный маршрутизатор	540
Список	Категории проблем, препятствующих использованию хостами IPv6 функций сервера DNS	541
Список	Требования для правильной работы протокола DHCPv6	543
Рис. 16.16	Ретранслятор DHCP IPv6	543
Список	Причины отказа процесса RS/RA протокола NDP между хостом и маршрутизатором	545
Список	Возможные причины проблем маршрутизации IPv6	546

Заполните таблицы и списки по памяти

Распечатайте приложение Г с веб-сайта или его раздел, относящийся к этой главе, и заполните таблицы и списки по памяти. В приложении Д приведены заполненные таблицы и списки для самоконтроля.

Ключевые термины

После первого прочтения главы попытайтесь дать определения следующим ключевым терминам. Но не расстраивайтесь, если не все получится сразу, в главе 22 описано, как использовать эти термины на завершающем этапе подготовки к экзамену.

протокол обнаружения соседних устройств (Neighbor Discovery Protocol — NDP), запрос на получение информации о наличии маршрутизатора (Router Solicitation — RS), анонс маршрутизатора (Router Advertisement — RA), запрос соседа (Neighbor Solicitation — NS), анонс соседа (Neighbor Advertisement — NA), автоматическая настройка адреса без фиксации состояния (Stateless Address Autoconfiguration — SLAAC), DHCP без фиксации состояния (stateless DHCP), глобальный одноадресатный адрес (global unicast address), уникальный локальный одноадресатный адрес (unique local unicast address), адрес, локальный в пределах канала связи (link-local address), EUI-64, двойной стек (dual stack)

Таблицы команд

Хоть и не обязательно заучивать информацию из таблиц данного раздела, ниже приведен список команд конфигурации и пользовательских команд главы. Фактически команды стоит запомнить, чтобы лучше понять содержимое главы и выполнить задания по подготовке к экзамену. Чтобы проверить, насколько хорошо вы запомнили команды, закройте левую сторону таблицы листом бумаги, читайте описания с правой стороны и пытайтесь вспомнить команду.

Таблица 16.3. Конфигурационные команды главы 16

Команда	Описание
`ipv6 unicast-routing`	Команда глобального режима конфигурирования, включающая маршрутизацию протокола IPv6 на маршрутизаторе
`ipv6 address {`*`ipv6-адрес/длина-префикса`*` |` *`название-префикса суббиты/длина-префикса`*`} [eui-64]`	Подкоманда интерфейса, вручную задающая либо весь IP-адрес интерфейса, либо префикс /64, а маршрутизатор автоматически создает идентификатор интерфейса в формате EUI-64
`ipv6 dhcp relay destination` *`адрес_сервера`*	Подкоманда интерфейса, разрешающая работу агента пересылки DHCP IPv6
`ipv6 router ospf` *`идентификатор_процесса`*	Переводит в режим конфигурации OSPFv3 для выбранного процесса
`router-id` *`идентификатор`*	Подкоманда OSPF, статически устанавливающая идентификатор маршрутизатора
`ipv6 ospf` *`идентификатор_процесса`* `area` *`номер_области`*	Подкоманда интерфейса, разрешающая на интерфейсе протокол OSPFv3 для конкретного процесса и определяющая область OSPFv3

Таблица 16.4. Команды EXEC главы 16

Команда	Описание
`show ipv6 route [ospf | connected | static]`	Выводит маршруты в таблице маршрутизации, изученные по протоколу OSPFv3
`show ipv6 ospf`	Отображает параметры протокола маршрутизации и текущие значения таймеров для OSPFv3, а также идентификатор маршрутизатора OSPFv3
`show ipv6 ospf interface brief`	Выводит по одной строке на каждый интерфейс, поддерживающий протокол OSPFv3, а также такие базовые параметры, как процесс OSPFv3, номер области и стоимость интерфейса
`show ipv6 interface [`*`тип номер`*`]`	Выводит параметры IPv6 на интерфейсе, включая локальные для канала связи и другие одноадресатные IP-адреса
`show ipv6 ospf neighbor [`*`RID_соседа`*`]`	Выводит соседей и их текущее состояние для каждого интерфейса, а дополнительно выводит подробности по указанному в команде идентификатору маршрутизатора

Окончание табл. 16.4

Команда	Описание
`show ipv6 ospf database`	Выводит отчет об анонсах LSA в базе LSDB локального маршрутизатора, выводя по одной строке для каждого анонса LSA
`show ipv6 ospf`	Выводит множество фактов о процессе OSPF локального маршрутизатора, в частности, первая строка содержит идентификатор маршрутизатора
`show ipv6 protocols`	Выводит более краткую информацию, чем команда `show ip protocols` IPv4. Сначала перечисляются все средства, позволяющие маршрутизатору изучать или создавать маршруты IPv6 и на тех интерфейсах, на которых разрешен протокол маршрутизации
`ping {`*`имя_хоста`*` | `*`ipv6-адрес`*`}`	Проверяет маршруты IPv6, посылая пакеты ICMP на хост получателя
`traceroute {`*`имя_хоста`*` | `*`ipv6-адрес`*`}`	Проверяет маршруты IPv6, обнаруживая IP-адреса по маршруту между маршрутизатором и заданным получателем
`show ipv6 neighbors`	Выводит таблицу соседних устройств маршрутизатора IPv6
`show ipv6 routers`	Выводит все соседние маршрутизаторы, анонсировавшие себя сообщением NDP RA

Таблица 16.5. Команды хоста главы 16

Команда (Microsoft / Apple / Linux)	Описание
`ipconfig / ifconfig / ifconfig`	Выводит параметры интерфейса, включая IPv4- и IPv6-адреса
`ping / ping6 / ping6`	Проверяет маршруты IP, посылая пакет ICMPv6 на хост получателя
`tracert / traceroute6 / traceroute6`	Проверяет маршруты IPv6, обнаруживая IP-адреса по маршруту между маршрутизатором и заданным получателем
`netsh interface ipv6 show neighbors / ndp -an / ip -6 neighbor show`	Выводит таблицу соседних устройств хоста IPv6

ГЛАВА 17

Реализация протокола OSPF для IPv6

На настоящий момент читатели узнали достаточно много о протоколе OSPF версии 3 (OSPFv3). В книге по ICND1 рассматривались основные концепции протокола OSPFv3, его настройка и проверка. Кроме того, протокол OSPFv3 очень похож на протокол OSPFv2, как упоминалось в главах 8 и 11 этой книги при более подробном обсуждении протокола OSPFv2.

В этой главе собраны вместе все детали "пазла" OSPFv3, включая также и весь другой материал по протоколу OSPFv2. Поскольку практически все концептуальные элементы, необходимые для обсуждения протокола OSPFv3, уже известны, первый раздел этой главы сразу начинается с настройки. В нем содержится обзор тем по конфигурации протокола OSPFv3 из книги ICND1, а также несколько новых тем.

Второй главный раздел главы увязывает концепции OSPF с командами проверки. В данном разделе обсуждаются темы, связанные как с протоколом OSPFv2, так и OSPFv3, а также команды проверки, демонстрирующие реализацию этих концепций на маршрутизаторах. В то же время здесь затрагиваются общие первопричины проблем, связанных с протоколом OSPFv3, и объясняется, как распознать эти проблемы.

В этой главе рассматриваются следующие экзаменационные темы

Технологии маршрутизации IP
Настройка и проверка протокола OSPF (одиночная область)
- Соседские отношения
- Состояние OSPF
- Несколько областей
- Настройка OSPF v3
- Идентификатор маршрутизатора
- Типы сообщений LSA

Различия методов маршрутизации и протоколов маршрутизации
- Метрика
- Следующий транзитный узел

Поиск и устранение неисправностей
Поиск и устранение проблем OSPF
- Соседские отношения
- Таймеры Hello и Dead
- Область OSPF
- Максимальный блок передачи данных интерфейса
- Типы сетей
- Состояние соседей
- База данных топологии OSPF

Основные темы

Настройка протокола OSPFv3

Компания Cisco ожидает, что сдающий экзамен ICND1 будет знать некоторые подробности протокола OSPFv3, но для экзамена ICND2 следует помнить и все темы по протоколу OSPFv3 экзамена ICND1 и знать все новые темы. В первом из двух главных разделов этой главы рассматривается настройка протокола OSPFv3, содержится обзор тем по настройке из экзамена ICND1, а также дополнительные темы экзамена ICND2. К новым темам относится настройка конфигурации протокола OSPFv3 в многообластной архитектуре, параметры стоимости OSPF, балансировка нагрузки и введение в стандартные маршруты.

Краткий обзор конфигурации OSPFv3

Сначала рассмотрим темы экзамена ICND1, посвященные конфигурации протокола OSPFv3. Ниже описаны этапы настройки конфигурации протокола OSPFv3, включенные в экзамен ICND1.



Этапы настройки протокола OSPFv3

Этап 1 Используя глобальную команду `ipv6 router ospf` *идентификатор_процесса* в режиме конфигурации OSPF, создайте и введите номер текущего процесса OSPFv3

Этап 2 Удостоверьтесь, что у маршрутизатора есть также идентификатор маршрутизатора OSPF:

A. Введите подкоманду маршрутизатора `router-id` *значение_id*.

B. Задайте IP-адрес на петлевом интерфейсе (выберите самый большой IP-адрес из всех работающих петлевых интерфейсов).

C. Задайте IP-адрес интерфейса (выберите самый высокий IP-адрес из всех работающих не петлевых интерфейсов)

Этап 3 Введите одну или несколько подкоманд маршрутизатора `ipv6 ospf` *идентификатор_процесса* `area` *идентификатор_области* для каждого соответствующего интерфейса с разрешенным протоколом OSPFv3 и присвойте ему номер области

Этап 4 Используя подкоманду маршрутизатора `passive-interface` *тип номер*, настройте все интерфейсы OSPFv3 как пассивные, если на интерфейсе не могут или не должны быть обнаружены никакие соседи. (Необязательно)

Прежде чем переходить к рассмотрению многообластной конфигурации, уделим немного времени обсуждению экзаменационных тем по протоколу OSPF. Откровенно говоря, на момент написания этой книги экзаменационные темы по протоколу OSPF имели четкую разделительную линию необходимых знаний как раз по многообластной конфигурации OSPF (и OSPFv2, и OSPFv3). Экзаменационные темы по конфигурации однозначно подразумевают настройку только одиночной области, хотя темы по поиску и устранению неисправностей могут подразумевать наличие знаний по многообластной конфигурации. Хорошая новость: зная концеп-

ции многообластной конфигурации и конфигурации одиночной области, изучить настройку многообластной конфигурации невероятно просто. Таким образом, следующая тема посвящена подробностям многообластной конфигурации, которые на всякий случай на экзамене желательно знать.

Пример многообластной конфигурации OSPFv3

Многие из фактов о протоколе OSPFv3, представленные в этой главе, относятся и к протоколу OSPFv2. Таким образом, чтобы извлечь больше пользы из этого подобия, в данном разделе используется пример многообластной конфигурации с той же топологией объединенной сети, что и в примере, представленном в главе 8 о протоколе OSPFv2.

Рис. 17.1 начинает описание проекта конфигурации демонстрацией подсетей IPv6. На рисунке не показаны индивидуальные IPv6-адреса маршрутизатора, чтобы не загромождать рисунок, но для простоты адреса заканчиваются тем же числом, что и номер маршрутизатора. Например, все пять адресов интерфейсов маршрутизатора R1 заканчиваются на 1.

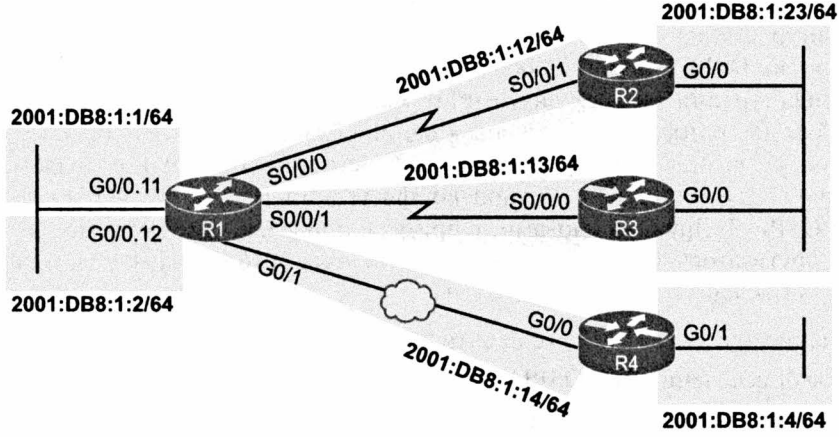


Рис. 17.1. Объединенная сеть для примера многообластной конфигурации OSPFv3

Далее, на рис. 17.2, представлен проект областей OSPFv3. Проект практически идентичен таковому на рис. 8.12, где представлен проект областей многообластной конфигурации примера главы 8. Маршрутизаторы R2 и R3 являются внутренними для области 23, маршрутизатор R4 является внутренним для области 4, а маршрутизатор R1 — *граничным маршрутизатором области* (Area Border Router — ABR), соединяющим все три области.

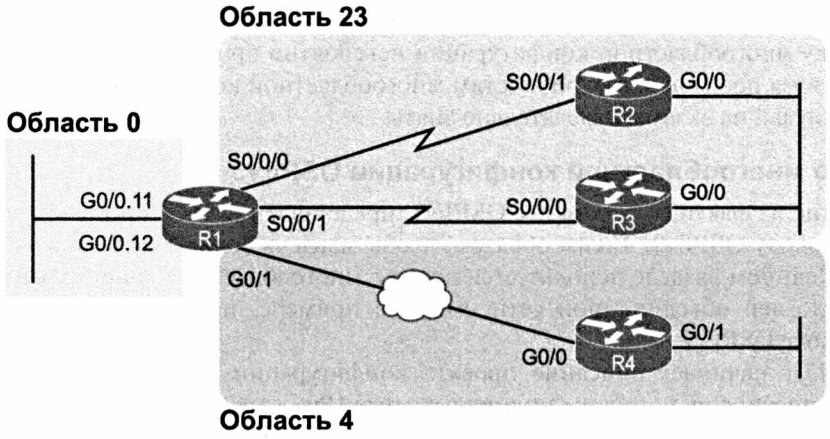


Рис. 17.2. Проект областей примера многообластной конфигурации OSPFv3

Конфигурация с одной областью на трех внутренних маршрутизаторах

Конфигурации на трех внутренних маршрутизаторах этого примера аналогичны конфигурации OSPF одиночной области уровня ICND1. В многообластном проекте OSPF конфигурации на всех внутренних маршрутизаторах (маршрутизаторы, все интерфейсы для которых подключены к одной области) являются конфигурациями одиночной области, поскольку все их интерфейсы находятся в одной области.

Пример 17.1 начинается с полной конфигурации IPv6 на маршрутизаторе R2, включая OSPFv3. Другими словами, в примере приведены все команды, необходимые маршрутизатору R2 для поддержки протокола IPv6. Обратите внимание, что в примере выделены следующие действия.

1. Создание процесса OSPFv3 с идентификатором процесса 2.
2. Явное определение RID OSPFv3 как 2.2.2.2.
3. Разрешение процесса 2 OSPFv3 на двух интерфейсах и помещение их в область 23.

Пример 17.1. Конфигурация IPv6 и OSPFv3 на внутреннем маршрутизаторе R2

```
ipv6 unicast-routing
!
interface GigabitEthernet0/0
mac-address 0200.0000.0002
ipv6 address 2001:db8:1:23::2/64
ipv6 ospf 2 area 23
!
interface serial 0/0/1
ipv6 address 2001:db8:1:12::2/64
ipv6 ospf 2 area 23
!
ipv6 router ospf 2
router-id 2.2.2.2
```

Сначала рассмотрим две команды, которые должны быть в каждой конфигурации OSPFv3: глобальную команду `ipv6 router ospf` *идентификатор_процесса* и подкоманду интерфейса `ipv6 ospf` *идентификатор_процесса* `area` *идентификатор_области*. Первая команда создает процесс OSPFv3 по номеру. Вторая команда, по одной на интерфейс, разрешает процесс OSPFv3 на интерфейсе и присваивает области номер. В данном случае у маршрутизатора R2 есть идентификатор процесса 2, а оба интерфейса присвоены области 23.

Теперь рассмотрим одно совершенно необязательное средство: пассивные интерфейсы OSPFv3. Они используют те же концепции и практически тот же синтаксис команд, что и в протоколе OSPFv2. Если маршрутизатор не должен формировать соседские отношения на интерфейсе, то он может быть сделан пассивным. В данном случае маршрутизатор R2 должен найти по крайней мере одного соседа OSPFv3 на каждом из двух его интерфейсов, поэтому конфигурация не включает команду `passive-interface` вообще.

И наконец, при установке идентификатора маршрутизатора OSPFv3 (RID) используются те же правила, что и у протокола OSPFv2. В данном случае маршрутизатор R2 устанавливает свой RID командой OSPFv3 `router-id`, но следует знать все три способа.

Конфигурация маршрутизатора R3, должна быть очень похожа на конфигурацию OSPFv3 маршрутизатора R2. Оба маршрутизатора внутренние в области 23, и у обоих есть по крайней мере один сосед на двух их интерфейсах соответственно. Таким образом, оба не могут сделать ни один из своих интерфейсов пассивным. Кроме того, лишь для демонстрации возможности использования соседями OSPFv3 разных значений идентификатора процесса, маршрутизатор R3 использует идентификатор процесса 3 OSPFv3, в то время как маршрутизатор R2 использует идентификатор процесса 2. Полученная конфигурация приведена в примере 17.2.

Пример 17.2. Конфигурация IPv6 и OSPFv3 на маршрутизаторе R3

```
ipv6 unicast-routing
!
interface GigabitEthernet0/0
mac-address 0200.0000.0003
ipv6 address 2001:db8:1:23::3/64
ipv6 ospf 3 area 23
!
interface serial 0/0/0
ipv6 address 2001:db8:1:13::3/64
ipv6 ospf 3 area 23
!
ipv6 router ospf 3
router-id 3.3.3.3
```

Конфигурация маршрутизатора R4 в примере 17.3 немного отличается от таковой у двух предыдущих маршрутизаторов. В первую очередь, маршрутизатор R4 вполне может сделать свой интерфейс G0/1 пассивным, поскольку он не собирается создавать соседские отношения OSPFv3 на этом интерфейсе LAN. Маршрутизатор R4 также использует другой идентификатор процесса OSPFv3.

ВНИМАНИЕ!

Хотя в этих примерах используются разные идентификаторы процесса OSPFv3 для демонстрации того, что это не создает проблем, большинство предприятий использует одинаковое значение идентификатора процесса на всех маршрутизаторах (для единообразия).

Пример 17.3. Конфигурация IPv6 и OSPFv3 на маршрутизаторе R4

```
ipv6 unicast-routing
!
interface GigabitEthernet0/0
mac-address 0200.0000.0004
ipv6 address 2001:db8:1:14::4/64
ipv6 ospf 4 area 4
!
interface GigabitEthernet0/1
ipv6 address 2001:db8:1:4::4/64
ipv6 ospf 4 area 4
!
ipv6 router ospf 4
router-id 4.4.4.4
passive-interface gigabitethernet0/1
```

Многообластная конфигурации на граничном маршрутизаторе области

Многообластная конфигурация OSPFv3 столь же скучна, как и OSPFv2. Многообластной проект OSPF может потребовать обсуждения перед принятием решения о том, какие каналы связи к каким областям отнести. После принятия этого решения правильная конфигурация не более чем вопрос чтения документации и ввода соответствующих номеров областей в подкоманды интерфейса `ipv6 ospf` *`идентификатор_процесса`* `area` *`идентификатор_области`*.

В этом примере у маршрутизатора ABR R1 есть процесс OSPFv3 (с идентификатором процесса 1), разрешающий протокол OSPFv3 на пяти интерфейсах следующим образом (согласно рис. 17.2).

Область 0. Интерфейсы G0/0.11 и G0/0.12.
Область 23. Интерфейсы S0/0/0 и S0/0/1.
Область 4. Интерфейс G0/1.

Для ясности: ничто в конфигурации маршрутизатора R1 не указывает на его многообластной характер или ABR. Маршрутизатор R1 просто действует как маршрутизатор ABR, поскольку его конфигурация помещает одни интерфейсы в область 0, а другие — в другие не магистральные области. Конфигурация показана в примере 17.4.

Ключевая тема

Пример 17.4. Конфигурация IPv6 и OSPFv3 на маршрутизаторе ABR R1

```
ipv6 unicast-routing
!
interface GigabitEthernet0/0
mac-address 0200.0000.0001
!
interface GigabitEthernet0/0.11
```

```
encapsulation dot1q 11
ipv6 address 2001:db8:1:1::1/64
ipv6 ospf 1 area 0
!
interface GigabitEthernet0/0.12
encapsulation dot1q 12
ipv6 address 2001:db8:1:2::1/64
ipv6 ospf 1 area 0
!
interface GigabitEthernet0/1
ipv6 address 2001:db8:1:14::1/64
ipv6 ospf 1 area 4
!
interface serial 0/0/0
ipv6 address 2001:db8:1:12::1/64
ipv6 ospf 1 area 23
!
interface serial 0/0/1
ipv6 address 2001:db8:1:13::1/64
ipv6 ospf 1 area 23
!
ipv6 router ospf 1
router-id 1.1.1.1
```

Другие параметры конфигурации OSPFv3

Пример завершает обзор конфигурации OSPFv3 из книги по ICND1 добавлением небольшого количества информации о многообластной конфигурации. Несколько следующих коротких разделов посвящено ряду других средств протокола OSPF, обсуждавшихся в контексте протокола OSPFv2 в главе 8, но уже для протокола OSPFv3. Как обычно, детали почти идентичны.

Установка параметра стоимости интерфейса OSPFv3, влияющего на выбор маршрута

Протокол OSPFv3 очень похож на протокол OSPFv2 способом вычисления метрики маршрута, но с некоторыми небольшими отличиями в концепциях, командах конфигурации и проверки.

Как уже говорилось в главе 8 о протоколе OSPFv2, протокол поиска первого кратчайшего маршрута (SPF) находит на маршрутизаторе все возможные маршруты к подсети. Затем суммируются стоимости всех исходящих интерфейсов OSPF на маршруте.

Например, рис. 17.3 практически повторяет рисунок из главы 8, немного измененный, чтобы представить теперь подсеть IPv6. На рисунке представлен проект одиночной области, в которой маршрутизатор R1 находит три возможных маршрута к подсети 33 (2001:DB8:1:33::/64); самую низкую стоимость имеет средний маршрут.

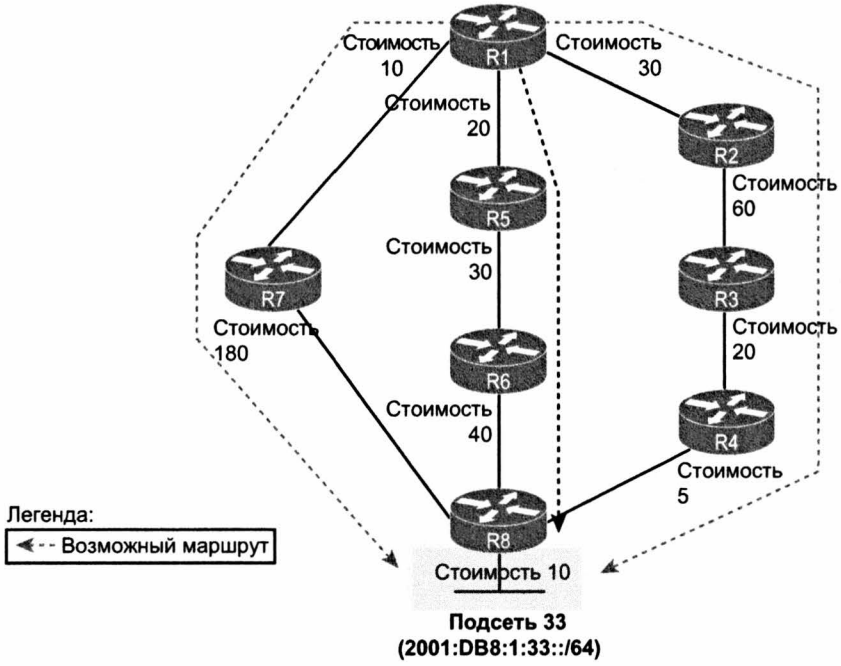


Рис. 17.3. Дерево SPF для поиска маршрута от маршрутизатора R1 к подсети 2001:DB8:1:33::/64

Чтобы можно было повлиять на метрику маршрута, протокол OSPFv3 предоставляет несколько способов изменения стоимости интерфейса OSPFv3, причем согласно тем же базовым правилами, что и у протокола OSPFv2. Они представлены ниже.

Ключевая тема **Способы влияния на вычисляемые метрики маршрута OSPFv3**

1. Стоимость может быть установлена явно, подкомандой интерфейса `ip ospf cost` *x* со значением от 1 до 65 535 включительно.
2. Полосу пропускания интерфейса можно изменить командой `bandwidth` *скорость*, где скорость задается числом в Кбит/с, что позволяет маршрутизатору вычислять значение на основании формулы *исходная_полоса_пропускания / полоса_пропускания_интерфейса*.
3. Исходную полосу пропускания можно изменить подкомандой OSPF маршрутизатора `auto-cost reference-bandwidth` *исходная_полоса_пропускания*, где значение задается числом в Мбит/с.

Балансировка нагрузки OSPF

Протоколы OSPFv3 и OSPFv2 следуют той же концепции и используют одинаковые команды конфигурации для распределения нагрузки с учетом равной стоимости.

Когда протокол OSPFv3 находит на маршрутизаторе несколько маршрутов с равными метриками к той же подсети, маршрутизатор может поместить в таблицу маршрутизации несколько маршрутов равной стоимости. Подкоманда маршрутизатора OSPFv3 `maximum-paths` *`количество`* определяет только количество таких маршрутов, добавляемых в таблицу маршрутизации IPv6. Например, если в объединенной сети есть шесть возможных маршрутов к некой подсети и у всех одинаковая метрика, а инженер хочет использовать все маршруты, то он может настроить маршрутизатор подкомандой `maximum-paths 6` при наличии команды `ipv6 router ospf`.

Ввод стандартных маршрутов

И наконец, еще одно средство протокола OSPFv3, работающее как и в протоколе OSPFv2, — маршрутизатор OSPFv3 может анонсировать стандартный маршрут. Эта функция позволяет одному маршрутизатору получить стандартный маршрут, а затем оповестить все остальные маршрутизаторы: "Если кому нужен стандартный маршрут, посылайте пакеты мне, а я перешлю их по своему отличному стандартному маршруту".

Классический случай использования протокола маршрутизации для анонсирования стандартного маршрута — это соединение предприятия с Интернетом. Если у компании есть одно подключение к Интернету с поддержкой протокола IPv6, то один маршрутизатор может использовать стандартный маршрут IPv6 для перенаправления всего трафика IPv6 Интернета через этот один канал связи. Однако остальная часть маршрутизаторов предприятия должна посылать свой трафик Интернета на этот маршрутизатор. Таким образом, инженер предприятия решал бы в проекте следующие задачи.

- Все маршрутизаторы изучают конкретные маршруты к подсетям компании, поэтому получателям внутри компании стандартный маршрут не нужен.
- У одного маршрутизатора, подключенного к Интернету, есть статический стандартный маршрут IPv6 для всего трафика IPv6 (не соответствующего никакому другому маршруту IPv6), предназначенного для Интернета.
- Все маршрутизаторы изучают (по протоколу OSPFv3) стандартный маршрут к маршрутизатору, подключенному к Интернету, чтобы все следующие в Интернет пакеты IPv6 поступали сначала на этот маршрутизатор.

На рис. 17.4 представлена концепция того, как распространяется информация о маршрутизации от подключенного к Интернету маршрутизатора (R1) к другим маршрутизаторам компании. В данном случае компания подключена к провайдеру ISP через маршрутизатор R1. На нем использована команда OSPFv3 `default-information originate` в режиме конфигурации OSPFv3; это буквально та же команда, используемая протоколом OSPFv2 (этап 1). В результате маршрутизатор R1 анонсирует стандартный маршрут другим маршрутизаторам OSPFv3 (этап 2). (Префикс для стандартного маршрута IPv6 — ::/0 при длине префикса 0, что несколько похоже на подсеть 0.0.0.0/0, используемую протоколом IPv4.)

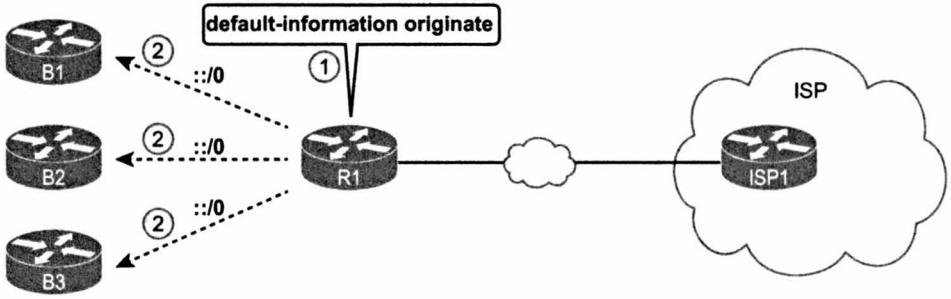


Рис. 17.4. Использование протокола OSPFv3 для анонсирования стандартного маршрута

Как только процесс на рис. 17.4 завершается, у каждого из трех маршрутизаторов слева будет стандартный маршрут. В их стандартных маршрутах маршрутизатор R1 указан как следующий транзитный маршрутизатор, чтобы весь предназначенный для Интернета трафик поступал сначала на маршрутизатор R1, а затем провайдеру ISP.

На этом завершается обсуждение новой конфигурации протокола OSPFv3. Следующий раздел посвящен различиям в концепциях OSPFv3, включая проверку, поиск и устранение неисправностей.

Концепции OSPF, проверка, поиск и устранение неисправностей

На необходимом для экзамена CCNA Routing and Switching уровне подробностей протоколы OSPFv3 и OSPFv2 очень похожи. На настоящий момент, с учетом усвоенного материала этой книги и книги по ICND1, читателям должны быть уже известны все схожие концепции, команды проверки и способы поиска неисправностей протокола OSPFv2. Этот раздел данной главы должен только продемонстрировать, где протокол OSPFv3 использует одинаковые концепции, а в каких редких случаях протокол OSPFv3 отличается от OSPFv2.

Между протоколами OSPFv3 и OSPFv2 есть следующие подобия.

Ключевая тема

Подобия протоколов OSPFv3 и OSPFv2

- Проект областей и связанные термины.
- Настройка подразумевает запуск процесса маршрутизации для каждого интерфейса в области.
- Процесс поиска соседей полагается на сообщения Hello.
- Переходные состояния соседей и процесс обмена топологической информацией.
- Использование состояний full и 2-way как нормальных стабильных состояний рабочих соседских отношений. Другие состояния являются либо временными, либо указывают на некую проблему с соседом.
- Общие концепции типов 1, 2 и 3 анонсов LSA, а также баз данных состояний каналов (LSDB).
- Используется протокол SPF и стоимость интерфейса для вычисления метрики.

- Зарезервированные многоадресатные адреса (FF02::5 для всех маршрутизаторов OSPF, FF02::6 для всех маршрутизаторов DR и BDR) подобны адресам 224.0.0.5 и 224.0.0.6 протокола OSPFv2.

Каковы различия между ними? Ниже приведено несколько из них. Описание большинства различий выходит за рамки этой книги.

Различия между протоколами OSPFv3 и OSPFv2



- Название анонса LSA типа 3.
- У соседей OSPFv3 не должно быть IPv6-адресов в той же подсети IPv6, тогда как соседи OSPFv2 должны находиться в той же подсети IPv4.
- Протокол OSPFv3 использует новые типы анонсов LSA, которых нет в протоколе OSPFv2 (в этой книге не рассматриваются).
- Данные в анонсах LSA типов 1, 2 и 3 отличаются (также не рассматриваются).

Как можно заметить, список различий относительно короткий.

Благодаря множеству подобий между протоколами OSPFv3 и OSPFv2 компания Cisco также сохранила максимальное подобие команд проверки. На рис. 17.5 приведены команды проверки OSPFv3, а также виды предоставляемой ими информации. Обратите внимание, что если во всех командах заменить часть `ipv6` на `ip`, то получится точный синтаксис соответствующих команд OSPFv2.

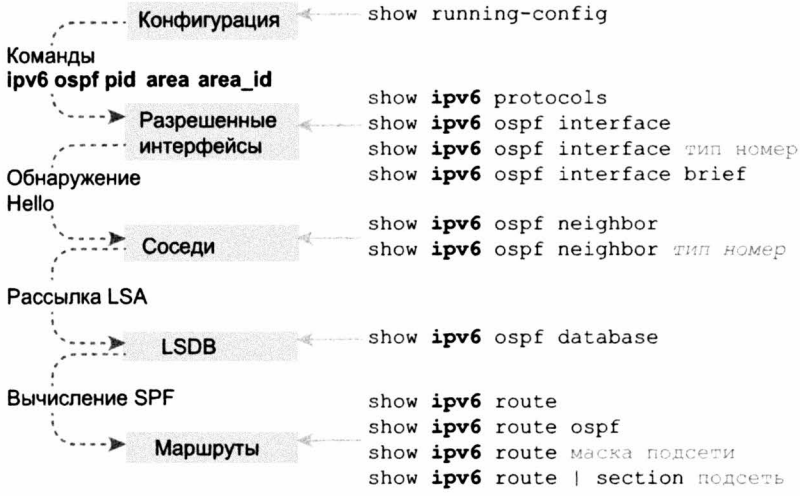


Рис. 17.5. Команды проверки OSPFv3

Когда маршрутизатор впервые запускает процесс OSPFv3, операционная система IOS читает конфигурацию OSPFv3 и разрешает протокол OSPFv3 на интерфейсах. Поэтому данный раздел начинается с обсуждения проверки интерфейса OSPFv3, а также поиска и устранения неисправностей. Далее обсуждение переходит к соседским отношениям OSPFv3, затем к топологической базе данных OSPFv3 и наконец к маршрутам OSPFv3, добавляемым к таблице маршрутизации IPv6.

ВНИМАНИЕ!

Во всех примерах поиска и устранения неисправностей в остальной части этой главы используются маршрутизаторы R1, R2, R3 и R4 из примера многообластной конфигурации, приведенного ранее в главе. За справками по топологии и схемам областей этой сети обращайтесь к рис. 17.1 и 17.2.

Интерфейсы OSPFv3

Стиль настройки протокола OSPFv3 подразумевает однозначную идентификацию интерфейсов с разрешенным процессом OSPFv3. Подкоманда интерфейса `ipv6 ospf` *идентификатор_процесса* `area` *идентификатор_области* просто означает "запустить процесс OSPFv3 на этом интерфейсе". Быстрый просмотр интерфейсов в выводе команды `show running-config` позволяет выявить все интерфейсы и номера их областей.

Ниже сначала рассматривается несколько других методов проверки интерфейсов OSPFv3, а затем приведено несколько советов по поиску и устранению неисправностей, связанных с интерфейсом OSPFv3.

Проверка интерфейсов OSPFv3

Предположим, вы тщательно изучали конфигурацию протокола OSPFv3, упорно практиковались и чувствуете себя теперь уверенно. И вот на экзамене вам попадается симлет на OSPFv3. К сожалению, симлет не позволяет перейти в привилегированный режим, поэтому вы не можете просмотреть конфигурацию! Команда `show running-config` плюс ваши прекрасные навыки в конфигурации позволили бы ответить на любой вопрос, но вы не можете просмотреть конфигурацию. Так как же узнать, например, на каких интерфейсах запущен процесс OSPFv3?

Об интерфейсах с разрешенным процессом OSPFv3 могут сообщить три команды: `show ipv6 protocols` , `show ipv6 ospf interface brief` и `show ipv6 ospf interface`. Все они выводят интерфейсы с протоколом OSPFv3. Первые две команды выводят информацию кратко, а третья выводит о каждом интерфейсе несколько строк. (Если необходим быстрый ответ, используйте любую из первых двух команд.)

Заметьте, что все три эти команды выводят как пассивные, так и не пассивные интерфейсы OSPFv3, — весьма важный факт, о котором не следует забывать при поиске и устранении проблем соседских отношений. Результат приведен в примере 17.5. Обратите внимание, что перед выводом в примере в процесс OSPFv3 маршрутизатора R1 была добавлена команда `passive-interface gigabitethernet0/0.11`.

Пример 17.5. Проверка интерфейсов OSPFv3 и их параметров

```
R1# show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "ND"
IPv6 Routing Protocol is "ospf 1"
  Interfaces (Area 0):
    GigabitEthernet0/0.12
    GigabitEthernet0/0.11
  Interfaces (Area 4):
```

```
    GigabitEthernet0/1
  Interfaces (Area 23):
    Serial0/0/1
    Serial0/0/0
  Redistribution:
    None
```

Как можно заметить в примере, вывод команды `show ipv6 protocols` демонстрирует все пять интерфейсов OSPFv3 на маршрутизаторе R1, включая пассивный интерфейс G0/0.11.

Поиск и устранение неисправностей интерфейсов OSPFv3

Большинство обсуждавшихся до сих пор вопросов поиска и устранения неисправностей OSPFv3 было связано с проблемами между двумя соседями OSPFv3. Однако причинами большинства проблем соседских отношений OSPF фактически являются ошибки в подкомандах интерфейса. Сначала рассмотрим проблемы, связанные только с подкомандами интерфейса, упомянутыми до сих пор в этой главе.

Общие проблемы OSPFv3 на интерфейсах



- В подкоманде интерфейса `ipv6 ospf` *`идентификатор_процесса`* `area` *`идентификатор_области`* неправильно задана область, что предотвращает соседские отношения на этом интерфейсе.
- Если интерфейс OSPFv3 ошибочно сделан пассивным, это не позволит локальному маршрутизатору сформировать соседские отношения на этом интерфейсе.

По первому элементу списка: помните, что все маршрутизаторы OSPFv3 на том же канале связи должны находиться в той же области. На экзамене следует проверять любую информацию об областях в рассматриваемом проекте. Для определения присвоенных интерфейсам областей используйте команды `show ipv6 ospf interface` и `show ipv6 ospf interface brief`.

Что касается проблемы с пассивным интерфейсом OSPFv3: если должны быть сформированы соседские отношения, то интерфейс маршрутизатора не должен быть пассивным интерфейсом OSPFv3. Обратите внимание: только что упомянутая команда `show ipv6 ospf interface` выводит пассивные интерфейсы OSPFv3.

Пример 17.6 демонстрирует две команды, весьма полезные для поиска обеих этих проблем. Обе выводят информацию об области, но только вторая упоминает пассивные интерфейсы.

Пример 17.6. Поиск пассивных интерфейсов OSPFv3 на маршрутизаторе R1

```
R1# show ipv6 ospf interface brief
Interface  PID  Area  Intf ID  Cost  State Nbrs F/C
Gi0/0.12   1    0     16       1     DR    0/0
Gi0/0.11   1    0     17       1     DR    0/0
Gi0/1      1    4     4        1     DR    1/1
Se0/0/1    1    23    7        64    P2P   1/1
Se0/0/0    1    23    6        64    P2P   1/1
```

```
R1# show ipv6 ospf interface G0/0.11
GigabitEthernet0/0.11 is up, line protocol is up
  Link Local Address FE80::FF:FE00:1, Interface ID 17
  Area 0, Process ID 1, Instance ID 0, Router ID 1.1.1.1
  Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 1.1.1.1, local address FE80::FF:FE00:1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    No Hellos (Passive interface)
! Остальные строки опущены для краткости
```

И наконец, рассмотрим пример одной из этих проблем в конфигурации маршрутизатора R4. Для правильной настройки инженер в примере 17.3 сделал интерфейс LAN G0/1 пассивным, поскольку в этой локальной сети нет никаких других маршрутизаторов. Но маршрутизатор R4 использует один интерфейс Ethernet как интерфейс WAN (G0/0) и один как интерфейс LAN (G0/1). Предположим, что инженер просто допустил ошибку и сделал пассивным интерфейс G0/0 маршрутизатора R4 вместо интерфейса G0/1. Для демонстрации происходящего пример 17.7 изменен так, что пассивным интерфейсом OSPFv3 стал интерфейс G0/0 маршрутизатора R4; обратите внимание, что соседские отношения между маршрутизаторами R4 и R1 исчезают почти немедленно после ввода команды `passive-interface`.

Пример 17.7. Разрыв соседских отношений между маршрутизаторами R4 с R1 из-за пассивности интерфейса

```
R4# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R4(config)# ipv6 router ospf 4
R4(config-rtr)# passive-interface gigabitEthernet 0/0
R4(config-rtr)# ^Z
R4#
Jan 17 23:49:56.379: %OSPFv3-5-ADJCHG: Process 4, Nbr 1.1.1.1 on Giga-
bitEthernet0/0 from FULL to DOWN, Neighbor Down: Interface down or de-
tached
```

Соседи OSPFv3

Как обычно, протокол OSPFv3 следует тем же соглашениям о соседских отношениях, что и протокол OSPFv2. В протоколе OSPFv3 использовано большинство тех же имен сообщений, состояний соседей и концепций в процессе формирования соседских отношений и обмена базами данных состояния каналов (LSDB). Ниже мы рассмотрим несколько примеров процесса и, что важней всего, покажем несколько мест, где имеет смысл искать проблемы OSP, препятствующие установлению маршрутизаторами соседских отношений.

Проверка соседей OSPFv3

В примере 17.8 показано несколько сходств между именами сообщений протоколов OSPFv3 и OSPFv2, а также между состояниями соседей. Читая в примере вывод команды `debug`, не заботьтесь обо всех деталях; сосредоточьтесь только на выделенных частях. Они демонстрируют некоторые из уже знакомых вам по протоколу

OSPFv2 соседских состояний, таких как 2-way, exstart, exchange, loading и full (последнее в данном случае является заключительным необходимым состоянием).

Сначала в примере приведен вывод команды `debug ipv6 ospf adj`, содержащий сообщения о событиях соседей OSPFv3 в сети, т.е. что происходит, когда соседи в ходе работы меняют свои соседские состояния. В конце примера приведен вывод команды `show ipv6 ospf neighbor` на маршрутизаторе R2, подтверждающий, что состоянием его соседа, маршрутизатора R3, является final, как и упомянуто в отладочном сообщении. (Обратите внимание, что некоторые отладочные сообщения были удалены для краткости.)

Пример 17.8. Отслеживание изменений состояния соседа (R3) с маршрутизатора R2

```
R2# debug ipv6 ospf adj
R2#
Jan 15 14:50:58.098: OSPFv3-2-IPv6 ADJ   Gi0/0: Added 3.3.3.3 to nbr list
Jan 15 14:50:58.098: OSPFv3-2-IPv6 ADJ   Gi0/0: 2 Way Communication to
3.3.3.3, state 2WAY
Jan 15 14:50:58.098: OSPFv3-2-IPv6 ADJ   Gi0/0: DR: 3.3.3.3 (Id) BDR:
2.2.2.2 (Id)
Jan 15 14:50:58.098: OSPFv3-2-IPv6 ADJ   Gi0/0: Nbr 3.3.3.3: Prepare
dbase exchange
Jan 15 14:50:58.098: OSPFv3-2-IPv6 ADJ   Gi0/0: Send DBD to 3.3.3.3 seq
0x2AC5B307 opt 0x0013 flag 0x7 len 28
Jan 15 14:50:58.102: OSPFv3-2-IPv6 ADJ   Gi0/0: Rcv DBD from 3.3.3.3 seq
0xBD091ED opt 0x0013 flag 0x7 len 28 mtu 1500 state EXSTART
Jan 15 14:50:58.102: OSPFv3-2-IPv6 ADJ   Gi0/0: NBR Negotiation Done. We
are the SLAVE
Jan 15 14:50:58.102: OSPFv3-2-IPv6 ADJ   Gi0/0: Nbr 3.3.3.3: Summary list
built, size 14
Jan 15 14:50:58.106: OSPFv3-2-IPv6 ADJ   Gi0/0: Rcv DBD from 3.3.3.3 seq
0xBD091EE opt 0x0013 flag 0x1 len 308 mtu 1500 state EXCHANGE
Jan 15 14:50:58.106: OSPFv3-2-IPv6 ADJ   Gi0/0: Exchange Done with
3.3.3.3
Jan 15 14:50:58.106: OSPFv3-2-IPv6 ADJ   Gi0/0: Synchronized with
3.3.3.3, state FULL
Jan 15 14:50:58.106: %OSPFv3-5-ADJCHG: Process 2, Nbr 3.3.3.3 on Giga-
bitEthernet0/0 from LOADING to FULL, Loading Done

R2# show ipv6 ospf neighbors

Neighbor ID  Pri  State     Dead Time  Interface ID  Interface
1.1.1.1      0    FULL/ -   00:00:38   6             Serial0/0/1
3.3.3.3      1    FULL/DR   00:00:37   3             GigabitEthernet0/0
```

Точно так же, как и при протоколе OSPFv2, работающие соседи OSPFv3 стабилизируются в состояние full или 2-way. Большинство соседей достигают состояния полной синхронизации (full), означающего, что они полностью обменялись друг с другом своими базами LSDB. Однако соседские отношения в сети OSPF любого типа, использующей выделенный маршрутизатор (DR) и резервный выделенный маршрутизатор (BDR), достигают только состояния полной синхронизации. Соседские отношения между маршрутизаторами, не являющимися ни DR, ни BDR (обычные маршрутизаторы), стабилизируются в состояние 2-way.

Поиск и устранение неисправностей соседских отношений OSPFv3

Каждый раз, когда протокол OSPFv3 не в состоянии изучить маршруты, которые должен, обращайте внимание на соседские отношения OSPFv3. Обнаружив отсутствие ожидаемых отношений или их неспособность достичь рабочего состояния (full или 2-way), можно сосредоточиться на различных причинах неработоспособности соседских отношений.

ВНИМАНИЕ!

Как и в протоколе OSPFv2, о соседях, находящихся в состоянии полной синхронизации (full), говорят как о *полностью согласованных* (fully adjacent), тогда как два обычных, невыделенных соседних маршрутизатора стабилизируются в состояние двустороннего канала (2-way), такие маршрутизаторы просто *согласованны* (adjacent).

Для поиска и устранения неисправностей соседских отношений OSPF следует помнить множество подробностей о факторах, способных воспрепятствовать тому, чтобы два маршрутизатора стали соседями вообще. К счастью, их список для протокола OSPFv3 практически совпадает с таковым у протокола OSPFv2, но с одним существенным различием: протокол OSPFv3 не требует, чтобы соседи находились в той же подсети. Требования, проверяемые при поиске и устранении неисправностей в соседских отношениях OSPF, приведены в табл. 17.1.

Ключевая тема

Таблица 17.1. Требования к соседям в протоколах OSPFv2 и OSPFv3

Требование	OSPFv2	OSPFv3
Интерфейсы должны быть в рабочем состоянии (up/up)	Да	Да
Интерфейсы должны относиться к той же подсети	Да	Нет
Списки (ACL) не должны фильтровать сообщения протокола маршрутизации	Да	Да
Аутентификация, если она настроена, должна пройти успешно	Да	Да
Таймеры Hello и Dead должны совпадать	Да	Да
Идентификаторы маршрутизаторов (Router ID) должны быть уникальными	Да	Да
В командах конфигурации маршрутизаторов должны совпадать идентификаторы процесса (Process ID)	Нет	Нет

Чтобы при поиске и устранении неисправностей быстро найти информацию, позволяющую проверить каждый конкретный параметр, способный воспрепятствовать установлению двумя маршрутизаторами соседских отношений, используйте команды из табл. 17.2.

В данном разделе приведено несколько примеров проблем, способных возникнуть между соседями OSPFv3. В первую очередь, пример 17.9 демонстрирует конфигурацию, где у маршрутизатора (R4) специально установлен такой же идентификатор RID, как и у его соседа (R1, RID 1.1.1.1). В выделенных частях примера происходит следующее.

1. Маршрутизатор R4 изменяет свой RID на 1.1.1.1.
2. Маршрутизатор R4 очищает свой процесс OSPFv3, чтобы начать использовать новый RID 1.1.1.1.
3. Маршрутизатор R4 выводит сообщение системного журнала, утверждающего, что соседские отношения разорваны (из-за команды `clear`).
4. Маршрутизатор R4 выводит сообщение системного журнала, объясняющее, почему маршрутизатор R4 больше не является соседом маршрутизатора R1 (1.1.1.1).

Таблица 17.2. Требования к соседям EIGRP и наилучшие команды `show/debug`

Ключевая тема

Требование	Наилучшие команды для изоляции проблемы
Аутентификация соседей должна быть пройдена	`show ipv6 ospf interface`
Таймеры Hello и Dead должны совпадать	`show ipv6 ospf interface`
Маршрутизаторы должны находиться в той же области	`show ipv6 ospf interface brief`, `show ipv6 protocols`
Идентификаторы маршрутизатора должны быть уникальными	`show ipv6 ospf`
Интерфейсы не должны быть пассивными	`show ipv6 ospf interface`

Пример 17.9. Результат изменения маршрутизатором R4 своего RID (1.1.1.1) на совпадающий с RID маршрутизатора R1

```
R4# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R4(config)# ipv6 router ospf 4
R4(config-rtr)# router-id 1.1.1.1
% OSPFv3: Reload or use "clear ipv6 ospf process" command, for this
to take effect
R4(config-rtr)# ^Z

R4# clear ipv6 ospf process
Reset ALL OSPF processes? [no]: yes
R4#
Jan 17 23:22:03.211: %OSPFv3-5-ADJCHG: Process 4, Nbr 1.1.1.1 on
GigabitEthernet0/0 from FULL to DOWN, Neighbor Down: Interface down
r detached
R4#
Jan 17 23:22:05.635: %OSPFv3-4-DUP_RTRID_NBR: OSPF detected duplicate
router-id 1.1.1.1 from FE80::604:5FF:FE05:707 on interface
GigabitEthernet0/0
R4#
R4# show ipv6 ospf neighbor
R4#
```

В конце примера команда `show ipv6 ospf neighbor` подтверждает, что теперь у маршрутизатора R4 нет соседей OSPFv3. (Обратите внимание, что эти примеры используют тот же проект сети, что и на рис. 17.1 и 17.2, где маршрутизатор имеет одного соседа, а именно R1.) Совпадающий RID не позволяет маршрутизаторам R4

и R1 стать соседями, поэтому в выводе команды `show ipv6 ospf neighbor` на маршрутизаторе R4 вообще нет ни строки.

Следующий пример (17.10) также основан на рис. 17.1 и 17.2, он похож на случай рассогласования таймеров Hello и Dead протокола OSPFv2, рассматривавшегося в главе 11. Таймеры Hello и Dead маршрутизатора R3 имеют стандартные для интерфейсов Ethernet значения 10 и 40 соответственно. Перед вводом команд примера в конфигурацию маршрутизатора R2 была введена подкоманда интерфейса `ipv6 ospf hello-interval 5`, изменившая значения таймеров Hello и Dead интерфейса G0/0 маршрутизатора R2 на 5 и 20 соответственно. (Эта команда устанавливает таймер Hello, а операционная система IOS сама устанавливает таймер Dead в четыре раза больше, чем таймер Hello.)

Пример 17.10. Маршрутизатор R3 отсутствует в таблице соседних устройств OSPFv3 маршрутизатора R2

```
R2# show ipv6 ospf neighbor

Neighbor ID  Pri  State     Dead Time  Interface ID  Interface
1.1.1.1        0  FULL/ -   00:00:35   6             Serial0/0/1

R2# show ipv6 ospf interface g0/0
GigabitEthernet0/0 is up, line protocol is up
  Link Local Address FE80::FF:FE00:2, Interface ID 3
  Area 23, Process ID 2, Instance ID 0, Router ID 2.2.2.2
  Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 2.2.2.2, local address FE80::FF:FE00:2
  No backup designated router on this network
  Timer intervals configured, Hello 5, Dead 20, Wait 20, Retransmit 5
```

В примере 17.10 приведены две команды, подтверждающие, что маршрутизаторы R2 и R3 более не являются соседями по LAN. Однако, подобно примеру OSPFv2 из главы 11, маршрутизатор не выдает сообщения системного журнала, указывающего первопричину проблемы. Команда `show` — это единственный способ поиска данного конкретного рассогласования. Просмотрите вывод команды `show ipv6 ospf interface` на обоих маршрутизаторах; пример 17.10 демонстрирует ее вывод на маршрутизаторе R2, свидетельствующий о новых значениях 5 и 20 таймеров Hello и Dead.

Базы LSDB и анонсы LSA протокола OSPFv3

Как только маршрутизаторы OSPFv3 становятся соседями, они начинают обмениваться своими базами LSDB по этой подсети. В большинстве случаев эти два маршрутизатора обмениваются своими базами LSDB непосредственно, а по завершении обмена каждый маршрутизатор отображает своего соседа как достигшего полной синхронизации. Находясь в состоянии полной синхронизации, оба маршрутизатора должны выдавать одинаковые *анонсы состояния канала* (Link-State Advertisement — LSA) для этой области.

В данном разделе коротко рассматриваются базы LSDB и анонсы LSA в области, которые также выглядят очень похоже на таковые у протокола OSPFv2. Кроме того,

здесь описана одна довольно редкая проблема конфигурации, позволяющая двум маршрутизаторам стать соседями OSPFv3 на непродолжительное время, приводя к сбою процесса обмена топологической информации.

Проверка анонсов LSA протокола OSPFv3

Протокол OSPFv3 использует подобные концепции, но с немного иными названиями, чем у эквивалентных анонсов LSA типа 1, 2 и 3 протокола OSPFv2. Как уже упоминалось в главе 8, для определения топологии в области протокол OSPFv2 использует анонс router LSA (тип 1) и анонс network LSA (тип 2). Анонс summary LSA, тип 3, описывает для одной области подсеть, существующую в некой другой области, — *межобластную подсеть* (interarea subnet), если хотите.

Для представленных в этой книге параметров настройки протокола OSPFv2 необходимы только эти три типа анонсов LSA в базе LSDB OSPFv2.

Протокол OSPFv3 продолжает использовать те же три концепции анонсов LSA, лишь анонс summary LSA переименован. Список трех ключевых типов анонсов LSA протокола OSPFv3 и причины их создания маршрутизатором приведены ниже.

Три типа ключевых анонсов LSA протокола OSPFv3 в многообластном проекте



- По одному анонсу router LSA (тип 1) для каждого маршрутизатора в области (включая подключенные к области маршрутизаторы ABR).
- По одному анонсу network LSA (тип 2) для каждой сети, обладающей маршрутизатором DR, плюс один для соседа DR.
- По одному анонсу interarea prefix LSA (тип 3) для каждого префикса IPv6 (подсети), расположенного в другой области.

Например, в области 4 используемого в этой главе примера сети есть два маршрутизатора: внутренний маршрутизатор R4 и маршрутизатор ABR R1. Таким образом, в базе LSDB области 4 будет по одному анонсу router LSA для каждого маршрутизатора. В этой области существует одна сеть, для которой будет использоваться маршрутизатор DR (Ethernet WAN между маршрутизаторами R1 и R4). Маршрутизаторы R1 и R4 станут соседями, поэтому для этой сети будет также создан один анонс network LSA. И наконец, маршрутизатору ABR (R1) будет известно приблизительно пять разных префиксов IPv6, существующих вне области 4, поэтому маршрутизатор ABR R1 должен создать и разослать в области 4 пять анонсов interarea prefix LSA. На рис. 17.6 приведена концептуальная модель анонсов LSA для области 4.

Вне этой базовой структуры анонсов LSA протокол OSPFv3 имеет несколько изменений по сравнению с протоколом OSPFv2. В частности, протокол OSPFv3 добавляет несколько новых типов анонсов LSA по сравнению с протоколом OSPFv2, но в этой книге они не рассматриваются.

ВНИМАНИЕ!

Кстати, различия между анонсами LSA протоколов OSPFv2 и OSPFv3 не рассматриваются не только в этой книге, но и в следующей.

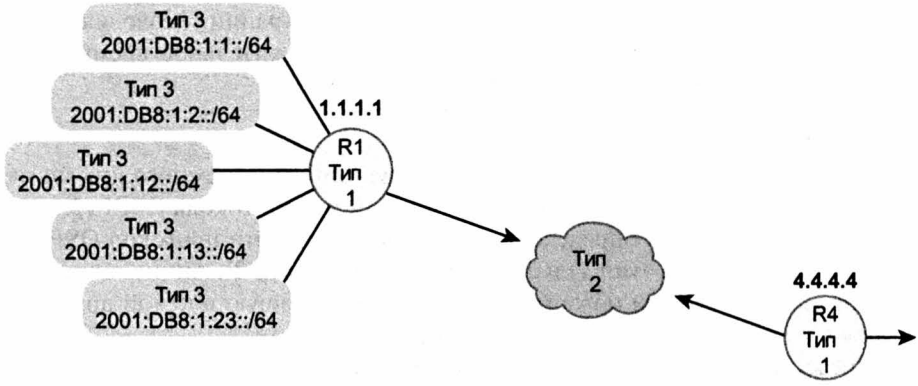


Рис. 17.6. Типы 1, 2 и 3 анонсов LSA, которые должны существовать в области 4

Чтобы увидеть представленные на рис. 17.6 анонсы LSA на фактическом маршрутизаторе, пример 17.11 демонстрирует начало базы LSDB области 4 маршрутизатора R4. В примере выделены заголовки и префиксы IPv6 анонсов interarea prefix LSA. Обратите внимание, что вывод демонстрирует два анонса router LSA, одну строку для одного анонса network LSA и пять строк с межобластными префиксами.

Пример 17.11. Содержимое базы LSDB в области 4 на маршрутизаторе R4

```
R4# show ipv6 ospf database

       OSPFv3 Router with ID (4.4.4.4) (Process ID 4)

                Router Link States (Area 4)

ADV Router      Age    Seq#       Fragment ID   Link count   Bits
1.1.1.1         258    0x80000072 0             1            B
4.4.4.4         257    0x80000003 0             1            None

                Net Link States (Area 4)

ADV Router      Age    Seq#       Fragment ID   Link count   Bits
4.4.4.4         257    0x80000001 4             2

                Inter Area Prefix Link States (Area 4)

ADV Router      Age    Seq#       Prefix
1.1.1.1         878    0x80000069 2001:DB8:1:1::/64
1.1.1.1         878    0x80000068 2001:DB8:1:2::/64
1.1.1.1         364    0x8000000A 2001:DB8:1:13::/64
1.1.1.1         364    0x8000000A 2001:DB8:1:23::/64
1.1.1.1         364    0x8000000A 2001:DB8:1:12::/64

! Строки опущены для краткости
```

Поиск и устранение неисправностей анонсов LSA протокола OSPFv3

Обмен базами данных обычно работает правильно, если два маршрутизатора действительно становятся соседями. Таким образом, большинство проблем как

протокола OSPFv2, так и протокола OSPFv3 обнаруживаются прежде, чем осуществится обмен топологическими базами данных. Напомним, что сначала два маршрутизатора должны пройти все проверки на возможность установления соседских отношений и достичь состояния 2-way прежде, чем они попытаются обменяться топологическими базами данных. Таким образом, проблемы конфигурации, способные воспрепятствовать установлению маршрутизаторами соседских отношений, проявятся прежде, чем начнется обмен базами данных.

Однако одна из ошибок конфигурации фактически позволяет двум маршрутизаторам установить соседские отношения, попытаться осуществить обмен базами данных, а затем, через несколько минут, потерпеть неудачу. Причина в несоответствии размеров максимального блока передачи данных (MTU) IPv4 или IPv6.

Сначала обсудим идею размера блока MTU, игнорируя на время протокол OSPF. Размер блока MTU — это параметр протокола уровня 3 как протокола IPv4, так и IPv6. Рассмотрим пока только протокол IPv6. Размер блока MTU интерфейса определяет максимальный размер пакета IPv6, который маршрутизатор может перенаправить через интерфейс. Концепция блока MTU протокола IPv4 та же.

ВНИМАНИЕ!

В протоколе IPv4 маршрутизаторы могут фрагментировать пакеты IPv4 на меньшие пакеты, если размер пакета превышает размер блока MTU интерфейса. В протоколе IPv6 хосты способны обнаруживать наименьший размер блока MTU по всему маршруту и избегать передачи превышающих его пакетов.

Стандартный размер блоков MTU интерфейсов большинства маршрутизаторов составляет 1500 байтов как для IPv4, так и IPv6. Это значение можно изменять подкомандами интерфейса `ip mtu` *`размер`* и `ipv6 mtu` *`размер`* для IPv4 и IPv6 соответственно.

Теперь вернемся к тому факту, что два маршрутизатора OSPFv3 могут стать соседями, а затем оказаться не в состоянии обменяться базами LSDB из-за неравных параметров MTU. В частности, соседи узнают друг о друге по сообщениям Hello, устанавливают двусторонний обмен данными (состояние 2-way) и после промежуточного постстартового (exstart) состояния начинают процесс обмена базами данных (состояние exchange). Но сбой обмена базами данных из-за несоответствия размера блоков MTU приводит к разрыву соседских отношений и отключению (состоянию down).

В примере 17.12 представлен именно этот случай отказа на маршрутизаторе R4. Сначала в примере размер блока MTU интерфейса G0/0 маршрутизатора R4 изменяется на 1400, а затем процесс OSPFv3 перезапускается.

Пример 17.12. Отказ обмена базами LSDB из-за несоответствия блоков MTU IPv6

```
R4# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R4(config)# interface gigabitethernet0/0
R4(config-if)# ipv6 mtu 1400
R4(config-if)# ^Z
R4#
R4# clear ipv6 ospf 4 process
```

```
Reset OSPF process? [no]: yes
R4#
Jan 17 23:53:24.439: %OSPFv3-5-ADJCHG: Process 4, Nbr 1.1.1.1 on Giga-
bitEthernet0/0 from FULL to DOWN, Neighbor Down: Interface down or de-
tached

R4# show ipv6 ospf neighbor

Neighbor ID  Pri  State        Dead Time  Interface ID  Interface
1.1.1.1      1    EXSTART/DR   00:00:37   4             GigabitEthernet0/0

Jan 17 23:55:29.063: %OSPFv3-5-ADJCHG: Process 4, Nbr 1.1.1.1 on Giga-
bitEthernet0/0 from EXSTART to DOWN, Neighbor Down: Too many retransmits

R4# show ipv6 ospf neighbor
Neighbor ID  Pri  State        Dead Time  Interface ID Interface
1.1.1.1      1    DOWN/DROTHER -          4            GigabitEthernet0/0
```

Последняя команда в примере может быть подсказкой, позволяющей обратить внимание на эту специфическую проблему на экзамене. Два маршрутизатора (R1 и R4) знают друг о друге, поскольку для сообщений Hello OSPF нет никаких препятствий вообще. Таким образом, команда `show ipv6 ospf neighbor` на каждом маршрутизаторе все еще отображает другой маршрутизатор, как демонстрирует вывод на маршрутизаторе R4, упоминающий соседа R1 (1.1.1.1). Но через некоторое время соседские отношения прерываются и происходит переход в состояние down. Таким образом, обнаружив соседа в постоянном состоянии down, проверьте размеры блоков MTU IPv6 с обеих сторон (командой `show ipv6 interface`).

Метрики OSPFv3 и маршруты IPv6

Завершив рассылку анонсов LSA, обмен базами данных, проверку соответствия параметров соседей и так далее, маршрутизаторы должны выбрать наилучшие маршруты IPv6 для использования. В этом заключительном разделе главы содержится обзор нескольких этапов, в ходе которых протокол OSPFv3 вычисляет метрики, а затем следуют советы по поиску и устранению неисправностей, на сей раз о том, что делать в отсутствие оптимального или при наличии неоптимального маршрута IPv6.

Проверка стоимостей и метрик интерфейсов OSPFv3

Алгоритм SPF находит все возможные маршруты, или пути, от локального маршрутизатора к каждой подсети. Когда между локальным маршрутизатором и некой дистанционной подсетью существуют избыточные пути, алгоритм SPF должен выбрать наилучший маршрут на основании самой низкой метрики всего маршрута, как было показано в примере на рис. 17.3.

Когда протокол OSPFv3 добавляет маршрут в таблицу маршрутизации IPv6, метрика маршрута будет вторым из двух чисел в записи. (Первое число в скобках — это административное расстояние (AD); протоколы маршрутизации IPv6 используют те же стандартные значения AD, что и их аналоги IPv4.)

Сначала рассмотрим метрики 65 двух маршрутов от маршрутизатора R1 к подсети 2001:DB8:1:23::/64 (рис. 17.7). Для вычисления метрики маршрута через маршру-

тизатор R2 стоимость 64 интерфейса S0/0/0 маршрутизатора R1 суммируется со стоимостью 1 интерфейса G0/0 маршрутизатора R2, что дает суммарную стоимость 65. Через маршрутизатор R3 маршрутизатор R1 вычисляет такую же метрику 65. При стандартных значениях команды `maximum-paths 4` маршрутизатор R1 поместит в таблицу маршрутизации оба маршрута. (Один маршрут использует как следующий транзитный узел маршрутизатор R2, а второй — маршрутизатор R3.)

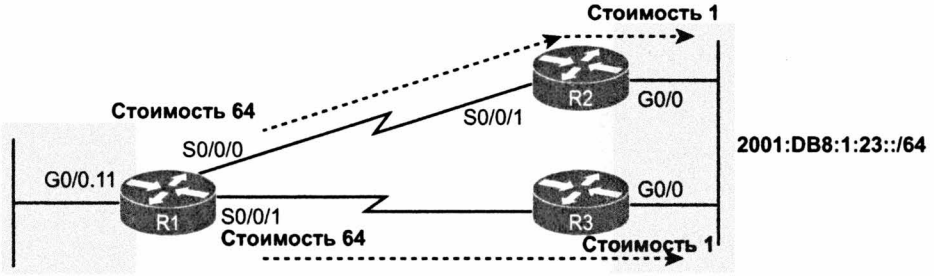


Рис. 17.7. Два маршрута с равными метриками от маршрутизатора R1 к подсети 2001:DB8:1:23::/64

В примере 17.13 эти два маршрута к подсети 2001:DB8:1:23::/64 выделены в выводе команды `show ipv6 route ospf` на маршрутизаторе R1. Как обычно, изученные по протоколу OSPF маршруты содержат локальный в пределах канала связи адрес следующей транзитной точки перехода. Чтобы увидеть, какой маршрут относится к маршрутизатору R2, а какой к маршрутизатору R3, проверьте исходящие интерфейсы и сравните их с рис. 17.7.

Пример 17.13. Маршруты OSPFv3 на маршрутизаторе R1

```
R1# show ipv6 route ospf
! Легенда опущена для краткости

O    2001:DB8:1:4::/64 [110/1]
       via GigabitEthernet0/1, directly connected
O    2001:DB8:1:23::/64 [110/65]
       via FE80::FF:FE00:3, Serial0/0/1
       via FE80::FF:FE00:2, Serial0/0/0
```

Для того чтобы показать, что происходит в случае, когда маршрутизатор имеет несколько маршрутов, но выбирает только один, поскольку у него лучшая метрика, рассмотрим в примере 17.14 изученные по протоколу OSPF маршруты IPv6 на маршрутизаторе R2, остановившись на маршруте к подсети (2001:DB8:1:1::/64) слева от маршрутизатора R1.

- У маршрутизатора R2 есть два возможных маршрута (согласно рис. 17.1) к подсети 2001:DB8:1:1::/64: один через маршрутизатор R1 и интерфейс S0/0/1 маршрутизатора R2, второй — через интерфейс G0/0 маршрутизатора R2 и маршрутизатор R3.
- В таблицу маршрутизации IPv6 маршрутизатор R2 поместит только один из этих двух маршрутов: маршрут с метрикой 65 через интерфейс S0/0/1 марш-

рутизатора R2. Его стоимость составит стандартная стоимость интерфейса S0/0/1 маршрутизатора R2 (64) плюс стоимость интерфейса G0/0.11 маршрутизатора R1 (1).

- Маршрутизатор R2 сочтет маршрут через маршрутизатор R3 худшим, поскольку его стоимость была суммой стоимости интерфейса G0/0 маршрутизатора R2 (1), интерфейса S0/0/0 маршрутизатора R3 (64) и интерфейса G0/0.11 маршрутизатора R1 (1), что составит в общей сложности 66.

На рис. 17.8 представлены стоимости интерфейсов этих двух конкурирующих маршрутов. Обратите внимание, что части сети, показанные ранее на рис. 17.1, здесь отсутствуют.

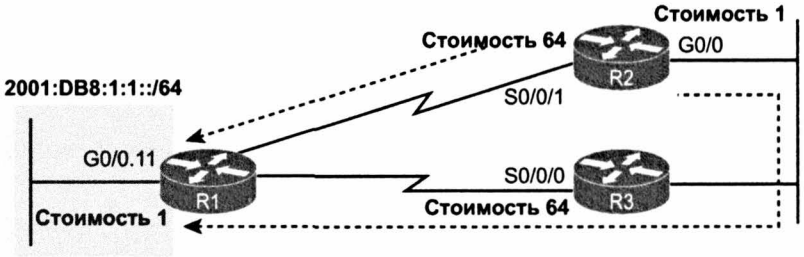


Рис. 17.8. Конкурирующий маршрут через маршрутизатор R2 к подсети 1

Пример 17.14. Маршруты OSPFv3 на маршрутизаторе R2

```
R2# show ipv6 route ospf
! Легенда опущена для краткости
OI    2001:DB8:1:1::/64 [110/65]
        via FE80::FF:FE00:1, Serial0/0/1
OI    2001:DB8:1:2::/64 [110/65]
        via FE80::FF:FE00:1, Serial0/0/1
OI    2001:DB8:1:4::/64 [110/65]
        via FE80::FF:FE00:1, Serial0/0/1
O    2001:DB8:1:13::/64 [110/65]
        via FE80::FF:FE00:3, GigabitEthernet0/0
OI    2001:DB8:1:14::/64 [110/65]
        via FE80::FF:FE00:1, Serial0/0/1
```

Обратите также внимание на кодовые знаки `OI` слева от большинства маршрутов на маршрутизаторе R2. `O` обозначает маршрут, изученный по протоколу OSPF, а `I` — межобластной маршрут. Например, в выделенном элементе указаны префикс/подсеть 1 (2001:DB8:1:1::/64), находящиеся в области 0, и маршрутизатор R2, находящийся в области 23. Таким образом, маршрут через маршрутизатор R2 к этой подсети является межобластным. (Ранее, в примере 17.13, было показано несколько внутриобластных маршрутов OSPF с кодовым знаком *O* вместо *OI*.)

Для отображения параметров стоимости интерфейса OSPFv3 используются те же команды, что и у протокола OSPFv2. Для стандартных вычислений команда `show ipv6 ospf` выводит исходную полосу пропускания, команда `show ipv6 ospf` — полосу пропускания интерфейса. В примере 17.15 показана текущая стоимость ин-

терфейса OSPFv3 на маршрутизаторе R1 в выводе команды `show ipv6 ospf interface brief`.

Пример 17.15. Стоимость интерфейса OSPFv3 маршрутизатора

```
R1# show ipv6 ospf interface brief
Interface  PID   Area   Intf ID  Cost  State  Nbrs F/C
Gi0/0.12   1     0      16       1     DR     0/0
Gi0/0.11   1     0      17       1     DR     0/0
Gi0/1      1     4      4        1     BDR    1/1
Se0/0/0    1     23     6        64    P2P    1/1
Se0/0/1    1     23     7        64    P2P    1/1
```

Поиск и устранение неисправностей маршрутов IPv6, характерные для протокола OSPFv3

Если есть вероятность, что проблема связана с маршрутизацией IPv6, ее причина может быть отнесена к двум общим категориям. Во-первых, на маршрутизаторе может отсутствовать маршрут для некоторого префикса, поэтому маршрутизатор отбрасывает пакеты и отказывает команда `ping`. Во-вторых, у маршрутизатора может быть рабочий, но неоптимальный маршрут. (Петлевой маршрут рассматривается в главе 16.)

Например, на рис. 17.9 у маршрутизатора R1 есть два возможных маршрута к подсети 33 через маршрутизатор R3. Верхний маршрут кажется лучшим, по крайней мере с точки зрения маршрутизаторов между маршрутизатором R1 и подсетью 33. Если у маршрутизатора R1 вообще нет никаких маршрутов к подсети 33, можно было бы искать один тип первопричины, но если маршрутизатор R1 использует нижний маршрут через пять маршрутизаторов, то следует искать первопричину другого типа.

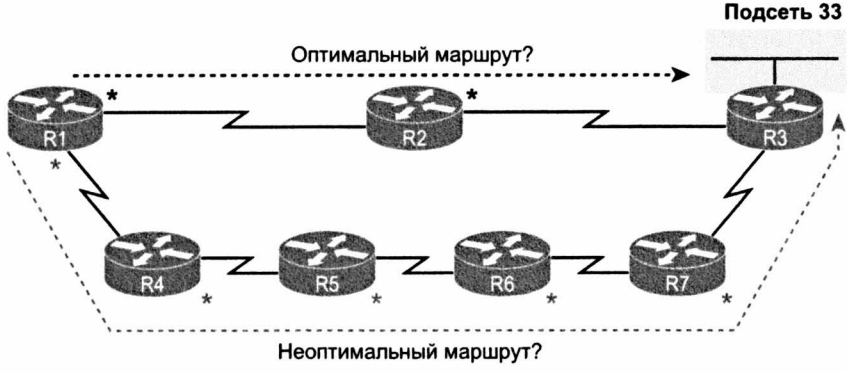


Рис. 17.9. Длинный и короткий параллельные маршруты от маршрутизатора R1 к подсети 33

Когда у маршрутизатора просто нет маршрута к данной подсети, например, если у маршрутизатора R1 нет никакого маршрута для подсети 33 вообще, происходит следующее.

Ключевая тема

Общие действия OSPFv3 при отсутствии маршрутов IPv6

Этап 1 Проверьте маршрутизаторы с интерфейсами, непосредственно подключенными к этому префиксу IPv6. Прежде чем протокол OSPFv3 начнет анонсировать подсеть, на том интерфейсе маршрутизатора должен быть разрешен протокол OSPFv3

Этап 2 Проверьте соседские отношения OSPFv3 всех маршрутизаторов между локальным маршрутизатором и маршрутизаторами с интерфейсом, подключенным к префиксу X IPv6

Например, если бы у маршрутизатора R3 на рис. 17.9 не было команды `ipv6 ospf` *`идентификатор_процесса`* `area` *`идентификатор_области`* на интерфейсе LAN, то у всех семи маршрутизаторов могли бы быть вполне рабочие соседские отношения, но маршрутизатор R3 все равно не анонсировал бы подсеть 33.

Когда у маршрутизатора есть маршрут, но это неправильный (неоптимальный) маршрут, происходит следующее.

Ключевая тема

Общие действия OSPFv3 при наличии неоптимального маршрута IPv6

Этап 1 Проверьте исправность соседских отношений по всему оптимальному пути от локального маршрутизатора к префиксу Y

Этап 2 Проверьте параметры стоимости OSPFv3 на интерфейсах по оптимальному пути

Предположим, например, что у маршрутизатора R1 действительно есть один маршрут к подсети 33 (нижний на рис. 17.9) со следующим транзитным маршрутизатором R4. Причиной подобного выбора может быть то, что

- не работают соседские отношения R2–R3;
- сумма стоимостей для верхнего маршрута больше (хуже), чем сумма стоимостей для нижнего маршрута. (Обратите внимание, что на рисунке около каждого интерфейса указана звездочка, представляющая их стоимость.)

Обзор

Резюме

- Глобальная команда `ipv6 router ospf` *идентификатор_процесса* создает процесс OSPFv3.
- Подкоманда интерфейса `ipv6 ospf` *идентификатор_процесса* `area` *идентификатор_области* разрешает процесс OSPFv3 на интерфейсе и присваивает номер области.
- В каждой конфигурации OSPFv3 должны быть обе эти команды.
- Если маршрутизатор не должен формировать соседские отношения на интерфейсе, то он может быть сделан пассивным.
- Протокол OSPFv3 очень похож на протокол OSPFv2 способом вычисления метрики маршрута.
- Протоколы OSPFv3 и OSPFv2 следуют той же концепции и используют одинаковые команды конфигурации для распределения нагрузки с учетом равной стоимости.
- Маршрутизатор OSPFv3 может анонсировать стандартный маршрут.
- Одно из важнейших отличий между протоколами OSPFv2 и OSPFv3 в том, что у соседей OSPFv3 не должно быть IPv6-адресов в той же подсети IPv6, тогда как соседи OSPFv2 должны находиться в той же подсети IPv4.
- Об интерфейсах с разрешенным процессом OSPFv3 могут сообщить три команды: `show ipv6 protocols`, `show ipv6 ospf interface brief` и `show ipv6 ospf interface`.
- Если интерфейс OSPFv3 ошибочно сделан пассивным, это не позволит локальному маршрутизатору сформировать соседские отношения на этом интерфейсе.
- Как только маршрутизаторы OSPFv3 становятся соседями, они начинают обмениваться своими базами LSDB по этой подсети. Находясь в состоянии полной синхронизации оба маршрутизатора должны выдавать одинаковые анонсы состояния канала для этой области.
- В многообластном проекте OSPFv3 есть три типа ключевых анонсов LSA: по одному анонсу router LSA (тип 1) для каждого маршрутизатора в области (включая подключенные к области маршрутизаторы ABR), по одному анонсу network LSA (тип 2) для каждой сети, обладающей маршрутизатором DR, плюс один для соседа DR и по одному анонсу interarea prefix LSA (тип 3) для каждого префикса IPv6 (подсети), расположенного в другой области.
- Большинство проблем как протокола OSPFv2, так и OSPFv3 обнаруживаются прежде, чем осуществится обмен топологическими базами данных.
- Несоответствие размера блоков MTU IPv4 или IPv6 приводит к разрыву соседских отношений и отказу в обмене базами данных.
- Когда у маршрутизатора просто нет маршрута к данной подсети, проверьте маршрутизаторы с интерфейсами, непосредственно подключенными к этому префиксу IPv6, или проверьте соседские отношения OSPFv3 всех маршрути-

заторов между локальным маршрутизатором и маршрутизаторами с интерфейсом, подключенным к префиксу X IPv6.

- Когда у маршрутизатора есть маршрут, но это неправильный (неоптимальный) маршрут, проверьте исправность соседских отношений по всему оптимальному пути от локального маршрутизатора к префиксу Y или проверьте параметры стоимости OSPFv3 на интерфейсах по оптимальному пути.

Контрольные вопросы

Ответьте на эти вопросы. Ответы можно найти на последней странице главы. Полное объяснение ответов приведено в приложении B на веб-сайте.

1. Инженер хочет установить идентификатор маршрутизатора OSPFv3 для маршрутизатора R1. Что из следующего могло бы повлиять на выбор идентификатора маршрутизатора OSPFv3 для маршрутизатора R1?

   А) Команда `ipv6 address` на интерфейсе Gigabit0/0.

   Б) Команда `ip address` на интерфейсе Serial0/0/1.

   В) Команда `ospf router-id` в режиме конфигурации OSPFv3.

   Г) Команда `ipv6 address` на интерфейсе loopback2.

2. У маршрутизатора R1 есть интерфейс Serial0/0/0 с адресом 2001:1:1:1::1/64 и интерфейс G0/0 с адресом 2001:2:2:2::1/64. Процесс OSPFv3 использует идентификатор процесса 1. Какие из следующих команд конфигурации OSPFv3 разрешают протокол OSPFv3 на интерфейсе G0/0 маршрутизатора R1 и помещает его в область 0?

   А) Команда `network 2001:1:1:1::/64 1 area 0` в режиме конфигурации маршрутизатора.

   Б) Команда `ipv6 ospf 1 area 0` в режиме конфигурации интерфейса на интерфейсе G0/0.

   В) Команда `network 2001:1:1:1::/64 1 area 0` в режиме конфигурации маршрутизатора.

   Г) Команда `ospf 1 area 0` в режиме конфигурации интерфейса на интерфейсе G0/0.

3. Предприятие использует модель двойного стека для реализации протоколов IPv4 и IPv6, а как протокол маршрутизации для обоих используется протокол OSPF. У маршрутизатора R1 есть как IPv4-, так и IPv6-адреса только на интерфейсах G0/0 и S0/0/0; на обоих интерфейсах разрешены протоколы OSPFv2 и OSPFv3 для области 0, причем для обоих протоколов идентификаторы маршрутизатора установлены явно. Если сравнить конфигурации OSPFv2 и OSPFv3, какие из следующих утверждений истинны?

   А) Конфигурация OSPFv3 использует подкоманду маршрутизатора `router-id` *`идентификатор_маршрутизатора`*.

   Б) Оба протокола используют подкоманду маршрутизатора `router-id` *`идентификатор_маршрутизатора`*.

   В) Оба протокола используют подкоманду маршрутизатора `network` *`номер_сети шаблон`* `area` *`идентификатор_области`*.

   Г) Оба протокола используют подкоманду интерфейса `ipv6 ospf` *`идентификатор_процесса`* `area` *`идентификатор_области`*.

4. Маршрутизаторы R1 и R2 подключены к той же сети VLAN. Что из следующего может помешать им стать соседями OSPFv3? (Выберите три ответа.)
   А) Несоответствие таймеров Hello.
   Б) Несоответствие идентификаторов процесса.
   В) IPv6-адреса расположены в разных подсетях.
   Г) Равенство идентификаторов маршрутизатора.
   Д) Один из интерфейсов маршрутизатора пассивен (на используемом канале связи).
5. В примере приведен отрывок вывода команды `show ipv6 route ospf` на маршрутизаторе R1. Какие ответы правильно интерпретируют значения вывода этой команды? (Выберите два ответа.)

```
R1# show ipv6 route ospf
OI  2001:DB8:1:4::/64 [110/129]
  via FE80::FF:FE00:1, Serial0/0/1
```

   А) 110 — метрика маршрута.
   Б) S0/0/1 — интерфейс маршрутизатора R1.
   В) FE80::FF:FE00:1 — адрес, локальный в пределах канала связи на маршрутизаторе R1.
   Г) OI означает, что маршрут является межобластным маршрутом OSPF.
6. Маршрутизатор R1 был настроен на использование двойного стека IPv4/IPv6 на интерфейсах S0/0/0, S0/0/1 и GigabitEthernet0/1. Новый инженер компании не знает, пассивен ли любой из этих интерфейсов. Какая из следующих команд позволяет выяснить, пассивен ли интерфейс G0/1 или засвидетельствовать этот факт, или какая команда исключает пассивные интерфейсы из своего списка интерфейсов?
   А) `show ipv6 ospf interface brief`.
   Б) `show ipv6 protocols`.
   В) `show ipv6 ospf interface G0/1`.
   Г) `show ipv6 ospf interface passive`.

Ключевые темы

Повторите все ключевые темы данной главы, отмеченные пиктограммой "Ключевая тема". Ключевые темы и соответствующие им страницы перечислены в табл. 17.3.

Таблица 17.3. Ключевые темы главы 17

Элемент	Описание	Страница
Список	Этапы настройки протокола OSPFv3	554
Прим. 17.4	Конфигурация IPv6 и OSPFv3 на маршрутизаторе ABR R1	558
Список	Способы влияния на вычисляемые метрики маршрута OSPFv3	560
Список	Подобия протоколов OSPFv3 и OSPFv2	562
Список	Различия между протоколами OSPFv3 и OSPFv2	563
Список	Общие проблемы OSPFv3 на интерфейсах	565
Табл. 17.1	Требования к соседям в протоколах OSPFv2 и OSPFv3	568
Табл. 17.2	Требования к соседям EIGRP и наилучшие команды show/debug	569

Окончание табл. 17.3

Элемент	Описание	Страница
Список	Три типа ключевых анонсов LSA протокола OSPFv3 в многообластном проекте	571
Список	Общие действия OSPFv3 при отсутствии маршрутов IPv6	578
Список	Общие действия OSPFv3 при наличии неоптимального маршрута IPv6	578

Заполните таблицы и списки по памяти

Распечатайте приложение Г с веб-сайта или его раздел, относящийся к этой главе, и заполните таблицы и списки по памяти. В приложении Д приведены заполненные таблицы и списки для самоконтроля.

Ключевые термины

После первого прочтения главы попытайтесь дать определения следующим ключевым терминам. Но не расстраивайтесь, если не все получится сразу, в главе 22 описано, как использовать эти термины на завершающем этапе подготовки к экзамену.

многообластной (multi-area), граничный маршрутизатор области (Area Border Router — ABR), внутренний маршрутизатор (internal router), опорная область (backbone area), идентификатор маршрутизатора (Router ID — RID), состояние полной синхронизации (full state), двусторонний канал (2-way state), анонс router LSA (router LSA), анонс network LSA (network LSA), анонс inter-area prefix LSA (inter-area prefix LSA), максимальный блок передачи (Maximum Transmission Unit — MTU)

Таблицы команд

Хоть и не обязательно заучивать информацию из таблиц данного раздела, ниже приведен список команд конфигурации и пользовательских команд главы. Фактически команды стоит запомнить, чтобы лучше понять содержимое главы и выполнить задания по подготовке к экзамену. Чтобы проверить, насколько хорошо вы запомнили команды, закройте левую сторону таблицы листом бумаги, читайте описания с правой стороны и пытайтесь вспомнить команду.

Таблица 17.4. Конфигурационные команды главы 17

Команда	Описание
`ipv6 router ospf` *идентификатор_процесса*	Переводит в режим конфигурации OSPF для заданного процесса
`ipv6 ospf` *идентификатор_процесса* `area` *номер_области*	Подкоманда интерфейса, разрешающая протокол OSPFv3 на интерфейсе для конкретного процесса и определяющая область OSPFv3
`ipv6 ospf cost` *стоимость_интерфейса*	Подкоманда интерфейса, устанавливающая связанную с интерфейсом стоимость OSPF
`bandwidth` *ширина_полосы_пропускания*	Подкоманда интерфейса, непосредственно устанавливающая ширину полосы пропускания интерфейса (Кбит/с)

Окончание табл. 17.4

Команда	Описание
`auto-cost reference-bandwidth` *значение*	Подкоманда маршрутизатора, задающая числитель OSPF в формуле *исходная_полоса_пропускания / полоса_пропускания_интерфейса*, используемой для вычисления стоимости OSPF на основании ширины полосы пропускания интерфейса
`router-id` *идентификатор*	Команда OSPF, статически устанавливающая идентификатор маршрутизатора
`maximum-paths` *количество_путей*	Подкоманда маршрутизатора, определяющая максимальное количество маршрутов равной стоимости, которые могут быть добавлены в таблицу маршрутизации

Таблица 17.5. Команды show главы 17

Команда	Описание
`show ipv6 ospf`	Выводит информацию о выполняющемся на маршрутизаторе процессе OSPF, включая идентификатор маршрутизатора OSPF, область, к которой подключен маршрутизатор, и количество интерфейсов в каждой области
`show ipv6 ospf interface brief`	Выводит интерфейсы, на которых разрешен протокол OSPF (на основании команд `network`), включая пассивные интерфейсы
`show ipv6 ospf interface` *тип номер*	Выводит длинный список параметров, состояние и счетчики операции OSPF на всех интерфейсах или на выбранном интерфейсе, включая таймеры Hello и Dead
`show ipv6 protocols`	Выводит все средства, позволяющие маршрутизатору изучить или создать маршруты IPv6, включая интерфейсы, на которых разрешен каждый протокол маршрутизации
`show ipv6 ospf neighbor` [*тип номер*]	Выводит краткую информацию о соседях, идентифицируемых идентификатором соседнего маршрутизатора, включая текущее состояние, с одной строкой на соседа; вывод может быть ограничен соседями на выведенном интерфейсе
`show ipv6 ospf neighbor` *идентификатор_соседа*	Тот же вывод, что и у команды `show ip ospf neighbor detail`, но только для соседа, заданного идентификатором соседнего маршрутизатора
`show ipv6 ospf database`	Выводит отчет об анонсах LSA в базе данных, выводя по одной строке для каждого анонса LSA. Вывод организован по типам анонсов LSA (сначала Тип 1, затем Тип 2 и т.д.)
`show ipv6 route`	Выводит все маршруты IPv4
`show ipv6 route ospf`	Выводит маршруты в таблице маршрутизации, изученные по протоколу OSPF
`show ipv6 route` *префикс/длина*	Отображает подробное описание маршрута для заданной подсети/маски

Ответы на контрольные вопросы:

1 Б. 2 Б. 3 Б. 4 А, Г, и Д. 5 Б и Г. 6 В.

Глава 18

Реализация протокола EIGRP для IPv6

Создавая *расширенный протокол маршрутизации внутреннего шлюза* (Enhanced Interior Gateway Routing Protocol — EIGRP) для IPv6 (EIGRPv6), компания Cisco постаралась сделать его насколько возможно похожим на протокол EIGRP для IPv4 (EIGRPv4). Насколько они похожи? Невероятно похожи, даже больше, чем версии *открытого протокола поиска первого кратчайшего маршрута* (Open Shortest Path First — OSPF) для протоколов IPv4 и IPv6. Единственное существенное различие кроется в конфигурации, требующей разрешения протокола EIGRPv6 непосредственно на интерфейсах, а также, конечно, использования IPv6-адресов и префиксов. Но когда дело доходит до концепций команды `show`, а также поиска и устранения неисправностей, прежний и новый протоколы EIGRP — фактически близнецы.

Структура настоящей главы та же, что и предыдущей. В первом главном разделе рассматриваются параметры настройки протокола EIGRPv6 и сравниваются с таковыми у протокола EIGRPv4. Во втором главном разделе демонстрируется проверка протокола EIGRPv6, а также приведено несколько советов по отладке.

В этой главе рассматриваются следующие экзаменационные темы

Технологии маршрутизации IP
Настройка и проверка EIGRP (одиночная область)
- Приемлемое расстояние / Возможные преемники / Административное расстояние
- Условие применимости
- Композиция метрик
- Идентификатор маршрутизатора
- Выбор пути
- Баланс нагрузки
  - Равномерный
  - Неравномерный
- Пассивный интерфейс

Различия методов маршрутизации и протоколов маршрутизации
- Метрика
- Следующий транзитный узел

Поиск и устранение неисправностей
Поиск и устранение проблем EIGRP
- Соседские отношения
- Номер AS
- Балансировка нагрузки
- Разделенный диапазон

Основные темы

Конфигурация EIGRPv6

Протокол EIGRPv6 очень похож на свой аналог EIGRP для протокола IPv4. После запуска протокола EIGRP на всех маршрутизаторах в объединенной сети они начинают обмениваться сообщениями EIGRP. Эти сообщения позволяют маршрутизаторам обнаруживать соседей и формировать соседские отношения, чтобы анонсировать подсети наряду с их компонентами метрик, а также вычислять метрики для параллельных маршрутов. Протокол EIGRPv6 использует ту же логику оптимального и резервного маршрутов (FS), а также процесс DUAL в отсутствие маршрута FS.

Но есть, конечно, и различия. Самым очевидным является то, что протокол EIGRPv6 анонсирует префиксы IPv6, а не подсети IPv4. Сообщения передаются в пакетах IPv6, многие из которых следуют на многоадресатный адрес IPv6 FF02::A. Но большинство основных концепций аналогично таковым у протокола EIGRP для IPv4.

Настройка протокола EIGRPv6 требует тех же этапов для всех протоколов маршрутизации. Должен быть создан процесс протокола маршрутизации EIGRPv6, а затем протокол должен быть разрешен на разных интерфейсах. Остальная часть конфигурации EIGRPv6 необязательна, она подразумевает изменение стандартной настройки и происходящего между соседями при вычислении метрики и т.д.

Первый раздел посвящен наиболее распространенным командам конфигурации EIGRPv6, а также некоторым другим командам, изменяющим второстепенные параметры.

Основы конфигурации EIGRPv6

Конфигурация протокола EIGRPv6 очень похожа на конфигурацию OSPFv3. Таким образом, команды создают процесс EIGRPv6 в одной части конфигурации, а подкоманды интерфейса разрешают протокол маршрутизации на интерфейсе. Основные принципы базовой конфигурации для протокола IPv6 приведены на рис. 18.1.



Рис. 18.1. Основы конфигурации EIGRPv6

Если вы помните конфигурацию EIGRPv4, то быстро заметите основное отличие между конфигурацией на рис. 18.1 и тем, что помните о EIGRPv4. В примере на рисунке не используются команды EIGRP `network` вообще, поскольку протокол

EIGRPv6 даже не поддерживает команду `network`, а вместо нее использует подкоманду интерфейса `ipv6 eigrp` *`номер_автономной_системы`*. Процесс проходит так же, как и в конфигурации OSPFv3, описанный ранее в главе, но с небольшими отличиями в командах для EIGRPv6.

Остальная часть команд конфигурации EIGRPv6 работает либо точно так, как команды EIGRPv4, либо очень похоже на них. Для демонстрации подобий в табл. 18.1 представлены параметры настройки EIGRPv4 из главы 10 для сравнения с подобными параметрами настройки EIGRPv6.



Таблица 18.1. Сравнение команд конфигурации EIGRPv4 и EIGRPv6

Функция	EIGRPv4	EIGRPv6
Создать процесс, определить номер ASN	`router eigrp` *`номер_автономной_системы`*	`ipv6 router eigrp` *`номер_автономной_системы`*
Определить идентификатор маршрутизатора явно (режим маршрутизатора)	`eigrp router-id` *`значение`*	Идентично
Изменить значение параллельных маршрутов (режим маршрутизатора)	`maximum-paths` *`значение`*	Идентично
Установить множитель вариации (режим маршрутизатора)	`variance` *`множитель`*	Идентично
Установить вычисление метрики (режим интерфейса)	`bandwidth` *`значение`* `delay` *`значение`*	Идентично
Изменение таймеров Hello и Hold (режим интерфейса)	`ip hello-interval eigrp` *`номер_автономной_системы время`* `ip hold-time eigrp` *`номер_автономной_системы время`*	Замена `ip` на `ipv6`
Разрешить протокол EIGRP на интерфейсе	`network` *`IP-адрес`* [*`шаблон_маски`*]	`ipv6 eigrp` *`номер_автономной_системы`* (подкоманда интерфейса)
Отключить и разрешить автоматическое суммирование (режим маршрутизатора)	`[no] auto-summary`	Для EIGRPv6 не нужно

Пример конфигурации EIGRPv6

Чтобы продемонстрировать конфигурацию EIGRPv6 в контексте, рассмотрим пример объединенной сети на рис. 18.2. Здесь представлены подсети IPv6 и последний квартет IPv6-адреса интерфейса каждого маршрутизатора как ::X, где X — это номер маршрутизатора, чтобы было очевидней, к какому маршрутизатору какой адрес относится.

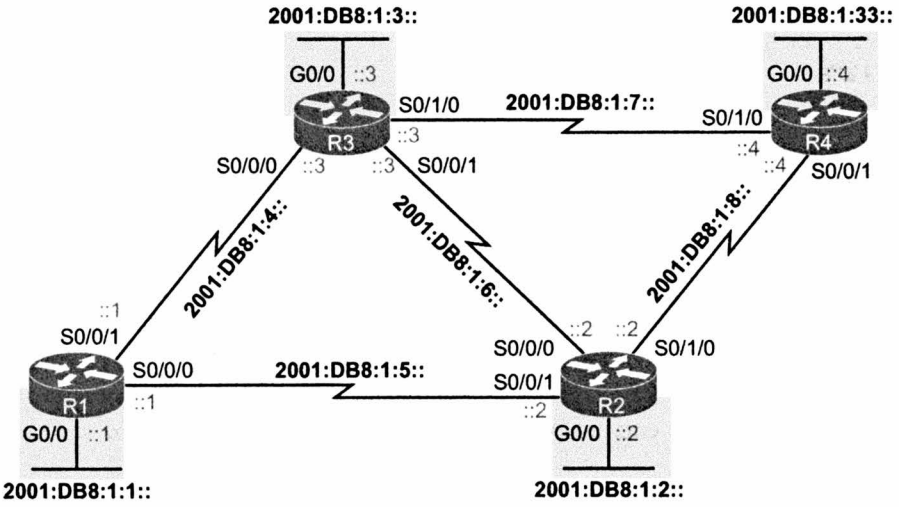


Рис. 18.2. Объединенная сеть примера многообластной конфигурации EIGRPv6

Обратите внимание, что рис. 18.2 похож на рис. 10.3, использовавшийся в нескольких примерах протокола EIGRPv4 в главе 10. На рис. 18.2 используются те же типы интерфейсов, номера и имена маршрутизаторов. Фактически здесь используется подобная схема нумерации подсетей. Рассмотрим, например, четыре подсети IPv6 на базе LAN — это подсети 1, 2, 3 и 33, их номера совпадают со значением последнего квартета. Та же схема нумерации подсетей использована в примерах главы 10, номера подсетей IPv4, также 1, 2, 3 и 33, соответствуют третьему октету.

Почему подобие объединенных сетей, используемых в этой главе и главе 10, имеет значение? Мало того, что подобны команды конфигурации EIGRP, но и вывод команд `show` также подобен. Команды `show` в этой главе, при использовании той же топологии сети, обеспечивают практически тот же вывод для протокола EIGRPv6, что и для EIGRPv4.

Данный конкретный пример 18.1 начинается с вывода дополнительной конфигурации IPv6, необходимой на маршрутизаторе R1, чтобы сделать его маршрутизатором двойного стека и добавить конфигурацию EIGRPv6. Выделенные строки — это специфические для протокола EIGRPv6 команды конфигурации, а остальная часть команд добавляет конфигурацию маршрутизации IPv6 и IPv6-адресации.

Пример 18.1. Конфигурация IPv6 и EIGRPv6 на маршрутизаторе R1

```
ipv6 unicast-routing
!
ipv6 router eigrp 1
eigrp router-id 1.1.1.1
!
interface GigabitEthernet0/0
ipv6 address 2001:db8:1:1::1/64
ipv6 eigrp 1
!
interface serial 0/0/0
```

```
description link to R2
ipv6 address 2001:db8:1:5::1/64
ipv6 eigrp 1
!
interface serial 0/0/1
description link to R3
ipv6 address 2001:db8:1:4::1/64
ipv6 eigrp 1
```

В первом примере уделим время полному обзору конфигурации. Все маршрутизаторы должны использовать тот же номер автономной системы EIGRPv6 (номер ASN), заданный глобальной командой `ipv6 router eigrp` *номер_автономной_системы*. Только после этой команды маршрутизатор R1 явно устанавливает свой идентификатор маршрутизатора EIGRP (RID) командой `eigrp router-id`. Обратите внимание, что протокол EIGRPv6 использует 32-разрядный RID, как и OSPFv3, с теми же правилами выбора значения.

Остальная часть конфигурации просто разрешает протокол EIGRPv6 на каждом интерфейсе, указывая правильный процесс EIGRPv6 и номер ASN в подкоманде интерфейса `ipv6 eigrp` *номер_автономной_системы*.

В примере 18.2 приведена конфигурация на втором маршрутизаторе (R2). И здесь также используется номер ASN 1, поскольку он должен совпадать с номером ASN, используемым маршрутизатором R1. В противном случае эти два маршрутизатора не станут соседями. Кроме того, обратите внимание, что маршрутизатор R2 устанавливает свой RID как 2.2.2.2.

Пример 18.2. Конфигурация EIGRPv6 на маршрутизаторе R2

```
ipv6 unicast-routing
!
ipv6 router eigrp 1
eigrp router-id 2.2.2.2
!
interface GigabitEthernet0/0
ipv6 address 2001:db8:1:2::2/64
ipv6 eigrp 1
!
interface serial 0/0/0
description link to R3
ipv6 address 2001:db8:1:6::2/64
ipv6 eigrp 1
!
interface serial 0/0/1
description link to R1
ipv6 address 2001:db8:1:5::2/64
ipv6 eigrp 1
!
interface serial 0/1/0
description link to R4
ipv6 address 2001:db8:1:8::2/64
ipv6 eigrp 1
```

ВНИМАНИЕ!

Используя команды `shutdown` и `no shutdown` в режиме конфигурации EIGRP, операционная система IOS позволяет отключить процесс маршрутизации EIGRPv6, а затем вновь запустить его. В примерах 18.1 и 18.2 нет команды `no shutdown`, поскольку версия операционной системы IOS, используемая на маршрутизаторах примеров этой книги (15.2 (M)), изначально находится в состоянии разрешения (`no shutdown`). Но в более ранних версиях IOS протокол EIGRPv6 изначально отключен, что требует команды `no shutdown` в режиме конфигурации EIGRP, прежде чем протокол EIGRPv6 заработает.

Другие параметры конфигурации EIGRPv6

В предыдущем примере были представлены основы конфигурации EIGRPv6. Ниже описано несколько параметров настройки в сравнении с таковыми в EIGRPv4.

Установка ширины полосы пропускания и задержки, влияющих на выбор маршрута EIGRPv6

Стандартно при вычислении метрик каждого маршрута протокол EIGRPv6 использует те же параметры, что и протокол EIGRPv4. Но если быть абсолютно точным, то параметры вовсе не подобны, просто используется тот же синтаксис команды. Протокол EIGRPv6 использует те же параметры, что и EIGRPv4: полосу пропускания интерфейса и задержку, задаваемые подкомандами интерфейса `bandwidth` и `delay`. Изменение этих значений влияет на вычисление метрик как протокола EIGRPv4, так и EIGRPv6.

Для вычисления метрик маршрута протокол EIGRPv6 использует ту же формулу, что и EIGRPv4. В результате при некоторых условиях метрика EIGRPv4 для маршрута к подсети IPv4 будет той же, что и метрика EIGRPv6 для того же маршрута к подсети IPv6 в той же области.

Например, все маршрутизаторы на рис. 18.3 являются маршрутизаторами двойного стека с разрешенными протоколами EIGRPv4 и EIGRPv6 на всех интерфейсах в проекте. Выделенная в правом верхнем углу подсеть 10.1.33.0/24 — это та же подсеть, что и 33 (2001:DB8:1:33::/64) протокола IPv6. Процессы EIGRPv4 и EIGRPv6 на маршрутизаторе R1 вычислят точно ту же метрику для этих маршрутов на основании тех же значений параметров полосы пропускания и задержки интерфейсов.

В примере 18.3 показаны маршруты IPv4 и IPv6 на маршрутизаторе R1 к подсетям, представленным на рис. 18.3. Обратите внимание, что во всех случаях выделены метрики 2 684 416.

На маршрутизаторе R1 обе команды выводят для подсети 33 два маршрута равной стоимости, но формат вывода немного отличается. Формат команды `show ip route` помещает подсеть назначения в ту же первую строку, что и инструкции перенаправления первого маршрута. Команда `show ipv6 route` указывает префикс назначения в первой строке, а инструкции перенаправления каждого маршрута — во второй и в третьей строках соответственно.

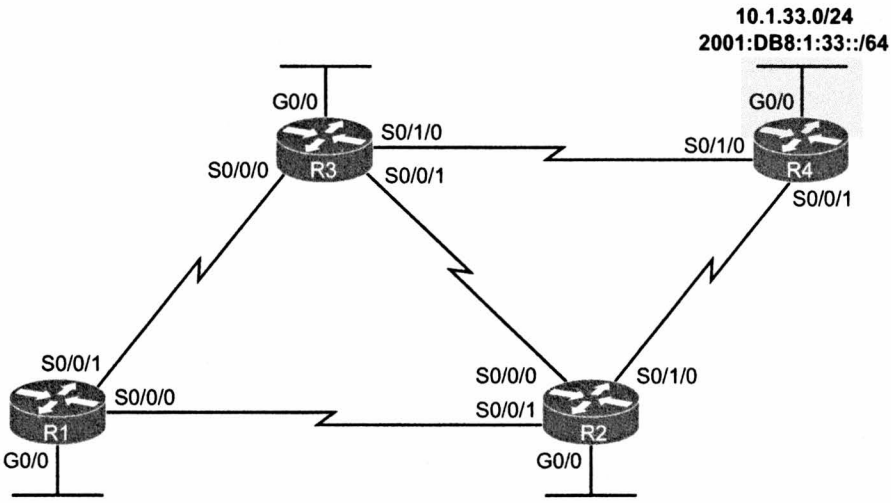


Рис. 18.3. Тот же маршрут через маршрутизатор R4 к подсетям IPv4 33 и IPv6 33

Пример 18.3. Одинаковые метрики для маршрутов IPv4 и IPv6 по протоколам EIGRPv4 и EIGRPv6

```
R1# show ip route | section 10.1.33.0
D     10.1.33.0/24 [90/2684416] via 10.1.5.2, 00:02:23, Serial0/0/0
                   [90/2684416] via 10.1.4.3, 00:02:23, Serial0/0/1

R1# show ipv6 route | section 2001:DB8:1:33::/64
D     2001:DB8:1:33::/64 [90/2684416]
       via FE80::FF:FE00:3, Serial0/0/1
       via FE80::FF:FE00:2, Serial0/0/0
```

Балансировка нагрузки EIGRP

Протоколы EIGRPv6 и EIGRPv4 используют те же концепции и тот же синтаксис команд конфигурации для балансировки нагрузки с одинаковыми и неодинаковыми стоимостями. Но у протокола EIGRPv6 есть собственные параметры конфигурации, задаваемые командами `maximum-paths` и `variance` в режиме конфигурации EIGRPv6. У протокола EIGRPv4 это отдельные параметры, для которых используются те же две команды в режиме конфигурации EIGRPv4.

Предположим, например, что в сети двойного стека маршрутизаторы используют протоколы EIGRPv4 и EIGRPv6. Сетевой инженер, вероятно, выберет одинаковые параметры `variance` и `maximum-paths` для обоих протоколов маршрутизации. Чтобы продемонстрировать различия, предположим, что инженер решил выбрать разные параметры.

- **EIGRPv4**. Максимум два маршрута с вариацией 3 для маршрутов неравной стоимости.
- **EIGRPv6**. Максимум пять маршрутов с вариацией 4 для маршрутов неравной стоимости.

В примере 18.4 показано, как задать эти параметры для двух разных процессов маршрутизации, однако команды используют практически тот же синтаксис.

Пример 18.4. Установка параметров балансировки нагрузки по каждому процессу маршрутизации

```
R1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
! Сначала настройка параметров для IPv4
R1(config)# router eigrp 10
R1(config-router)# maximum-paths 2
R1(config-router)# variance 3
! Затем, настройка подобных параметров для IPv6
R1(config-router)# ipv6 router eigrp 11
R1(config-rtr)# maximum-paths 5
R1(config-rtr)# variance 4
R1(config-rtr)# ^Z
R1#
```

Таймеры EIGRP

Протоколы EIGRPv6 и EIGRPv4 используют те же концепции таймеров для Hello и Hold. Для установки их разных значений для каждого процесса маршрутизации операционная система IOS предоставляет команды с несколько разным синтаксисом для протоколов EIGRPv6 и EIGRPv4: в командах EIGRPv6 используется ключевое слово `ipv6`, а не `ip`. В остальном синтаксис команд EIGRPv6 аналогичен таковому у их версий EIGRPv4.

В примере 18.5 показано изменение таймеров Hello EIGRPv4 и EIGRPv6 двумя разными командами. Для протокола EIGRPv4 таймер Hello установлен на 6 секунд, для EIGRPv6 — на 7 секунд.

Пример 18.5. Установка таймеров Hello EIGRPv4 и EIGRPv6

```
R1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)# interface gigabitethernet0/1
R1(config-if)# ip hello-interval eigrp 10 6
R1(config-if)# ipv6 hello-interval eigrp 11 7
R1(config-rtr)# ^Z
R1#
```

Значения таймеров выбраны произвольно, только для демонстрации команд для каждого протокола маршрутизации. В реальных сетях эти параметры, вероятно, будут иметь одинаковые значения и для EIGRPv4, и для EIGRPv6.

Концепции, проверка, поиск и устранение неисправностей EIGRPv6

Протоколы EIGRPv4 и EIGRPv6 ведут себя почти одинаково. В табл. 18.1 были приведены команды конфигурации, чтобы показать их сходства. В этом разделе по-

дробней рассматривается проверка, поиск и устранение неисправностей EIGRPv6 в сравнении с таковыми у протокола EIGRPv4.

В работе протоколов EIGRPv6 и EIGRPv4 очень много подобного, практически они одинаковы, за исключением нескольких следующих различий.

Ключевая тема

Различия в концепциях EIGRPv4 и EIGRPv6

- Протокол EIGRPv6 анонсирует префиксы IPv6, а протокол EIGRPv4 — подсети IPv4.
- Команды `show` протокола EIGRPv6 используют ключевое слово `ipv6` там, где команды `show` протокола EIGRP используют ключевое слово `ip`.
- У протокола EIGRPv6 тот же список требований к соседям, но маршрутизаторы EIGRPv6 могут стать соседями, только если их IPv6-адреса находятся в разных подсетях. (Адреса соседей EIGRPv4 должны быть в той же подсети IPv4.)
- В отличие от протокола EIGRPv4, у EIGRPv6 нет концепции автоматического суммирования.

Как можно заметить, список упомянутых здесь различий очень короткий. Множество примеров вывода команд `show`, приведенных далее, сделают подобия еще более очевидными. Для начала на рис. 18.4 приведен обзор EIGRPv6 команд `show`, обсуждавшихся в этой главе. Обратите внимание, что все команды используют тот же синтаксис, что и их эквивалент EIGRPv4, но ключевое слово `ip` заменено на `ipv6`.

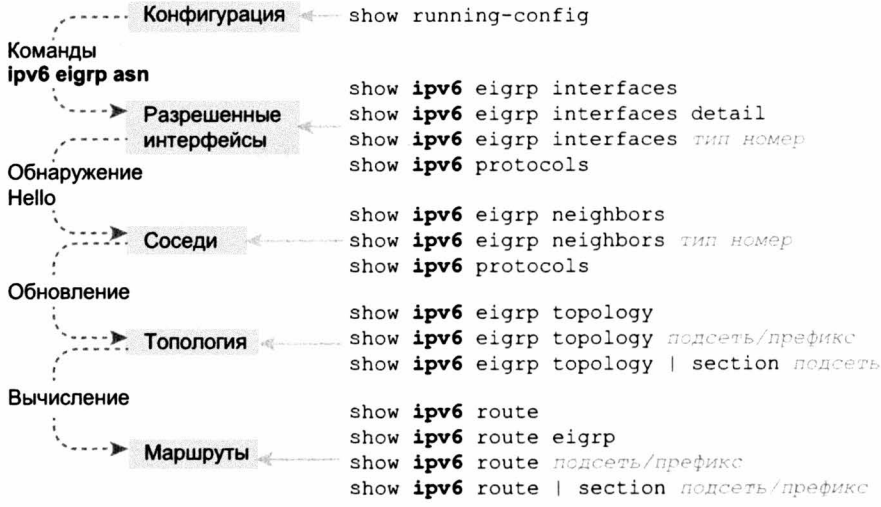


Рис. 18.4. Команды проверки EIGRPv6

Как и в предыдущей главе, второй главный раздел этой главы следует той же общей схеме: сначала рассматриваются интерфейсы EIGRPv6, затем соседские отношения, топология и наконец маршруты IPv6.

ВНИМАНИЕ!

Во всех примерах поиска и устранения неисправностей в остальной части этой главы используется конфигурация примера с маршрутизаторами R1, R2, R3 и R4, показанная на рис. 18.2.

Интерфейсы EIGRPv6

Разрешив протокол EIGRPv6 на интерфейсе, маршрутизатор должен сделать следующее.

1. Обнаружить соседей EIGRPv6 на этом интерфейсе.
2. Анонсировать префикс, подключенный к этому интерфейсу.

Проверяя работу протокола EIGRPv6, инженер должен удостовериться, что он разрешен на правильных интерфейсах. Другими словами, с точки зрения поиска и устранения неисправностей причиной наиболее распространенных проблем EIGRPv6 является отсутствие разрешения протокола EIGRPv6 на интерфейсе маршрутизатора.

Как и в случае EIGRPv4, одни команды EIGRPv6 выводят все интерфейсы, на которых разрешен протокол EIGRP (включая пассивные), другие выводят все интерфейсы EIGRP, указывая, какие из них пассивны, а некоторые просто не выводят пассивные интерфейсы. Эти различия показаны в примере 18.6, с учетом, что интерфейс G0/0 маршрутизатора R1 является пассивным. Как можно заметить, в выводе команды `show ipv6 eigrp interfaces` интерфейс G0/0 отсутствует, а в выводе команды `show ipv6 protocols` он есть, но отмечен как пассивный.

Пример 18.6. Проверка интерфейсов OSPFv3 и связанных параметров

```
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)# ipv6 router eigrp 1
R1(config-rtr)# passive-interface g0/0
R1(config-rtr)# ^Z
R1#
R1# show ipv6 eigrp interfaces
EIGRP-IPv6 Interfaces for AS(1)
                Xmit Queue   Mean Pacing Time Multicast   Pending
Interface Peers Un/Reliable SRTT Un/Reliable Flow Timer Routes
Se0/0/0   1     0/0         1    0/15        50         0
Se0/0/1   1     0/0         1    0/15        50         0

R1# show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "eigrp 1"
EIGRP-IPv6 Protocol for AS(1)
  Metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  NSF-aware route hold timer is 240
  Router-ID: 1.1.1.1
  Topology : 0 (base)
    Active Timer: 3 min
    Distance: internal 90 external 170
    Maximum path: 16
    Maximum hopcount 100
    Maximum metric variance 1
```

```
  Interfaces:
    Serial0/0/0
    Serial0/0/1
    GigabitEthernet0/0 (passive)
  Redistribution:
    None
IPv6 Routing Protocol is "ND"
```

Обратите внимание, что команда `show ipv6 eigrp interfaces` выводит несколько строк по каждому интерфейсу. Кроме того, команда `show ipv6 protocols` выводит все интерфейсы с поддержкой EIGRP, включая пассивные.

Теперь остановимся на поиске и устранении неисправностей, связанных с интерфейсами EIGRPv6. Как и в случае с протоколом OSPF, поиск и устранение неисправностей в основном сосредоточивается на соседских отношениях. Тем не менее ниже приведены две вероятные проблемы, связанные с интерфейсами.



Возможные проблемы EIGRPv6, связанные с интерфейсами

- Отсутствие подкоманды интерфейса `ipv6 eigrp` *номер_автономной_системы* на интерфейсе, у которого нет возможных соседей, вполне может остаться незамеченным. Этот пропуск не повлияет на соседей EIGRPv6, но он означает, что протокол EIGRPv6 не разрешен на этом интерфейсе, а потому маршрутизатор не будет анонсировать подключенную подсеть. Эта проблема обнаруживается как отсутствующий маршрут.
- Если интерфейс EIGRPv6 сделан пассивным, когда к его каналу связи подключен потенциальный сосед EIGRPv6, то это воспрепятствует формированию этими двумя маршрутизаторами соседских отношений. Обратите внимание, что для утраты соседских отношений достаточно наличия пассивного интерфейса только на одном из двух маршрутизаторов.

Рассмотрим маршрутизатор R4 в примере сети этой главы. Его интерфейс G0/0 подключен к сети LAN без других маршрутизаторов. В настоящее время конфигурация маршрутизатора R4 включает подкоманду интерфейса `ipv6 eigrp 1` на интерфейсе G0/0. Если бы эта команда по ошибке отсутствовала (или была удалена в ходе лабораторного эксперимента), маршрутизатор R4 не анонсировал бы маршрут для подключенной подсети (подсети 33, или 2001:DB8:1:33::/64).

В примере 18.7 приведен данный конкретный случай. Чтобы воссоздать проблему, перед вводом команд в примере 18.7 на интерфейсе G0/ маршрутизатора R4 была введена команда `no ipv6 eigrp 1`, запретившая протокол EIGRP на этом интерфейсе. В примере 18.7 маршрутизатор R1 не имеет маршрута к подсети 33 или топологических данных EIGRP.

Пример 18.7. Отсутствие маршрута к подсети 33 на маршрутизаторе R1

```
R1# show ipv6 route 2001:DB8:1:33::
% Route not found

R1# show ipv6 eigrp topology | include 2001:DB8:1:33
R1#
```

Соседи EIGRPv6

С одной стороны, соседские отношения EIGRP довольно просты. Когда два маршрутизатора EIGRPv6 находятся на том же канале связи, они обнаруживают друг друга при помощи сообщений Hello EIGRPv6. Эти сообщения содержат несколько параметров, и соседи проверяют их, чтобы определить, могут ли эти маршрутизаторы стать соседями.

- Если параметры подходящие, каждый маршрутизатор добавляет другой маршрутизатор в свою таблицу соседних устройств EIGRPv6, выводимую командой `show ipv6 eigrp neighbors`.
- Если параметры не подходят, маршрутизаторы не становятся соседями и не добавляют друг друга в свои таблицы соседних устройств, и в выводе команды `show ipv6 eigrp neighbors` они не отображаются.

С другой стороны, при поиске и устранении неисправностей соседских отношений EIGRP следует помнить множество мелких деталей, включая списки параметров соседей, требующих соответствия. В то же время воспрепятствовать соседским отношениям маршрутизаторов могут и другие проблемы. К счастью, их списки для протоколов EIGRPv6 и EIGRPv4 практически совпадают, но с одним существенным различием: протокол EIGRPv6 не требует, чтобы соседи находились в той же подсети.

Учитываемые при поиске и устранении неисправностей соседских отношений EIGRP факторы приведены в табл. 18.2.



Таблица 18.2. Требования к соседям в протоколах EIGRPv4 и EIGRPv6

Требование	EIGRPv4	EIGRPv6
Интерфейсы должны быть в рабочем состоянии (`up/up`)	Да	Да
Интерфейсы должны относиться к той же подсети	Да	Нет
Списки (ACL) не должны фильтровать сообщения протокола маршрутизации	Да	Да
Аутентификация, если она настроена, должна пройти успешно	Да	Да
В командах конфигурации маршрутизатора должен использоваться тот же номер ASN	Да	Да
Коэффициенты K должны совпадать	Да[1]	Да[1]
Таймеры Hello и Hold должны совпадать	Нет	Нет
Идентификаторы маршрутизаторов (Router ID) должны быть уникальными	Нет[2]	Нет[2]

[1] Коэффициенты K определяют алгоритм вычисления метрики EIGRP. В данной книге не обсуждается изменение этих параметров, так как компания Cisco рекомендует оставлять их как есть.

[2] Дублирующиеся идентификаторы маршрутизаторов в протоколе EIGRP не препятствуют установлению соседских отношений, но могут создать проблемы при добавлении внешних маршрутов EIGRP в таблицу маршрутизации.

Например, все четыре маршрутизатора в примере конфигурации этой главы использовали номер ASN 1 протокола EIGRPv6. Но предположим, что в конфигура-

ции маршрутизатора R2 ошибочно использован номер ASN 2, в то время как три других маршрутизатора правильно использовали номер ASN 1. Что будет? Маршрутизатор R2 окажется не в состоянии сформировать соседские отношения с любым из других маршрутизаторов.

Номер ASN упоминается во многих командах EIGRPv6 `show`. Например, команда EIGRPv6 `show ipv6 protocols` демонстрирует это значение в нескольких очевидных местах (см. пример 18.6).

При поиске и устранении неисправностей на экзамене помните, что каждая пара маршрутизаторов EIGRPv6 на том же канале связи должна стать соседями. Таким образом, если в экзаменационном вопросе указано на некую проблему маршрутизации IPv6, проверьте соседские отношения EIGRP маршрутизаторов и удостоверьтесь, что все они существуют. Если они где-то отсутствуют, начните поиск и устранение неисправностей соседских отношений EIGRPv6, руководствуясь табл. 18.2.

Для обследования соседей используйте команду `show ipv6 eigrp neighbors`. Из-за длины IPv6-адресов команда выводит соседей в двух строках, а не в одной (как в версии EIGRPv4 этой команды). В примере 18.8 показан вывод этой команды на маршрутизаторе R2 с двумя выделенными строками для одного соседа (R3).

Пример 18.8. Соседи EIGRPv6 маршрутизатора R2

```
R2# show ipv6 eigrp neighbors
EIGRP-IPv6 Neighbors for AS(1)
H   Address                 Interface   Hold Uptime   SRTT   RTO  Q  Seq
                                        (sec)         (ms)       Cnt Num
2   Link-local address:     Se0/1/0     10 06:37:34   104    624  0  13
    FE80::D68C:B5FF:FE6B:DB48
1   Link-local address:     Se0/0/0     11 06:37:54   1      100  0  38
    FE80::FF:FE00:3
0   Link-local address:     Se0/0/1     11 06:46:11   1      100  0  30
    FE80::FF:FE00:1
```

Уделим минуту IPv6-адресам на интерфейсе в двух выведенных строках. Вывод команды на маршрутизаторе R2 содержит локальный в пределах канала связи адрес маршрутизатора R3, находящегося на другом конце кабеля, подключенного к интерфейсу S0/0/0 маршрутизатора R2. Указанный интерфейс S0/0/0 принадлежит маршрутизатору R2. В результате команда выводит интерфейс локального маршрутизатора и локальный в пределах канала связи адрес соседа. Таким образом, чтобы идентифицировать соседа EIGRPv6, необходимо использовать локальный в пределах канала связи адрес этого соседа (а не его RID EIGRPv6).

Топологическая база данных EIGRPv6

В этой книге уже неоднократно упоминалось, что как только маршрутизаторы EIGRPv6 становятся соседями, они должны обменяться всеми топологическими данными. Хоть это и не рассматривается в данной книге, но некоторые средства маршрутизатора способны фильтровать передаваемые топологические данные. Но в принципе можно считать, что если маршрутизаторы стали соседями, то они обмениваются топологическими данными.

Однако следует быть готовым интерпретировать значение некоторых из топологических данных, описанных в протоколе EIGRPv6. К счастью, топологические данные EIGRPv6 точно такие же, как и в протоколе EIGRPv4, кроме одного очевидного различия: в них указаны префиксы IPv6. Идентичные концепции приведены ниже.

- Компоненты метрики (ширина полосы пропускания, задержка, надежность, загруженность).
- Для вычисления метрики используется тот же математический механизм.
- Концепция оптимального маршрута (наилучшего).
- Концепция маршрутов FS.
- Условие резервирования, при котором анонсируемое расстояние (сообщаемая соседом составная метрика) ниже (лучше), чем метрика локального маршрутизатора.

Например, на рис. 18.5 приведен фрагмент вывода команды `show ipv6 eigrp topology`. Приведены также топологические данные маршрутизатора R1 для подсети 3 (2001:DB8:1:3::/64), подключенной к его интерфейсу LAN G0/0. Слева представлены две детали, характерные для протокола IPv6: префикс/длина и локальный в пределах канала связи адрес следующего транзитного маршрутизатора.

Обратите внимание, что хотя слева приведен префикс IPv6 и адрес следующего транзитного маршрутизатора IPv6, справа представлены те же идеи, что и в EIGRPv4. Фактически этот пример аналогичен примеру из главы 10, представленному на рис. 10.4. Там также представлены топологические данные из базы маршрутизатора R1 для подсети на интерфейсе LAN G0/0 маршрутизатора R3. Однако то был пример для протокола EIGRPv4 и подсети 10.1.3.0/24. Если вернуться к рис. 10.4, то можно заметить все те же данные справа, полученные на основании топологической базы данных EIGRPv4, но слева приведена информация IPv4 о подсети, маске и адресе следующей транзитной точки перехода.

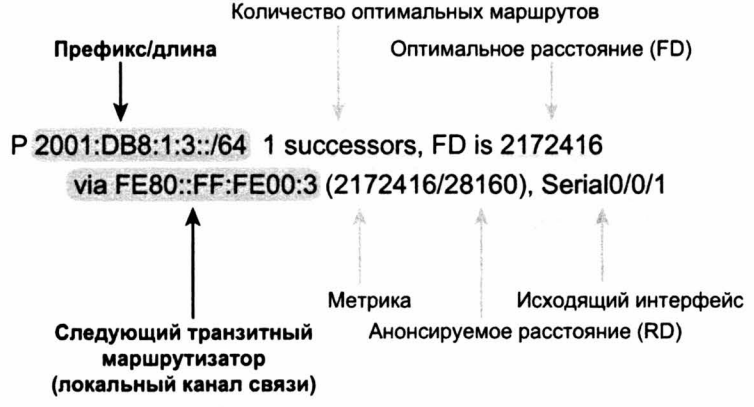


Рис. 18.5. Сравнение подробностей IPv6 с общими элементами топологических данных EIGRP

Короче говоря, подробности о компонентах метрики, формулах их вычисленная, оптимальном маршруте, маршруте FS и так далее см. в главе 10. Если вы владеете этими подробностями для протокола EIGRPv4, то владеете ими и для протокола EIGRPv6.

Для полного понимания внутренней организации протокола EIGRPv6 в примере 18.9 приведена таблица топологии EIGRP. Вывод демонстрирует топологические данные маршрутизатора R1 для подсети 3 (2001:DB8:1:3::/64). Первая выделенная строка отображает адрес следующей транзитной точки перехода и исходящий интерфейс. Во второй выделенной строке следует составная метрика (т.е. метрика, вычисленная по разным компонентам метрики). В двух следующих выделенных строках показаны два компонента метрики, влияющие на вычисление (стандартно): ширина полосы пропускания и задержка. И наконец, обратите внимание, что протокол EIGRP использует здесь минимальную ширину полосы пропускания (1544 Кбит/с) и полную задержку (20 100).

Пример 18.9. Соседи EIGRPv6 маршрутизатора R1

```
R1# show ipv6 eigrp topology 2001:DB8:1:3::/64
EIGRP-IPv6 Topology Entry for AS(1)/ID(1.1.1.1) for 2001:DB8:1:3::/64
State is Passive, Query origin flag is 1, 1 Successor(s), FD is 2172416
Descriptor Blocks:
FE80::FF:FE00:3 (Serial0/0/1), from FE80::FF:FE00:3, Send flag is 0x0
  Composite metric is (2172416/28160), route is Internal
  Vector metric:
    Minimum bandwidth is 1544 Kbit
    Total delay is 20100 microseconds
    Reliability is 255/255
    Load is 1/255
    Minimum MTU is 1500
    Hop count is 1
    Originating router is 3.3.3.3
FE80::FF:FE00:2 (Serial0/0/0), from FE80::FF:FE00:2, Send flag is 0x0
  Composite metric is (2684416/2172416), route is Internal
  Vector metric:
    Minimum bandwidth is 1544 Kbit
    Total delay is 40100 microseconds
    Reliability is 255/255
    Load is 1/255
    Minimum MTU is 1500
    Hop count is 2
```

Маршруты IPv6 EIGRPv6

Проверка маршрутов, изученных по протоколу EIGRPv6, относительно проста, если помнить значение кода D. В примере 18.10 приведена вся таблица маршрутизации IPv6 маршрутизатора R1 с шестью маршрутами IPv6, изученными по протоколу EIGRP.

Пример 18.10. Маршруты EIGRPv6 на маршрутизаторе R1

```
R1# show ipv6 route
IPv6 Routing Table - default - 13 entries
```

```
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, I1 - ISIS L1, I2 - ISIS L2
       IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - Neighbor Discovery, l - LISP
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1
       OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
C    2001:DB8:1:1::/64 [0/0]
      via GigabitEthernet0/0, directly connected
L    2001:DB8:1:1::1/128 [0/0]
      via GigabitEthernet0/0, receive
D    2001:DB8:1:2::/64 [90/2172416]
      via FE80::FF:FE00:2, Serial0/0/0
D    2001:DB8:1:3::/64 [90/2172416]
      via FE80::FF:FE00:3, Serial0/0/1
C   2001:DB8:1:4::/64 [0/0]
      via Serial0/0/1, directly connected
L    2001:DB8:1:4::1/128 [0/0]
      via Serial0/0/1, receive
C    2001:DB8:1:5::/64 [0/0]
      via Serial0/0/0, directly connected
L    2001:DB8:1:5::1/128 [0/0]
      via Serial0/0/0, receive
D    2001:DB8:1:6::/64 [90/2681856]
      via FE80::FF:FE00:3, Serial0/0/1
      via FE80::FF:FE00:2, Serial0/0/0
D    2001:DB8:1:7::/64 [90/2681856]
      via FE80::FF:FE00:3, Serial0/0/1
D    2001:DB8:1:8::/64 [90/2681856]
      via FE80::FF:FE00:2, Serial0/0/0
D    2001:DB8:1:33::/64 [90/2684416]
      via FE80::FF:FE00:3, Serial0/0/1
      via FE80::FF:FE00:2, Serial0/0/0
L    FF00::/8 [0/0]
      via Null0, receive
```

Две выделенные строки ближе к середине примера описывают один маршрут к подсети IPv6 3 (2001:DB8:1:3::/64). Для каждого маршрута выводится по крайней мере по две строки, в первой указаны префикс/длина, а в скобках — административное расстояние и метрика (оптимальное расстояние). Вторая строка выводит инструкции перенаправления для маршрута.

Когда у маршрутизатора есть несколько маршрутов к префиксу IPv6, первая строка вывода содержит префикс, а последующие строки содержат каждый маршрут. Строки каждого маршрута содержат инструкции перенаправления (локальный в пределах канала связи адрес соседа и исходящий интерфейс локального маршрутизатора). Выделенные строки в конце примера, для подсети 33, демонстрируют такой пример с двумя маршрутами, каждый со своим адресом следующей транзитной точки перехода и разными исходящими интерфейсами.

Что касается поиска и устранения неисправностей маршрутов IPv6, то по большей части они начинаются с вопросов о соседях. Поиск потенциальных проблем EIGRPv6 фактически следует той же логике, что и OSPFv3. Повторим логику случаев из предыдущей главы. Если у маршрутизатора нет маршрута к данной подсети (например, если у маршрутизатора R1 вообще нет никакого маршрута к подсети 33), то имеет смысл сделать следующее.



Общие действия EIGRPv6 в отсутствие маршрутов

Этап 1 Проверьте маршрутизаторы с интерфейсами, непосредственно подключенными к этому префиксу IPv6. Прежде чем протокол EIGRPv6 начнет анонсировать подсеть, на том интерфейсе маршрутизатора должен быть разрешен протокол EIGRPv6

Этап 2 Проверьте соседские отношения EIGRPv6 всех маршрутизаторов между локальным маршрутизатором и маршрутизаторами с интерфейсом, подключенным к префиксу X IPv6

Например, если бы на рис. 18.2 у маршрутизатора R4 не было команды `ipv6 eigrp 1` на интерфейсе G0/0, то у всех маршрутизаторов были бы правильные соседские отношения EIGRPv6, но маршрутизатор R4 не анонсировал бы подсеть 33.

Если у маршрутизатора есть маршрут, но это неправильный (неоптимальный) маршрут, имеет смысл сделать следующее.



Общие действия EIGRPv6 при наличии неоптимального маршрута

Этап 1 Проверьте исправность соседских отношений по всему оптимальному пути от локального маршрутизатора к префиксу Y

Этап 2 Проверьте параметры задержки и полосу пропускания интерфейса. Обратите особое внимание на самую низкую ширину полосы пропускания по всему маршруту, поскольку при вычислении метрики протокол EIGRP игнорирует более быстрые полосы пропускания, используя только самую низкую (самую медленную)

Обзор

Резюме

- Одним из главных отличий между конфигурациями EIGRPv4 и EIGRPv6 является то, что протокол EIGRPv6 не поддерживает команду `network`.
- Протокол EIGRPv6 использует подкоманду интерфейса `ipv6 eigrp` *`номер_автономной_системы`*.
- При вычислении метрик каждого маршрута протокол EIGRPv6 использует те же параметры, что и протокол EIGRPv4.
- Изменение значений полосы пропускания интерфейса и задержки влияет на вычисление метрик как протокола EIGRPv4, так и EIGRPv6.
- Для вычисления метрик маршрута протокол EIGRPv6 использует ту же формулу, что и протокол EIGRPv4.
- Протоколы EIGRPv6 и EIGRPv4 используют те же концепции и тот же синтаксис команд конфигурации для балансировки нагрузки с одинаковыми и неодинаковыми стоимостями.
- Протоколы EIGRPv6 и EIGRPv4 используют те же концепции таймеров для Hello и Hold.
- Для установки разных значений для каждого процесса маршрутизации операционная система IOS предоставляет команды с несколько разным синтаксисом для протоколов EIGRPv6 и EIGRPv4: в командах EIGRPv6 используется ключевое слово `ipv6`, а не `ip`.
- Протокол EIGRPv6 анонсирует префиксы IPv6, а протокол EIGRPv4 — подсети IPv4.
- У протокола EIGRPv6 тот же список требований к соседям, но маршрутизаторы EIGRPv6 могут стать соседями, только если их IPv6-адреса находятся в разных подсетях. (Адреса соседей EIGRPv4 должны быть в той же подсети IPv4.)
- Разрешив протокол EIGRPv6 на интерфейсе, маршрутизатор должен сделать две вещи: обнаружить соседей EIGRPv6 на этом интерфейсе и анонсировать префикс, подключенный к этому интерфейсу.
- Проверяя работу протокола EIGRPv6, инженер должен удостовериться, что он разрешен на правильных интерфейсах.
- Отсутствие подкоманды интерфейса `ipv6 eigrp` *`номер_автономной_системы`* на интерфейсе, у которого нет возможных соседей, вполне может пройти незамеченным. Этот пропуск не повлияет на соседей EIGRPv6, но он означает, что протокол EIGRPv6 не разрешен на этом интерфейсе, а потому маршрутизатор не будет анонсировать подключенную подсеть. Эта проблема обнаруживается как отсутствующий маршрут.
- Если интерфейс EIGRPv6 сделан пассивным, когда к его каналу связи подключен потенциальный сосед EIGRPv6, то это воспрепятствует формирова-

нию этими двумя маршрутизаторами соседских отношений. Для утраты соседских отношений достаточно наличия пассивного интерфейса только на одном из двух маршрутизаторов.

- Когда два маршрутизатора EIGRPv6 находятся на том же канале связи, они обнаруживают друг друга при помощи сообщений Hello EIGRPv6.
- Как только маршрутизаторы EIGRPv6 становятся соседями, они должны обменяться всеми топологическими данными.
- Когда у маршрутизатора есть несколько маршрутов к префиксу IPv6, первая строка вывода содержит префикс, а последующие строки содержат каждый маршрут.
- Поиск и устранение неисправностей маршрутов IPv6, как правило, начинается с вопросов о соседях.

Контрольные вопросы

Ответьте на эти вопросы. Ответы можно найти на последней странице главы. Полное объяснение ответов приведено в приложении B на веб-сайте.

1. На предприятии используется модель двойного стека, реализующая протоколы IPv4 и IPv6, и протокол маршрутизации EIGRP для обоих. У маршрутизатора R1 есть IPv4- и IPv6-адреса на его интерфейсах G0/0 и S0/0/0, причем на обоих интерфейсах разрешены протоколы EIGRPv4 и EIGRPv6. Какой из следующих способов настройки маршрутизатора R1, разрешающих протокол EIGRPv6 на тех же интерфейсах, что и EIGRPv4, является правильным?

   А) Добавить подкоманду маршрутизатора `dual-stack all-interfaces` для EIGRPv6.

   Б) Добавить подкоманду интерфейса `dual-stack` для интерфейсов G0/0 и S0/0/0

   В) Добавить подкоманду интерфейса `ipv6 eigrp` *`номер_автономной_системы`* для интерфейсов G0/0 и S0/0/0

   Г) Добавить подкоманду маршрутизатора `dual-stack all-interfaces` для EIGRPv4.

2. У какого из следующих параметров конфигурации нет отдельного значения в IPv4/EIGRPv4 и IPv6/EIGRPv6, а используется единый параметр как для EIGRPv4, так и для EIGRPv6?

   А) Полоса пропускания интерфейса.

   Б) Таймер Hello.

   В) Вариация.

   Г) Максимальное количество путей.

3. На предприятии используется модель двойного стека, реализующая протоколы IPv4 и IPv6, и протокол маршрутизации EIGRP для обоих. У маршрутизатора R1 есть IPv4- и IPv6-адреса на его интерфейсах G0/0 и S0/0/0, причем только на обоих интерфейсах разрешены протоколы EIGRPv4 и EIGRPv6, а идентификатор маршрутизатора явно установлен для обоих протоколов. Какие из следующих утверждений истинны для конфигураций EIGRPv4 и EIGRPv6?

А) Конфигурация EIGRPv6 использует глобальную команду `router eigrp` *номер_автономной_системы*.

Б) Оба протокола используют подкоманду маршрутизатора `router-id` *идентификатор_маршрутизатора*.

В) Оба протокола используют подкоманду маршрутизатора `network` *номер_сети*.

Г) Конфигурация EIGRPv6 использует подкоманду интерфейса `ipv6 eigrp` *номер_автономной_системы*.

4. На маршрутизаторе R1 есть три избыточных маршрута IPv6 к подсети IPv6 9 (2009:9:9:9::/64), подключенной к интерфейсу G0/0 маршрутизатора R9. Текущий оптимальный маршрут маршрутизатора R1 использует как следующий транзитный узел маршрутизатор R2 и резервные маршруты через маршрутизаторы R3 и R4. Затем инженер вносит изменения в конфигурацию сети, и маршрутизатор R1 теряет маршруты к подсети 9. Какое из следующих действий приводит к потере маршрутизатором R1 маршрутов к подсети 9?

   А) Сделать интерфейс G0/0 маршрутизатора R9 пассивным.

   Б) Изменить номер ASN EIGRP маршрутизатора R2 на другое число, но сохранить ту же конфигурацию.

   В) Изменить таймеры Hello на всех интерфейсах маршрутизатора R1 с 5 на 4.

   Г) Изменить номер ASN EIGRP маршрутизатора R1 на некое другое число, но сохранить ту же конфигурацию.

5. Маршрутизаторы R1 и R2 подключены к той же сети VLAN. Что из следующего может воспрепятствовать этим двум маршрутизаторам стать соседями EIGRPv6? (Выберите два ответа.)

   А) Несоответствие таймеров Hello.

   Б) Несоответствие номеров ASN.

   В) IPv6-адреса находятся в разных подсетях.

   Г) Используется тот же идентификатор маршрутизатора.

   Д) Один из используемых на канале связи интерфейсов маршрутизатора пассивен.

6. Вывод команды `show ipv6 eigrp neighbors` на маршрутизаторе R2 указывает одного соседа. Какой из следующих ответов правильно интерпретирует вывод команды в этом примере?

```
R2# show ipv6 eigrp neighbors
EIGRP-IPv6 Neighbors for AS(1)
H Address                 Interface Hold Uptime   SRTT   RTO  Q  Seq
                                    (sec)         (ms)       Cnt Num
0 Link-local address:     Gi0/0      11 06:46:11 1      100  0  30
  FE80::FF:FE22.2222
```

   А) FE80::FF:FE22:2222 — локальный в пределах канала связи адрес соседа на общем канале.

   Б) FE80::FF:FE22:2222 — идентификатор соседнего маршрутизатора EIGRPv6.

   В) FE80::FF:FE22:2222 — локальный в пределах канала связи адрес маршрутизатора R2 на общем канале связи.

   Г) FE80::FF:FE22 :2222 — идентификатор EIGRPv6 маршрутизатора R2.

Ключевые темы

Повторите все ключевые темы данной главы, отмеченные пиктограммой "Ключевая тема". Ключевые темы и соответствующие им страницы перечислены в табл. 18.3.

Таблица 18.3. Ключевые темы главы 18

Элемент	Описание	Страница
Табл. 18.1	Сравнение команд конфигурации EIGRPv4 и EIGRPv6	586
Список	Различия в концепциях EIGRPv4 и EIGRPv6	592
Список	Возможные проблемы EIGRPv6, связанные с интерфейсами	594
Табл. 18.2	Требования к соседям в протоколах EIGRPv4 и EIGRPv6	595
Список	Общие действия EIGRPv6 в отсутствие маршрутов	600
Список	Общие действия EIGRPv6 при наличии неоптимального маршрута	600

Заполните таблицы и списки по памяти

Распечатайте приложение Г с веб-сайта или его раздел, относящийся к этой главе, и заполните таблицы и списки по памяти. В приложении Д приведены заполненные таблицы и списки для самоконтроля.

Ключевые термины

После первого прочтения главы попытайтесь дать определения следующим ключевым терминам. Но не расстраивайтесь, если не все получится сразу, в главе 22 описано, как использовать эти термины на завершающем этапе подготовки к экзамену.

номер автономной системы (Autonomous System Number — ASN), протокол EIGRP для IPv6 (EIGRP for IPv6 — EIGRPv6), оптимальный маршрут (successor), резервный маршрут (feasible successor)

Таблицы команд

Хоть и не обязательно заучивать информацию из таблиц данного раздела, ниже приведен список команд конфигурации и пользовательских команд главы. Фактически команды стоит запомнить, чтобы лучше понять содержимое главы и выполнить задания по подготовке к экзамену. Чтобы проверить, насколько хорошо вы запомнили команды, закройте левую сторону таблицы листом бумаги, читайте описания с правой стороны и пытайтесь вспомнить команду.

Таблица 18.4. Конфигурационные команды главы 18

Команда	Описание
`ipv6 router eigrp` *`номер-автономной_системы`*	Глобальная команда, переводящая пользователя в режим конфигурации EIGRP для выбранного номера автономной системы
`ipv6 eigrp` *`номер-автономной_системы`*	Подкоманда интерфейса, разрешающая протокол EIGRPv6 на интерфейсе

Окончание табл. 18.4

Команда	Описание
`maximum-paths` *количество_путей*	Подкоманда маршрутизатора, определяющая максимальное количество маршрутов равной стоимости, которые могут быть добавлены в таблицу маршрутизации
`variance` *множитель*	Подкоманда маршрутизатора, определяющая множитель EIGRP, используемый для определения, достаточно ли метрика маршрута FS близка к метрике оптимального маршрута, чтобы они считались равными
`bandwidth` *ширина_полосы_пропускания*	Подкоманда интерфейса, непосредственно устанавливающая ширину полосы пропускания интерфейса (Кбит/с)
`delay` *значение_задержки*	Подкоманда интерфейса для установки значения задержки интерфейса шагом в десять микросекунд
`ipv6 hello-interval eigrp` *номер_автономной_системы значение_таймера*	Подкоманда интерфейса, устанавливающая интервал Hello EIGRP для данного процесса EIGRP
`ipv6 hold-time eigrp` *номер_автономной_системы значение_таймера*	Подкоманда интерфейса, устанавливающая время задержки EIGRP для данного интерфейса
`eigrp router-id` *идентификатор_маршрутизатора*	Подкоманда маршрутизатора, определяющая идентификатор маршрутизатора EIGRPv6
`[no] shutdown`	Подкоманда маршрутизатора, отключающая (`shutdown`) или включающая (`no shutdown`) процесс EIGRPv6

Таблица 18.5. Команды show главы 18

Команда	Описание
`show ipv6 eigrp interfaces`	Выводит по одной строке на каждый интерфейс, на котором разрешен протокол EIGRP, но он не сделан пассивным командой конфигурации `passive-interface`
`show ipv6 eigrp interfaces` *тип номер*	Выводит статистику по интерфейсам, на которых разрешен протокол EIGRP, но он не сделан пассивным командой конфигурации `passive-interface`
`show ipv6 eigrp interfaces detail` [*тип номер*]	Выводит подробности конфигурации и статистику для всех или только для выбранных интерфейсов, которые разрешены, но не пассивны
`show ipv6 protocols`	Отображает краткую информацию о каждом источнике маршрутной информации, включая интерфейсы с разрешенным протоколом EIGRPv6, и отмечает пассивные интерфейсы
`show ipv6 eigrp neighbors`	Выводит соседей EIGRP и их состояние
`show ipv6 eigrp neighbors` *тип номер*	Выводит соседей EIGRP, доступных для заданного интерфейса
`show ipv6 eigrp topology`	Выводит содержимое таблицы топологии EIGRP, включая оптимальные и резервные маршруты

Окончание табл. 18.5

Команда	Описание
`show ipv6 eigrp topology` *`префикс/длина`*	Выводит подробную топологическую информацию о выбранном префиксе
`show ipv6 eigrp topology | section` *`префикс/длина`*	Выводит подмножество команд `show ipv6 eigrp topology` (только раздел для выбранного префикса/длины)
`show ipv6 route`	Выводит все маршруты IPv4
`show ipv6 route eigrp`	Выводит маршруты в таблице маршрутизации IPv6, изученные по протоколу EIGRPv6
`show ipv6 route` *`префикс/длина`*	Выводит подробное описание маршрута для заданного префикса/длины
`show ipv6 route | section` *`префикс`*	Выводит подмножество команд `show ip route` (только раздел для выбранного префикса)

Ответы на контрольные вопросы:

1 В. 2 А. 3 Г. 4 Г. 5 Б и Д. 6 А.

Обзор части V

Проследите свой прогресс изучения материала части по контрольному списку в следующей таблице. Подробно задачи описаны ниже.

Контрольный список обзора части V

Задача	Первая дата завершения	Вторая дата завершения
Повторите вопросы из обзоров глав		
Ответьте на вопросы обзора части		
Повторите ключевые темы		
Создайте диаграмму связей поиска и устранения неисправностей		
Создайте диаграмму связей команд OSPFV3 и EIGRPV6		

Повторите вопросы из обзоров глав

Ответьте снова на вопросы обзоров глав этой части книги, используя программное обеспечение PCPT. Инструкция по запуску программного обеспечения PCPT с вопросами обзоров глав только этой части приведена в разделе "Как просмотреть вопросы только обзоров глав конкретной части" введения к книге.

Ответьте на вопросы обзора части

Ответьте на вопросы обзора этой части книги, используя программное обеспечение PCPT. Инструкция по запуску программного обеспечения PCPT с вопросами обзоров только этой части приведена в разделе "Как просмотреть вопросы только обзоров частей" введения к книге.

Повторите ключевые темы

Снова просмотрите темы прочитанных глав, отмеченные пиктограммой "Ключевая тема". Если понятны не все их подробности, уделите время повторному изучению.

Создайте диаграмму связей поиска и устранения неисправностей

В главе 16 основное внимание уделено поиску и устранению неисправностей маршрутизации IPv6 и не рассматриваются проблемы открытого протокола поиска первого кратчайшего маршрута версии 6 (Open Shortest Path First Version 3 — OSPFv3) и расширенного протокола маршрутизации внутреннего шлюза версии 3 (Enhanced Interior Gateway Routing Protocol Version 6 — EIGRPv6). В главах 17 и 18 обсуждается поиск и устранение неисправностей этих двух протоколов маршрутизации.

В первой диаграмме связей обзора этой части попытайтесь вспомнить все первопричины проблем сети IPv6 и организовать их в диаграмму связей. Как обычно, ис-

пользуйте не полные описания, а только сокращения, достаточные, чтобы самому понять их смысл. Кроме того, организуйте концепции так, как сами себе это представляете. Как обычно, не заглядывайте в главы; это упражнение должно помочь сформировать представление и организовать идеи в собственной памяти, а не просто читать выводы из книги.

Если хотите совет, то можете организовать темы по главам. Для соответствия главам поместите поиск и устранение неисправностей EIGRPv6 в одну часть диаграммы связей, OSPFv3 — в другую, а маршрутизация IPv6 — в третью.

Создайте диаграмму связей команд OSPFV3 и EIGRPV6

В данной части обсуждалась также настройка и проверка протоколов OSPFv3 и EIGRPv6. Создайте диаграмму связей команд, как и в других обзорах частей. Первый уровень организации должен быть для протоколов OSPFv3 и EIGRPv6, затем для настройки и проверки. Далее в области проверки организуйте команды по интерфейсам, соседям, топологии и маршрутам. (Обратите внимание, что подобные диаграммы связей уже встречались в обзоре части III для версий IPv4 этих протоколов маршрутизации.)

Ответы приведены в приложении E на веб-сайте, но ваши диаграммы связей могут выглядеть иначе.

Часть VI посвящена множеству небольших тем, связанных с управлением сетью и устройствами в сети, включая управление сетью с использованием протокола SNMP, управление сетевым трафиком с использованием NetFlow, управление информационными сообщениями системного журнала, работа с образами IOS на маршрутизаторах, а также управление программными средствами и лицензиями.

Часть VI. Управление сетью

Глава 19. “Управление сетевыми устройствами”

Глава 20. “Управление файлами IOS”

Глава 21. “Управление лицензиями IOS”

Обзор части VI

Глава 19

Управление сетевыми устройствами

Современная сеть способна на многое. Больше недостаточно просто передавать данные (электронные таблицы, транзакции, документы), необходимые для работы компании. Зачастую по сети должен передаваться также голосовой и видеотрафик организации. Современные сети должны быть быстрее и надежные, чем прежде. Они должны обладать очень высокой доступностью и масштабируемостью. Наличие широкого диапазона высокоразвитых протоколов и очень полезных методик управления сетью помогает администратору даже самых сложных сетей.

В этой главе рассматриваются три главных инструмента управления сетью для устройств Cisco. Правильная реализация *простого управления сетью* (Simple Network Management — SNMP), регистрации системных сообщений (системный журнал) и NetFlow способны существенно облегчать работу администратора Cisco. Полезные советы в этих областях помогут администратору быть *превентивными*, а не *реактивными*. Превентивное управление сетью действительно будет главной темой этой главы, что очень важно.

В этой главе рассматриваются следующие экзаменационные темы
Службы IP
Настройка и проверка системного журнала
Использование вывода системного журнала
Описание SNMP v2 и v3
Поиск и устранение неисправностей
Использование данных сетевого потока
Контроль статистики NetFlow

Основные темы

Простой протокол управления сетью

В 1988 году был опубликован документ RFC 1065: *Structure and Identification of Management Information for TCP/IP-based Internets*. Его основная идея сводилась к тому, что устройства в сети TCP/IP могут быть разделены на базы данных переменных и эти переменные можно контролировать, чтобы управлять всей сетью на базе протокола IP. В конце концов, элементы любых машин на базе протокола IP имели бы некие общности. Например, компьютер, сетевой принтер и маршрутизатор имеют такие общности, как интерфейсы, IP-адреса и буфера. Почему бы не создать стандартизированную базу данных этих переменных и простую систему их контроля и управления? Эта блестящая идея быстро завоевала популярность и стала основой трех разных версий *простого протокола управления сетью* (Simple Network Management Protocol — SNMP).

Описание протокола SNMP

Простой протокол управления сетью — это протокол уровня приложений, определяющий формат сообщения для связи между *диспетчерами* (manager) и *агентами* (agent). Диспетчер SNMP — это приложение управления сетью, выполняющееся на компьютере, а агент — это программное обеспечение, выполняющееся на управляемом устройстве. Агент должен возвращать (или записывать) значения хранимых в базе данных переменных, составляющих параметры устройства. (Речь идет о *базе управляющей информации* (Management Information Base — MIB).) Cisco Prime — классический пример диспетчера SNMP. Маршрутизатор Cisco мог бы выполнять агент SNMP, а переменной MIB могла бы быть загруженность интерфейса маршрутизатора. Элементы среды SNMP приведены на рис. 19.1.

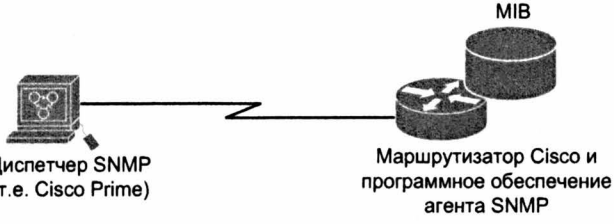


Рис. 19.1. Элементы простого протокола управления сетью

В процессе периодического (или последовательного) опроса агента SNMP на устройстве можно собрать и проанализировать статистику об управляемом устройстве. Используя эти переменные SNMP в базе MIB, можно даже перенастроить устройство, если это разрешено. Сообщения GET запрашивают информацию у программного обеспечения агента SNMP, а сообщения SET содержат информацию для записи в переменные

Протокол SNMP обеспечивает большую гибкость контроля переменных в базе MIB. Как правило, сетевой администратор собирает и хранит статистику, используя *станцию управления сетью* (Network Management Station — NMS) — программное обеспечение наподобие Cisco Prime. Оно позволяет администраторам проанализиро-

вать различные важные статистические данные, находить их среднее значение, минимумы и максимумы. Чтобы быть превентивным, администратор может установить пороговые значения для определенных ключевых переменных, и станция NMS динамически уведомит о приближении к недопустимым значениям. Пример применения протокола SNMP для превентивного управления сетью приведен на рис. 19.2.



Рис. 19.2. Протокол SNMP в процессе контроля сети

Превосходный пример этого стиля управления сетью — контроль использования процессора на маршрутизаторе Cisco. Благодаря протоколу SNMP станция NMS способна периодически запрашивать это значение и представлять сетевому администратору эту информацию в виде графика. Имея базовую линию, администратор может легко заметить, когда использование процессора поднимается выше нормальных для сети значений.

Кроме регулярного запроса у управляемых SNMP устройств информации о переменных MIB, используя команду SNMP GET, устройство может само уведомить NMS о проблеме при помощи *сообщения SNMP Trap*. Сообщения SNMP Trap передаются сетевыми устройствами и также содержат информацию о состоянии переменной MIB; но передать его устройство решает само, без запроса, и станция NMS может реагировать на него по-другому.

Предположим, например, что на маршрутизаторе 1 отказал интерфейс G0/0, как показано на этапе 1 рис. 19.3. При настроенных сообщениях Trap маршрутизатор послал бы такое сообщение станции NMS, уведомив его о состоянии down интерфейса G0/0. После этого программное обеспечение NMS может послать текстовое сообщение персоналу поддержки сети, вывести на экран NMS окно, вывести красную пиктограмму на интерфейсе маршрутизатора в графическом интерфейсе пользователя и т.д.

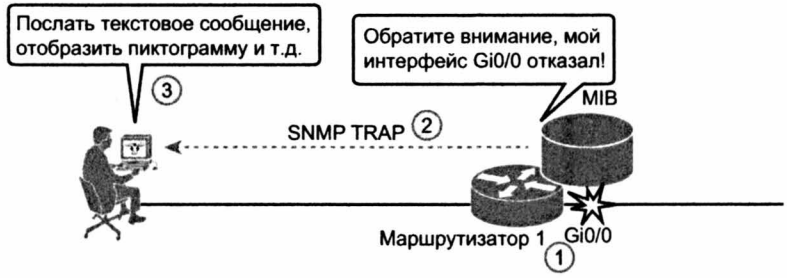


Рис. 19.3. Использование протокола SNMP для контроля сети

Протокол SNMP предоставляет две возможности передачи этих незапрашиваемых сообщений с управляемого устройства на станцию NMS. Сообщения Trap

представлены на рис. 19.3. Устройства передают сообщения Trap без подтверждения их получения станцией NMS; используя терминологию протокола; эти сообщения считаются ненадежными. Более поздняя версия протокола SNMP (версия 3) предоставляет альтернативный процесс с сообщениями Inform, обеспечивающими подтверждения, поэтому они считаются надежными.

База управляющей информации

Как уже упоминалось, *база управляющей информации* (Management Information Base — MIB) определяет переменные, которые позволяют программному обеспечению контролировать сетевые устройства и управлять ими. Формально база MIB определяет каждую переменную как *объектный идентификатор* (object ID — OID). Далее база MIB организует идентификаторы OID на основании стандартов RFC в иерархию, обычно представляемую в виде дерева.

База MIB любого конкретного устройства включает некоторые из ветвей дерева MIB с переменными, общими для многих сетевых устройств, и ветви с переменными, специфическими для этого устройства. Документы RFC определяют некоторые из общих открытых переменных, реализуемых базами MIB большинства устройств. Кроме того, такие производители сетевого оборудования, как Cisco, могут определить собственные частные ветви дерева, использовать новые переменные, специфические для их собственных устройств.

На рис. 19.4 представлены части структуры MIB, определенной компанией Cisco Systems. Обратите внимание, что при поиске специфической переменной в дереве идентификатор OID может быть описан как буквами, так и числами.

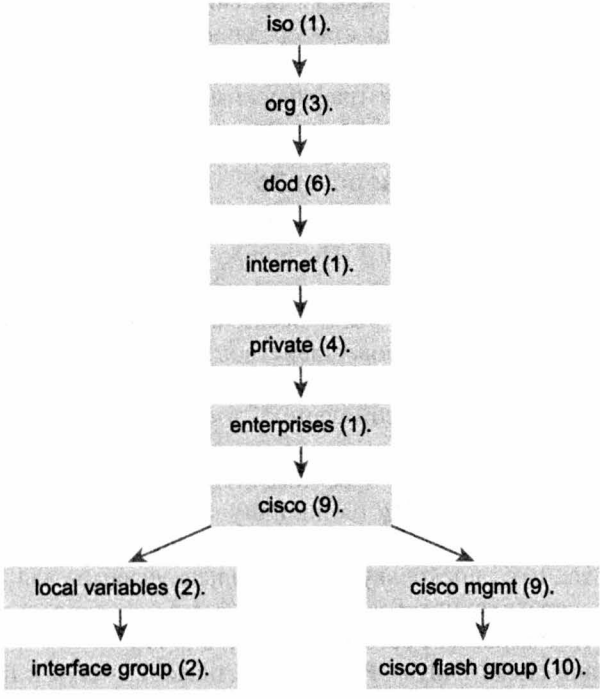


Рис. 19.4. База управляющей информации (MIB)

В качестве другого примера инструмента, который можно опробовать в домашней лабораторной работе, рассмотрим бесплатную утилиту SNMPGET, позволяющую быстро искать информацию в базе MIB. В примере 19.1 утилита SNMPGET используется на компьютере для получения 5-минутного экспоненциального среднего значения загрузки процессора на маршрутизаторе.

Пример 19.1. Получение значения из базы MIB при помощи SNMPGET

```
[13:22][cisco@NMS~ ]$ snmpget -v2c -c community 10.250.250.14
1.3.6.1.4.1.9.2.1.58.0
SNMPv2-SMI::enterprises.9.2.1.58.0 = INTEGER: 11
```

Выделенный полужирным шрифтом текст демонстрирует довольно длинную команду с несколькими следующими параметрами.

-v2c. Используемая версия протокола SNMP.

-c community. Пароль SNMP (общая строка).

10.250.250.14. IP-адрес контролируемого устройства.

1.3.6.1.4.1.9.2.1.58.0. Числовой идентификатор объекта (OID) переменной MIB.

Ответ приведен в последней строке и демонстрирует сокращенную версию переменной MIB. Это фактическое значение в указанной области MIB, в данном случае 5-минутное экспоненциальное среднее значение загрузки процессора в процентах (11 процентов).

Представленная в примере 19.1 утилита дает представление о базовом механизме работы протокола SNMP. Однако работа с такими длинными именами переменных MIB, как 1.3.6.1.4.1.9.2.1.58.0, может стать реальной проблемой для среднего пользователя. Обычно персонал поддержки сети использует такие средства управления сетью, как Cisco Prime, с удобным графическим интерфейсом, где данные имена переменных MIB скрыты от типичного пользователя.

Настройка протокола SNMP версии 2c

Тремя основными версиями протокола SNMP, используемого на протяжении многих лет, являются версии 1, 2c и 3. Поскольку версия 1 уже чрезвычайно устарела и ныне в сетях встречается крайне редко, сосредоточимся на версиях 2c и 3.

В версии 2c протокола SNMP было несколько дополнений к первой версии. Большинство их было связано с усовершенствованием системы обмена сообщениями, призванным повысить эффективность получения больших объемов статистических данных от устройства. К сожалению, в области защиты было сделано не очень много.

Для аутентификации доступа к объектам MIB протоколы SNMP версий 1 и 2c полагались на *общие строки SNMP* (community string). Общие строки — это всего лишь открытые текстовые пароли. Сейчас открытые текстовые пароли даже не считают механизмом защиты, поскольку они настолько уязвимы для атаки внедрения, что создают угрозу перехвата пакетов.

В протоколе SNMP версии 2c есть два типа общих строк.

Только для чтения (Read-Only — RO). Предоставляет доступ к переменным базы MIB, но не разрешает изменять их, только читать. Поскольку в версии 2c защита

очень слабая, большинство организаций используют протокол SNMP только в этом режиме.

Для чтения и записи (Read-Write — RW). Предоставляет доступ ко всем объектам в базе MIB для чтения и записи.

ВНИМАНИЕ!

Реальная защита протокола SNMP появилась только в версии 3. Она описана далее в главе.

Настройка протокола SNMP версии 2c на маршрутизаторе или коммутаторе Cisco требует только одной глобальной команды конфигурации: `snmp-server community`. Однако большинство конфигураций SNMP включает также несколько необязательных параметров. Ниже описаны общие этапы настройки.

Этапы настройки протокола SNMPv2c

Ключевая тема

Этап 1 Задайте в глобальной команде `snmp-server community` *строка* `RO|RW` общую строку и уровень доступа (только для чтения или чтения и записи). (Обязательно.)

Этап 2 Используя глобальную команду конфигурации `snmp-server location` *текст_описания_области*, документируйте область устройства. (Необязательно.)

Этап 3 Используя глобальную команду конфигурации `snmp-server contact` *контактное_имя*, документируйте контактное имя устройства. (Необязательно.)

Этап 4 Ограничьте доступ SNMP к хостам станций NMS только разрешенными в списке управления доступом (ACL), указав список ACL в глобальной команде конфигурации `snmp-server community` *строка имя_или_нимер_acl*. (Необязательно.)

В примере 19.2 используется обязательная команда и несколько необязательных из списка. Здесь использована трудная для подбора общая строка, доступ разрешен только для NMS по адресу 10.10.10.101, а также определены область и контактное имя ответственного за это устройство (маршрутизатор R1).

Пример 19.2. Настройка протокола SNMP версии 2c на доступ только для чтения

Ключевая тема

```
R1(config)# ip access-list standard ACL_PROTECTSNMP
R1(config-std-nacl)# permit host 10.10.10.101
R1(config-std-nacl)# exit
R1(config)# snmp-server community V011eyB@11!!! RO ACL_PROTECTSNMP
R1(config)# snmp-server location Tampa
R1(config)# snmp-server contact Anthony Sequeira
R1(config)# end
R1#
```

Пример 19.3 устанавливает подобную конфигурацию на маршрутизатор R2, расположенный в Нью-Йорке. Управление маршрутизатором разрешено другой станции NMS (также в Нью-Йорке), и в данном случае доступ разрешен для чтения и записи (RW).

Пример 19.3. Настройка протокола SNMP версии 2c на доступ для чтения и записи

```
R2(config)# ip access-list standard ACL_PROTECTSNMP
R2(config-std-nacl)# permit host 10.20.20.201
R2(config-std-nacl)# exit
R2(config)# snmp-server community T3nn1sB@ll RW ACL_PROTECTSNMP
R2(config)# snmp-server location New York
R2(config)# snmp-server contact John Sequeira
R2(config)# end
R2#
```

Выбор доступа только для чтения на маршрутизаторе R1 и доступ для чтения/записи на маршрутизаторе R2 для протокола SNMP оказывают большее влияние на работу сети, чем можно было бы предположить на основании столь малого различия в конфигурации. Маршрутизаторы и коммутаторы, доступ к которым разрешен для чтения и записи, позволяют станции NMS изменять конфигурацию маршрутизатора или коммутатора. Например, при доступе для чтения и записи станция NMS может отключить интерфейс или включить его снова, тогда как доступ только для чтения не позволяет изменять конфигурацию.

Протокол SNMP версии 3

Появление третьей версии протокола SNMP стало настоящим праздником для большинства сетевых администраторов. Наконец у мощного протокола управления сетью появилась защита. Протокол SNMPv3 предоставляет следующие средства безопасности.

Ключевая тема

Средства безопасности протокола SNMPv3

- **Целостность сообщения** гарантирует неизменность пакета при передаче.
- **Аутентификация** гарантирует получение пакетов только от известного, проверенного отправителя.
- **Шифрование** гарантирует невозможность прочтения информации, если данные будут перехвачены по пути.

В этом списке приведены все возможности протокола SNMPv3, но устройства могут реализовать только часть из них на основании конфигурации. Но даже самые слабые средства безопасности протокола SNMPv3 обеспечивают лучшую защиту по сравнению с протоколом SNMPv2c, поскольку управляемое устройство требует идентификации пользователя. Как показано в табл. 19.1, каждый уровень безопасности SNMPv3 требует разных комбинаций средств защиты, включая защиту аутентификации хешированием и шифрование данных, передаваемых между устройством и станцией NMS.

ВНИМАНИЕ!

Даже уровень noAuthNoPriv имеет преимущество по сравнению с протоколом SNMP версии 2c, поскольку он способен отслеживать учетные записи пользователя.

Таблица 19.1. Возможные уровни защиты протокола SNMP

Ключевая тема

Уровень	Ключевое слово в команде `snmp-server`	Метод аутентификации	Шифрование
noAuthNoPriv	`noauth`	По имени пользователя	Нет
authNoPriv	`auth`	Алгоритм MD5 (Message Digest 5) или SHA (Secure Hash Algorithm)	Нет
authPriv	`priv`	Алгоритм MD5 или SHA	DES или DES-56

Регистрация системных сообщений (системный журнал)

Просто удивительно, насколько устройства Cisco пытаются быть услужливыми для своих администраторов. Когда происходит серьезное (и даже не очень серьезное) событие, устройства Cisco пытаются уведомить о них администраторов подробными системными сообщениями. Как описано в этом разделе, сообщения варьируются от весьма незначительных до невероятно важных. К счастью, у администраторов есть множество возможностей для сохранения этих сообщений и оповещения тех, кто может оказать наибольшее влияние на сетевую инфраструктуру.

Краткий обзор регистрации системных сообщений

Наиболее распространенный метод использования всего богатства системных сообщений устройств Cisco подразумевает применение протокола *системного журнала* (syslog). Протокол системного журнала позволяет различным устройствам Cisco (и некоторым другим устройствам) передавать свои системные сообщения по сети на сервер системного журнала. Обратите внимание, что для этого можно даже создать специальную *внеполосную* (Out-Of-Band — OOB) сеть. Существует множество разных программных пакетов сервера системного журнала, и для операционной системы Windows, и для UNIX. Большинство из них бесплатны.

Внутренне сетевые устройства Cisco передают системные и отладочные сообщения локальному процессу регистрации устройства. Этому процессу регистрации вполне можно указать (в конфигурации), что затем делать с этими сообщениями. Например, их можно передавать по сети на сервер системного журнала, как было описано ранее, или во внутренний буфер, чтобы просмотреть их позже, в удобное время, через CLI устройства. Можно даже указать, чтобы разным получателям передавались только определенные типы системных сообщений. Например, сообщения уровня отладки, вероятно, нет смысла посылать на внешний сервер системного журнала, поскольку их обычно наблюдают в интерфейсе CLI.

Вот наиболее популярные получатели сообщений системного журнала.

- Буфер регистрации (оперативная память маршрутизатора или коммутатора).
- Канал консоли.
- Терминальные каналы.
- Сервер системного журнала.

На рис. 19.5 представлены различные устройства Cisco, передающие системные сообщения на сервер системного журнала.

Ключевая тема



Рис. 19.5. Регистрация системных сообщений в сети

Формат системных сообщений

Давайте рассмотрим одно из сообщений маршрутизатора Cisco, чтобы исследовать его стандартный формат:

```
*Dec 18 17:10:15.079: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/0, changed state to down
```

Обратите внимание, что стандартно устройство выводит следующее.

- **Временная метка**. `*Dec 18 17:10:15.079`.
- **Средство маршрутизатора, создавшее сообщение**. `%LINEPROTO`.
- **Уровень серьезности**. `5`.
- **Мнемосхема сообщения**. `UPDOWN`.
- **Описание сообщения**. `Line protocol on Interface FastEthernet0/0, changed state to down` (Протокол линии на интерфейсе FastEthernet0/0 изменил состояние на down.)

Это стандартный формат системных сообщений на конкретном маршрутизаторе Cisco, но следует знать, что формат сообщений можно контролировать. Например, можно отключить временные метки и включить порядковые номера, как показано в примере 19.4.

Пример 19.4. Изменение системных сообщений

```
R1(config)# no service timestamps
R1(config)# service sequence-numbers
R1(config)# end
R1#
000011: %SYS-5-CONFIG_I: Configured from console by console
```

Как обычно, когда пользователь выходит из режима конфигурации, маршрутизатор выдает еще одно системное сообщение, показанное в конце примера. По сравнению с предыдущим примером это сообщение больше не выводит время — оно выводит порядковый номер. Теперь сообщения имеют следующий формат.

- **Порядковый номер**. `000011`.
- **Средство**. `%SYS`.
- **Уровень серьезности**. `5`.
- **Мнемосхема**. `Config_I`.
- **Описание**. `Configured from console by console` (Настроено с консоли).

Уровни серьезности системных сообщений

Безусловно, один из самых важных компонентов в системном сообщении устройства Cisco — это уровень серьезности. Уровни серьезности позволяют легко контролировать, какие сообщения каким регистрирующим получателям посылать. Уровни серьезности системного сообщения, возможные на устройстве Cisco, приведены в табл. 19.2.

Таблица 19.2. Уровни серьезности системного сообщения

Ключевая тема

Уровень	Название	Описание
0	Emergency (Авария)	Система может быть неисправна
1	Alert (Тревога)	Возможно, требуется немедленное действие
2	Critical (Критическое)	Имело место критически важное событие
3	Error (Ошибка)	Произошла ошибка
4	Warning (Предупреждение)	Событие заслуживает внимания
5	Notification (Уведомление)	Произошло нормальное, но важное событие
6	Informational (Информация)	Произошло нормальное событие
7	Debugging (Отладка)	Результат отладочной команды

Обратите внимание, что события уровней 0–4 способны серьезно повлиять на устройство, а события уровней 5–7 менее важны. Вполне очевидно, что администратор может учитывать это, принимая решение об обработке сообщения. Например, администратор может решить посылать на сервер системного журнала только сообщения уровня 4 (предупреждения) и ниже (наиболее серьезные), чтобы не загромождать сервер системного журнала сообщениями всех восьми уровней.

Настройка и проверка системного журнала

Стандартно маршрутизаторы и коммутаторы Cisco передают регистрационные сообщения всех уровней серьезности на консоль. Операционная система IOS некоторых устройств стандартно также буферизует регистрационные сообщения. Для разрешения этих двух возможностей в конфигурации использовались бы глобальные команды конфигурации `logging console` и `logging buffered` соответ-

ственно. Для отключения любой из этих служб регистрации используются команды `no logging console` и `no logging buffered`.

Команда `show logging` позволяет просмотреть параметры службы регистрации на маршрутизаторе Cisco, как показано в примере 19.5. Первые строки вывода содержат информацию о процессе регистрации, а последние — регистрационные сообщения.

Пример 19.5. Просмотр стандартных параметров службы регистрации на маршрутизаторе Cisco

```
R1# show logging
Syslog logging: enabled (0 messages dropped, 2 messages rate-limited,0
flushes, 0 overruns,
xml disabled, filtering disabled)
No Active Message Discriminator.
No Inactive Message Discriminator.
Console logging: level debugging, 10 messages logged, xml disabled, fil-
tering disabled
Monitor logging: level debugging, 0 messages logged, xml disabled, fil-
tering disabled
Buffer logging: level debugging, 10 messages logged, xml disa-
bled,filtering disabled
Logging Exception size (8192 bytes)
Count and timestamp logging messages: disabled
Persistent logging: disabled
No active filter modules.
ESM: 0 messages dropped
Trap logging: level informational, 13 message lines logged
Log Buffer (8192 bytes):
*Dec 18 17:10:14.079: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed
state to down
*Dec 18 17:10:15.079: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/0, changed state to down
...
```

Сосредоточимся на первых двух выделенных строках, сообщающих о службе регистрации. В первой строке утверждается, что этот маршрутизатор выводит сообщения на консоль, включая отладочные сообщения. Фактически это означает уровень отладочных сообщений и все более низкие уровни (см. табл. 19.2). Вывод также информирует, что были зарегистрированы десять таких сообщений. Во второй выделенной строке утверждается, что этот маршрутизатор регистрирует сообщения во внутреннем буфере.

Поскольку этот маршрутизатор разрешил регистрацию во внутренний буфер, команда `show logging` также выводит сообщения в этот буфер. В конце примера можно увидеть некоторые из зарегистрированных системных сообщений.

Настроить маршрутизатор на передачу системных сообщений на сервер системного журнала, где они могут храниться, фильтроваться и анализироваться, вовсе не сложно.

Этап 1 Сначала задать имя хоста получателя или IP-адрес сервера системного журнала:

```
R1(config)# logging 192.168.1.101
```

Этап 2 Затем можно указать, какие сообщения куда посылать. Например, чтобы ограничить сообщения для уровня 4 и ниже (0 – 4), используйте следующую команду:

```
R1(config)# logging trap 4
```

Обратите внимание, что указание самого высокого уровня (наименее серьезного) подразумевает включение всех уровней ниже (более серьезных). Кроме того, эта команда допускает имена уровней, поэтому вполне возможна команда `logging trap warning`.

Использование сервера системного журнала

Регистрация во внутренний буфер устройства — это самый эффективный способ обработки системных сообщений, но самым популярным является их передача программному обеспечению сервера системного журнала.

Серверы системного журнала регистрируют сообщения и предоставляют обычно простые средства отображения и сортировки сообщения для упрощения поиска и устранения неисправностей.

Благодаря серверам системного журнала администраторы могут легко использовать все богатство информации, предоставляемой системными сообщениями. Они позволяют искать сообщения по определенным ключевым словам или уровням серьезности. Можно даже написать сценарий передачи оповещений по электронной почте на основании серьезности полученных сообщений.

Конечно, администраторы могут также использовать программное обеспечение сервера системного журнала для удаления всех неважных системных сообщений из базы данных. Напомню, что ключевым аспектом использования системных сообщений является пропуск всех сообщений, не предоставляющих полезной информации.

Протокол NetFlow

Даже при наличии такого мощного инструмента, как простой протокол управления сетью (SNMP), довольно быстро стало очевидным, что инженерам Cisco и специалистам по работе с сетями необходим простой и эффективный метод отслеживания путей в сети TCP/IP. Эта информация облегчает выявление потенциальных узких мест сети, ее усовершенствование и изменение проекта, она может даже помочь в расчете платы потребителей сети. Для удовлетворения этих потребностей компания Cisco разработала протокол NetFlow. Этот мощный сетевой протокол быстро стал стандартом и теперь поддерживается другими сетевыми гигантами.

Краткий обзор протокола NetFlow

В отличие от таких сетевых протоколов, как SNMP, пытающихся предоставить очень широкий диапазон средств и возможностей управления сетью, задача протокола NetFlow проста и конкретна: максимально эффективно собрать статистику по пакетам IP, передаваемым через сетевые устройства.

Например, хост A на рис. 19.6 соединен с хостом B, использующим некое приложение (например, протокол HTTP). Протокол NetFlow может контролировать это соединение (подсчитывать пакеты, байты и т.д.) по каждому индивидуальному потоку. Затем он может передать статистику на внешний сервер — *коллектор NetFlow* (NetFlow collector).

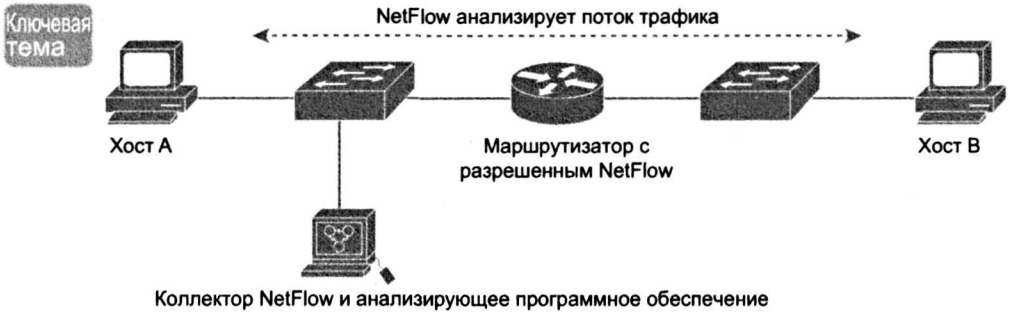


Рис. 19.6. NetFlow в типичной сети

Хотя предоставляемые протоколом NetFlow статистические данные можно потенциально использовать для чего угодно, большинство организаций использует их лишь для следующих целей.

- Общий сетевой трафик для базового анализа.
- Расчет платы за трафик потребителей сетевых услуг.
- Проектирование и изменение проекта сети, подразумевающее добавление новых сетевых устройств и приложений, удовлетворяющих растущие потребности инфраструктуры.
- Общий проект защиты сети.
- Обнаружение и предотвращение атаки отказа в обслуживании (DoS) и распределенной атаки DoS (DDoS).
- Постоянный дистанционный мониторинг сети.

Если считать такой протокол управления сетью, как SNMP, программным обеспечением дистанционного управления беспилотником, то протокол NetFlow, как правило, сравнивают с подробным телефонным счетом. Его записи содержат все вызовы со всеми статистическими данными, позволяющими администратору (плательщику по счету) проследить междугородные и местные звонки, а также те звонки, которых, казалось бы, не было вообще.

ВНИМАНИЕ!

Не стоит путать цели и результаты протокола NetFlow с таковыми у аппаратных средств и программного обеспечения перехвата пакетов. Перехват пакетов подразумевает запись всей возможной информации на входе и выходе сетевого устройства для последующего анализа, а протокол NetFlow предназначен для сбора вполне определенной статистической информации.

При разработке протокола NetFlow компания Cisco руководствовалась двумя ключевыми критериями.

- Протокол NetFlow должен быть полностью прозрачным для приложений и устройств в сети.
- Для функционирования протокол NetFlow не придется поддерживать или запускать на всех устройствах в сети.

Удовлетворение проекта этим критериям гарантировало, что протокол NetFlow очень прост в реализации самых сложных из существующих сетей.

ВНИМАНИЕ!

Хотя протокол NetFlow прост в реализации и прозрачен в сети, он все же использует дополнительную память на маршрутизаторе Cisco. Это связано с тем, что протокол NetFlow хранит информацию на устройстве в кеше. Его стандартный размер зависит от платформы, но администратор вполне может изменить это значение.

Сетевые пути

Суть технологии NetFlow, как и следует из ее названия, заключается в том, что она разделяет коммуникации TCP/IP для статистического хранения записи, используя концепцию пути. Что такое путь согласно пониманию NetFlow? *Путь* (flow) — это однонаправленный *поток* (stream) пакетов между конкретными передающей и получающей системами. Поскольку протокол NetFlow построен на базе TCP/IP, на сетевом уровне отправитель и получатель определяются IP-адресами, а на транспортном уровне — номерами портов.

Технология NetFlow насчитывает несколько поколений, все более совершенствуя определение путей трафика, но "классическая" версия NetFlow различала пути, используя комбинацию из семи основных полей. Если хоть одно из этих полей отличалось по значению от другого, то пакеты могли быть однозначно отнесены к другому пути.

- IP-адрес отправителя.
- IP-адрес получателя.
- Номер порта отправителя.
- Номер порта получателя.
- Тип протокола третьего уровня.
- Маркер типа обслуживания (Type of Service — ToS).
- Входной логический интерфейс.

Первые четыре поля, использующиеся NetFlow для идентификации пути, должны быть вам уже знакомы. IP-адреса отправителя и получателя, а также порты отправителя и получателя идентифицируют соединение между приложениями отправителя и получателя. Тип протокола третьего уровня идентифицирует заголовок протокола третьего уровня, следующий после заголовка IP. Кроме того, байт ToS в заголовке IPv4 содержит информацию о том, как устройства должны применять правила качества обслуживания (QoS) к пакетам на этом пути.

Настройка NetFlow

Настройка протокола NetFlow на маршрутизаторе требует двух отдельных действий.

1. Настроить захват данных о путях подкомандой интерфейса `ip flow`.
2. Настроить передачу этих данных на коллектор NetFlow глобальной командой `ip flow-export`.

Сначала, для захвата данных пути, инженер должен добавить команду `ip flow ingress` или `ip flow egress` на один или несколько интерфейсов. Обе команды указывают маршрутизатору захватывать данные NetFlow для путей на интерфейсе. Параметр `ingress` указывает маршрутизатору контролировать входящие пакеты на интерфейсе, а параметр `egress` — исходящие. (Путь NetFlow имеет только одно направление, поэтому у одного пользовательского соединения с приложением существуют как бы два пути NetFlow, по одному для каждого направления.)

Для настройки коллектора на маршрутизаторе также необходимо выполнить несколько действий.

1. Задать IP-адрес и номер порта UDP коллектора NetFlow глобальной командой `ip flow-export destination` *адрес порт*.
2. Задать глобальной командой `ip flow-export version` *версия* версии NetFlow для выбора формата передаваемых на коллектор записей NetFlow.
3. Задать глобальной командой `ip flow-export source` *тип номер* исходящего интерфейса, используемого в качестве отправителя передаваемых на коллектор пакетов.

В примере 19.6 показана конфигурация на основании сети, представленной на рис. 19.7. Маршрутизатор R1 собирает данные о путях на интерфейсе F0/0, для пакетов и входного, и выходного трафика. Затем он обращается к коллектору NetFlow по IP-адресу 10.1.10.100, используя порт UDP 99. В конфигурации определена также версия 9 записей NetFlow и использование петлевого интерфейса для IP-адреса отправителя пакетов, посланных на коллектор.

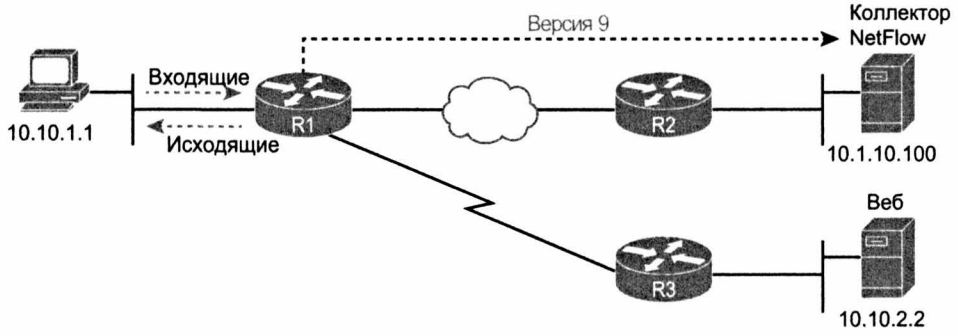


Рис. 19.7. Сеть, используемая для примера конфигурации NetFlow

Ключевая тема

Пример 19.6. Настройка NetFlow на маршрутизаторе Cisco

```
R1(config)# interface fastethernet0/0
R1(config-if)# ip flow ingress
R1(config-if)# ip flow egress
R1(config-if)# exit
R1(config)# ip flow-export destination 10.1.10.100 99
R1(config)# ip flow-export version 9
R1(config)# ip flow-export source loopback 0
```

```
R1(config)# end
R1#
```

ВНИМАНИЕ!

Как уже упоминалось, протокол NetFlow был выпущен в нескольких версиях. В настоящее время доступны пять форматов, пронумерованных как 1, 5, 7, 8 и 9. Последняя версия, 9, для разнообразия названная Flexible NetFlow, позволяет определять пути и хранить записи для различных параметров. К сожалению, эта версия несовместима с предыдущими версиями NetFlow.

Проверка и использование NetFlow

После настройки следует проверить работу протокола NetFlow, а затем можно приступать к использованию собранных данных. Окончательная проверка NetFlow подразумевает исследование информации, хранимой на коллекторе NetFlow, но можно также проверить локальный кеш NetFlow на самом маршрутизаторе. Это докажет, что маршрутизатор по крайней мере собирает данные. Для этого используется команда `show ip cache flow`, представленная в примере 19.7.

Пример 19.7. Исследование кеша NetFlow

```
R1# show ip cache flow
IP packet size distribution (255 total packets):
1-32   64   96  128  160  192  224  256  288  320  352  384  416  448
480
.000 .000 .000 1.00 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000
.000

 512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
.000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 4456704 bytes
  1 active, 65535 inactive, 1 added
  32 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 533256 bytes
  1 active, 16383 inactive, 1 added, 1 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
  last clearing of statistics never
Protocol  Total  Flows  Packets  Bytes  Packets  Active(Sec)  Idle(Sec)
--------  Flows  /Sec   /Flow    /Pkt   /Sec     /Flow        /Flow

SrcIf  SrcIPaddress  DstIf   DstIPaddress  Pr SrcP DstP Pkts
Fa0/0  10.10.1.1     S0/0/0  10.10.2.2     01 0200 0050 255
```

В верхней части вывода команды подтверждается, что маршрутизатор действительно собирает данные. Первый выделенный элемент выводит количество (255) пакетов, зарегистрированных NetFlow. В нижней части вывода приведена статистика одного пути, созданного для данного конкретного примера. Пример демонстрирует результаты соединения компьютера PC1 с веб-сервером согласно рис. 19.7. В выделенной строке отображается IP-адрес отправителя 10.10.1.1, IP-адрес получа-

теля 10.10.2.2 и полное количество пакетов на этом пути (255). Представлен также порт отправителя (SrcP) и порт получателя (DstP) в шестнадцатеричном формате, чтобы лучше идентифицировать путь; обратите внимание, что шестнадцатеричные 50 равны десятичным 80 — это общеизвестный порт TCP для веб-служб.

Хотя данные в примере 19.7 подтверждают, что маршрутизатор собирает данные, следует еще удостовериться в том, что протокол NetFlow настроен на правильных интерфейсах в правильных направлениях. Для этого можно использовать команду `show ip flow interface`, показанную в примере 19.8. Затем, чтобы проверить конфигурацию параметров экспорта, можно использовать команду `show ip flow export`, также представленную в примере. Обратите внимание, что выделенные строки в примере ссылаются непосредственно на конфигурацию, представленную в примере 19.6.

Пример 19.8. Проверка конфигурации интерфейса NetFlow

```
R1# show ip flow interface
FastEthernet0/0
  ip flow ingress
  ip flow egress

R1# show ip flow export
Flow export v9 is enabled for main cache
  Export source and destination details :
  VRF ID : Default
    Source(1) 1.1.1.1 (Loopback0)
    Destination(1) 10.1.10.100 (99)
  Version 9 flow records
  0 flows exported in 0 udp datagrams
  0 flows failed due to lack of export packet
  0 export packets were sent up to process level
  0 export packets were dropped due to no fib
  0 export packets were dropped due to adjacency issues
  0 export packets were dropped due to fragmentation failures
  0 export packets were dropped due to encapsulation fixup failures
R1#
```

Коллектор NetFlow

Как же упоминалось, коллектор NetFlow — это системное программное обеспечение, специализирующееся на обработке исходных данных NetFlow. Оно может быть настроено на получение информации NetFlow от многих разных систем в инфраструктуре. Просмотр всех необработанных исходных данных может дать немного, однако программное обеспечение коллектора NetFlow способно объединить и организовать информацию множеством способов, чтобы они имели смысл для сетевых администраторов. Для представления информации множеством способов разным заинтересованным лицам используются отчеты.

Для коллекторов NetFlow доступно широкое разнообразие бесплатного программного обеспечения и коммерческих приложений, обладающих наборами отчетов, наиболее типичные из которых приведены ниже.

- "Главные передатчики" в сети.
- "Главные приемники" в сети.
- Наиболее часто посещаемые веб-сайты.
- Наиболее часто загружаемое содержимое.
- Системы с наименее доступной шириной полосы пропускания.

Объем анализируемой информации зависит от используемой версии протокола NetFlow. Это связано с тем, что у разных версий определен разный объем записей NetFlow. Запись NetFlow содержит специфическую информацию о фактическом трафике, создаваемом в пути NetFlow. Например, записи NetFlow версии 5 включает следующую информацию:

- Индекс входного интерфейса, используемый протоколом SNMP.
- Индекс выходного интерфейса.
- Временные метки для начала и конца пути.
- Количество байтов и пакетов в пути.
- Заголовок уровня 3.
- Флаги TCP.
- Информации о маршрутизации уровня 3, включая следующий транзитный узел.

Запись NetFlow версии 9 содержит эти поля и другие, включая метки MPLS, IPv6-адреса и порты.

Обзор

Резюме

- Простой протокол управления сетью (SNMP) — это протокол уровня приложений, определяющий формат сообщения для связи между диспетчерами и агентами.
- Диспетчер SNMP — это приложение управления сетью, выполняющееся на компьютере, а агент — это программное обеспечение, выполняющееся на управляемом устройстве.
- В процессе периодического (или последовательного) опроса агента SNMP на устройстве можно собрать и проанализировать статистику об управляемом устройстве.
- Протокол SNMP обеспечивает большую гибкость контроля переменных в базе MIB.
- Сообщения Trap передаются сетевыми устройствами и также содержат информацию о состоянии переменной MIB; но передать его устройство решает само, без запроса, и станция NMS может реагировать на него по-другому.
- Тремя основными версиями протокола SNMP, используемого на протяжении многих лет, являются версии 1, 2c и 3.
- В протоколе SNMP версии 2c есть два типа общих строк: только для чтения (RO), для чтения и записи (RW).
- Протокол SNMPv3 предоставляет следующие средства безопасности: целостность, аутентификация, шифрование.
- Наиболее распространенный метод использования всего богатства системных сообщений устройств Cisco подразумевает применение протокола системного журнала.
- Протокол системного журнала позволяет различным устройствам Cisco (и некоторым другим устройствам) передавать свои системные сообщения по сети на сервер системного журнала.
- Стандартно маршрутизаторы и коммутаторы Cisco передают регистрационные сообщения всех уровней серьезности на консоль.
- Регистрация во внутренний буфер устройства — это самый эффективный способ обработки системных сообщений, но самым популярным является их передача программному обеспечению сервера системного журнала.
- Компания Cisco разработала протокол NetFlow для отслеживания пути TCP/IP в сети.
- Суть технологии NetFlow, как и следует из ее названия, заключается в том, что она разделяет коммуникации TCP/IP для статистического хранения записи, используя концепцию пути.
- Настройка протокола NetFlow на маршрутизаторе требует двух отдельных действий: настройка захвата данных о путях подкомандой интерфейса `ip flow`, настройка передачи этих данных на коллектор NetFlow глобальной командой `ip flow-export`.

- Настройка коллектора на маршрутизаторе требует задания IP-адреса и номера порта UDP коллектора NetFlow; версии NetFlow для выбора формата передаваемых на коллектор записей NetFlow и исходящего интерфейса, используемого в качестве отправителя передаваемых на коллектор пакетов.
- Хотя окончательная проверка NetFlow подразумевает исследование информации, хранимой на коллекторе NetFlow, но можно также проверить локальный кеш NetFlow на самом маршрутизаторе. Это докажет, что маршрутизатор по крайней мере собирает данные.
- Коллектор NetFlow — это системное программное обеспечение, специализирующееся на обработке исходных данных NetFlow.
- Объем анализируемой информации зависит от используемой версии протокола NetFlow. Это связано с тем, что у разных версий определен разный объем записей NetFlow.

Контрольные вопросы

Ответьте на эти вопросы. Ответы можно найти на последней странице главы. Полное объяснение ответов приведено в приложении В на веб-сайте.

1. Как называется расположенная на сетевых устройствах база данных, доступная агентам SNMP?

   А) Хранилище NetFlow.

   Б) Хранилище управления.

   В) Хранилище управляющих переменных.

   Г) База управляющей информации.

2. Какой программный пакет является примером станции NMS, использующей протокол SNMP?

   А) Cisco Monitor.

   Б) Cisco Insight.

   В) Cisco Prime.

   Г) Cisco View.

3. Какая команда настраивает контролируемое устройство, но не настраивает SNMP версии 2c с использованием общей строки CiscoSanFran?

   А) `snmp-server secret CiscoSanFran ro`.

   Б) `snmp-server community CiscoSanFran ro`.

   В) `snmp-server 2c community CiscoSanFran read-only`.

   Г) `snmp-server 2c community CiscoSanFran monitor-only`.

4. Какой режим SNMP версии 3 полагается на имя пользователя для аутентификации и не использует шифрование?

   А) noAuthPriv.

   Б) AuthPriv.

   В) noAuthNoPriv.

   Г) AuthOnly.

5. Какой уровень регистрации на консоль является стандартным для устройств Cisco?

   А) Informational.

   Б) Errors.

   В) Warnings.

   Г) Debugging.

6. Какая команда ограничивает сообщения, передаваемые на сервер системного журнала до уровней 4–0?

   А) `logging trap 0-4`.

   Б) `logging trap 1,2,3,4`.

   В) `logging trap 4`.

   Г) `logging trap through 4`.

7. Что протокол NetFlow не использует для идентификации пути?

   А) Номер порта получателя.

   Б) Маркер ToS (типа обслуживания).

   В) Тип протокола третьего уровня.

   Г) Логический выходной интерфейс.

8. Какая команда обеспечивает протоколу NetFlow захват статистики исходящего трафика на интерфейсе?

   А) `ip netflow egress`.

   Б) `ip flow out`.

   В) `ip flow egress`.

   Г) `ip netflow egre ss`.

Ключевые темы

Повторите все ключевые темы данной главы, отмеченные пиктограммой "Ключевая тема". Ключевые темы и соответствующие им страницы перечислены в табл. 19.3.

Таблица 19.3. Ключевые темы главы 19

Элемент	Описание	Страница
Рис. 19.1	Элементы простого протокола управления сетью	613
Список	Этапы настройки протокола SNMPv2c	617
Прим. 19.2	Настройка протокола SNMP версии 2c на доступ только для чтения	617
Список	Средства безопасности протокола SNMPv3	618
Табл. 19.1	Возможные уровни защиты протокола SNMP	619
Рис. 19.5	Регистрация системных сообщений в сети	620
Табл. 19.2	Уровни серьезности системного сообщения	621
Рис. 19.6	NetFlow в типичной сети	624
Прим. 19.6	Настройка NetFlow на маршрутизаторе Cisco	626

Заполните таблицы и списки по памяти

Распечатайте приложение Г с веб-сайта или его раздел, относящийся к этой главе, и заполните таблицы и списки по памяти. В приложении Д приведены заполненные таблицы и списки для самоконтроля.

Ключевые термины

После первого прочтения главы попытайтесь дать определения следующим ключевым терминам. Но не расстраивайтесь, если не все получится сразу, в главе 22 описано, как использовать эти термины на завершающем этапе подготовки к экзамену.

простой протокол управления сетью (Simple Network Management Protocol — SNMP), база управляющей информации (Management Information Base — MIB), агент SNMP (SNMP agent), станция управления сетью (Network Management Station — NMS), приложение Cisco Prime, сообщение GET (GET message), сообщение SET (SET message), сообщение trap (trap), сообщение inform (inform), идентификатор объекта (Object Identifier — OID), целостность (integrity), аутентификация (authentication), шифрование (encryption), системный журнал (syslog), внеполосный (Out-Of-Band — OOB), протокол NetFlow (NetFlow)

Ответы на контрольные вопросы:

1 Г. 2 В. 3 Б. 4 В. 5 Г. 6 В. 7 Г. 8 В.

ГЛАВА 20

Управление файлами IOS

Сетевые инженеры играют ключевую роль в управлении устройствами Cisco IOS. Это подразумевает управление файлами конфигурации устройства, создание и сохранение резервных копий, а также обновление образов программного обеспечения IOS.

В данной главе рассматриваются три темы, связанные с управлением процессом загрузки, образами и файлами конфигурации устройств Cisco IOS. Хотя это обсуждение и не является исчерпывающим, оно позволяет получить предоставление об управлении файлами операционной системы Cisco IOS большинства маршрутизаторов и коммутаторов.

В этой главе рассматриваются следующие экзаменационные темы
Технологии маршрутизации IP
Процесс загрузки операционной системы Cisco IOS маршрутизатора
POST
Процесс загрузки маршрутизатора
Управление файлами Cisco IOS
Параметры загрузки
Образ (образы) Cisco IOS

Основные темы

Управление файлами Cisco IOS

В качестве *операционной системы* (Operating System — OS) маршрутизаторы Cisco используют программное обеспечение Cisco IOS. По большей части, в этой книге и книге по ICND1 игнорируются некоторые из подробностей о работе операционной системы IOS самой по себе. В основном в них обсуждаются сетевые функции IOS. Теперь же обратим внимание на основные проблемы управления устройством, например, на настройку операционной системы IOS и ее загрузку при включении питания маршрутизатора.

В отличие от многих других OS, которые вы, возможно, использовали, операционная система Cisco IOS существует в виде единого файла — образа IOS. Процесс ее обновления включает такие этапы, как копирование более нового образа IOS во флеш-память, указание маршрутизатору, какой именно образ IOS использовать, и удаление прежнего образа IOS после проверки работоспособности новой версии. При включении процесс загрузки на маршрутизаторе должен быть готов выбрать правильный образ IOS для использования, а если этот процесс по какой-нибудь причине терпит неудачу, то иметь способ преодолеть или устранить эту проблему.

Первый раздел главы начинается с обсуждения обновления программного обеспечения Cisco IOS и процесса загрузки маршрутизатора.

ВНИМАНИЕ!

В данной главе основное внимание уделено маршрутизаторам, а не коммутаторам. Но большинство концепций относится также и к коммутаторам.

Обновление образа программного обеспечения Cisco IOS во флеш-памяти

У маршрутизаторов Cisco обычно нет дисковода. Вместо этого они используют другие типы памяти, как показано на рис. 20.1.



Рис. 20.1. Типы памяти маршрутизатора и их назначение

Обычно маршрутизаторы хранят образы IOS во флеш-памяти. Флеш-память — это перезаписываемое постоянное хранилище, идеально подходящее для хранения файлов с учетом возможности отключения питания маршрутизатора. Компания Cisco специально использует в своих изделиях флеш-память, а не дисководы, поскольку в ней нет никаких движущихся частей, а следовательно, меньше вероятность отказа по сравнению с дисками. Одни модели маршрутизаторов используют

внутренние микросхемы флеш-памяти, а другие — внешние слоты флеш-памяти, поддерживающие обычные бытовые накопители флеш. Новые маршрутизаторы зачастую поддерживают также флеш-диски USB, подключаемые к внешнему порту USB на стороне маршрутизатора.

Кроме того, маршрутизаторы Cisco могут хранить свои образы IOS на внешнем сервере, доступном по сети, и обычно для этого используются протоколы FTP или TFTP. Однако внешние серверы обычно используют для проверки и устранения проблем, возникших с файлом IOS во флеш-памяти. На практике фактически каждый маршрутизатор Cisco загружает образ IOS, хранящийся в единственном его типе постоянной памяти достаточно большого объема — во флеш-памяти.

Один из первых этапов обновления операционной системы IOS маршрутизатора до новой версии подразумевает получение нового образа IOS и помещение его в правильную область, обычно во флеш-память на маршрутизаторе. Процесс обновления образа IOS во флеш-памяти (рис. 20.2) состоит из следующих этапов.

Этап 1 Получить образ Cisco IOS. Обычно его загружают с `Cisco.com`, используя протокол HTTP или FTP

Этап 2 Поместить образ IOS туда, где он будет доступен маршрутизаторам. Это серверы TFTP или FTP в сети или носитель флеш для USB, который затем вставляется в маршрутизатор

Этап 3 Ввести команду `copy` на маршрутизаторе, скопировав файл в его флеш-память, где он останется на постоянной основе. (Обычно маршрутизаторы не могут загружаться с образа IOS на носителе флеш для USB.)



Рис. 20.2. Копирование образа IOS в ходе процесса обновления программного обеспечения Cisco IOS

Пример 20.1 демонстрирует третий этап, показанный на рис. 20.2, — копирование образа IOS во флеш-память. В данном случае маршрутизатор R2, 2901, копирует образ IOS с сервера TFTP по IP-адресу 2.2.2.1.

Пример 20.1. Команда `copy tftp flash` копирует образ IOS во флеш-память

```
R2# copy tftp flash
Address or name of remote host []? 2.2.2.1
Source filename []? c2900-universalk9-mz.SPA.152-4.M1.bin
Destination filename [c2900-universalk9-mz.SPA.152-4.M1.bin]?
Accessing tftp://2.2.2.1/c2900-universalk9-mz.SPA.152-4.M1.bin...
Loading c2900-universalk9-mz.SPA.152-4.M1.bin from 2.2.2.1 (via Gigabit
Ethernet0/1): !!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!
[OK - 74503236 bytes]

74503236 bytes copied in 187.876 secs (396555 bytes/sec)
R2#
```

Команда `copy` выполняет простую задачу — копирует файл, а также выполняет несколько небольших проверок. Она нуждается в некой информации от пользователя, поэтому в приглашении к вводу пользователь указывает эту информацию, как показано в строках примера, выделенных полужирным. Затем следует проверить работоспособность новой копии. Команда задает такие вопросы.

1. Каков IP-адрес или имя хоста сервера TFTP?
2. Каково имя файла?
3. Запрос у сервера размера файла и проверка достаточности места для этого файла во флеш-памяти локального маршрутизатора.
4. Есть ли у сервера файл с таким именем?
5. Должен ли маршрутизатор удалить какие-нибудь старые файлы во флеш-памяти?

По мере необходимости маршрутизатор запрашивает у пользователя ответы на некоторые из этих вопросов. Для каждого вопроса следует либо ввести ответ и нажать клавишу <Enter>, если стандартный ответ (представленный в квадратных скобках в конце вопроса) приемлем. Затем, при необходимости, маршрутизатор очистит флеш-память, скопирует файл и проверит контрольную сумму файла, чтобы удостовериться в отсутствии ошибки при передаче.

По завершении можно использовать команду `show flash`, чтобы проверить содержимое флеш-памяти, как показано в примере 20.2. (Вывод команды `show flash` зависит от конкретного семейства маршрутизаторов.)

Пример 20.2. Проверка содержимого флеш-памяти командой `show flash`

```
R2# show flash
-#- --length-- -----date/time------ path
1   74503236   Feb 12 2013 19:06:54 +00:00 c2900-universalk9-mz.SPA.151-
4.M4.bin
2   97794040   Sep 21 2012 14:02:50 +00:00 c2900-universalk9-mz.SPA.152-
```

```
4.M1.bin

78909440 bytes available (172297280 bytes used)
```

Как только новый файл IOS будет скопирован во флеш, маршрутизатор следует перезагрузить, чтобы был использован новый образ IOS. Например, в представленном в примере 20.2 выводе во флеш-памяти маршрутизатора R2 содержатся теперь два образа IOS: первоначальный образ версии 15.1(4) и вновь скопированный версии 15.2(4). В следующем разделе рассматривается последовательность загрузки IOS и объясняются подробности настройки маршрутизатора, чтобы он загружал правильный образ IOS.

ВНИМАНИЕ!

Обычно образ IOS — это сжатый файл, который занимает меньше места во флеш-памяти. После загрузки в оперативную память маршрутизатор распаковывает образ IOS.

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 операционную систему, которую следует 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

Этапы загрузки маршрутизатора Cisco

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 (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. 20.3 показаны различные возможности и этапы загрузки устройств 2–4.

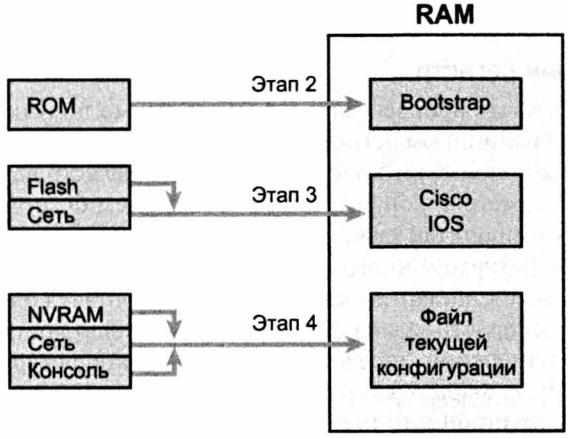


Рис. 20.3. Загрузка программы bootstrap, операционной системы IOS и начальной конфигурации

Как можно заметить, на этапах 3 и 4, показанных на рис. 20.3, у маршрутизатора есть несколько возможностей. Но на этапе 4 маршрутизаторы почти всегда загружают конфигурацию из NVRAM (файл `startup-config`), когда он там есть. Поскольку нет никаких реальных преимуществ сохранения начальной конфигурации где-нибудь, кроме NVRAM, в этой главе не рассматриваются другие возможности этапа 4. Однако резоны сохранения образов IOS во флеш-памяти и на серверах в сети есть, поэтому далее в этом разделе этап 3 рассматривается более подробно.

Ниже будет рассмотрен процесс загрузки маршрутизатора и выбора маршрутизатором загружаемого образа IOS. Но сначала необходимо узнать немного больше о некоторых других OS, помимо IOS, и нечто об инструменте, используемом во время загрузки, а именно о конфигурационном регистре.

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 табл. 20.1 приведены две альтернативные операционные системы, которые можно встретить в маршрутизаторах.

Таблица 20.1. Операционные системы 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

Конфигурационный регистр

Прежде чем обсуждать процесс загрузки, необходимо получить некоторое представление о конфигурационном регистре маршрутизатора Cisco.

Маршрутизаторы используют конфигурационный регистр во время загрузки для получения неких параметров конфигурации прежде, чем будет загружена операционная система IOS и прочитан файл `startup-config`. 16 битов (4 шестнадцатеричные цифры) конфигурационного регистра позволяют задать множество разных параметров. Например, стандартно канал консоли работает со скоростью 9600 битов в секунду, и эта скорость задана стандартно в конфигурационном регистре двумя битами. После изменения определенных битов в конфигурационном регистре при следующей загрузке маршрутизатора скорость канала консоли изменится.

Значение конфигурационного регистра можно установить глобальной командой конфигурации `config-register`. Инженеры меняют значения конфигурационного регистра по разным причинам, но чаще всего для указания маршрутизатору загружаемого образа IOS и восстановления пароля, как будет описано далее. Например, команда `config-register 0x2100` устанавливает шестнадцатеричное значение 2100, заставляющее маршрутизатор загружать OS ROMMON, а не IOS после следующей перезагрузки.

Маршрутизаторы Cisco автоматически сохраняют новое значение конфигурационного регистра после нажатия клавиши <Enter> в конце ввода команды `config-register`; поэтому после изменения конфигурационного регистра не нужно использовать команду `copy running-config startup-config`. Однако до следующей перезагрузки маршрутизатора новое значение конфигурационного регистра никак и ни на что не влияет.

ВНИМАНИЕ!

На большинстве маршрутизаторов Cisco стандартно установлено шестнадцатеричное значение 2102 параметра конфигурационного регистра, задающее скорость 9600 бит/с канала консоли и загрузку образа IOS.

Как маршрутизатор выбирает загружаемую OS

Маршрутизатор выбирает загружаемую OS на основании двух факторов.

- Последней шестнадцатеричной цифры значения конфигурационного регистра (загрузочного поля).
- Любых глобальных команд конфигурации `boot system` в файле `startup-config`.

Загрузочное поле (boot field), четвертая шестнадцатеричная цифра в конфигурационном регистре, указывает маршрутизатору загружаемую OS. Маршрутизатор проверяет значение загрузочного поля при включении и перезагрузке, чтобы узнать, какую OS выбрать для загрузки.

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 первый образ операционной системы Cisco IOS из флеш-памяти

Этап 3 Если загрузочное поле регистра содержит значение от 2 до F:

А) По порядку выполняется перебор всех команд `boot system` в стартовом конфигурационном файле 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 исключительно 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 гло-

бальной 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"? 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. 20.4 представлена схема ключевых этапов поиска и загрузки образа операционной системы.

Ключевая тема

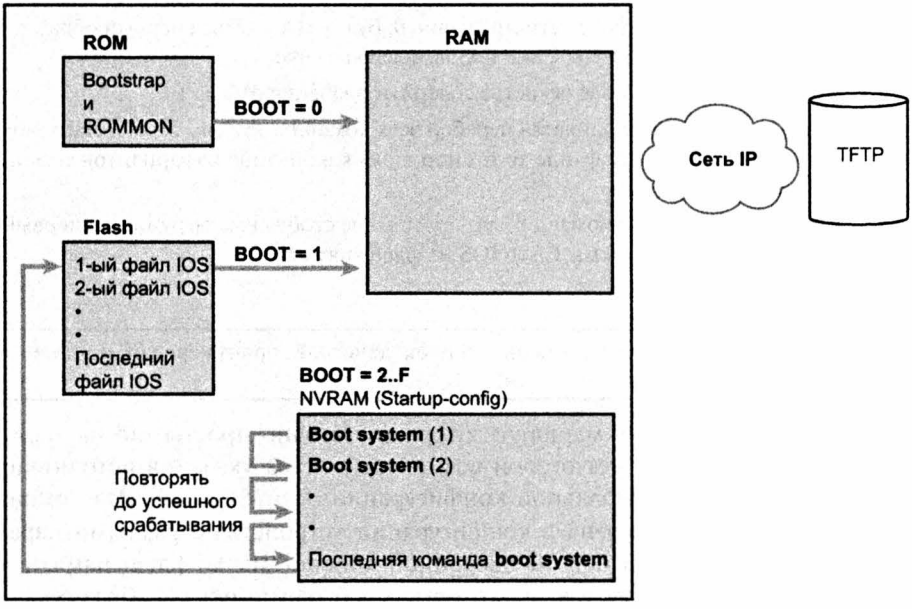


Рис. 20.4. Варианты загрузки операционной системы в современных маршрутизаторах Cisco

Таблица 20.2. Примеры команды `boot system`

Команда `boot system`	Результат
`boot system flash`	Загружается первый файл из системной флеш-памяти
`boot system flash` *имя_файла*	Из системной флеш-памяти загружается IOS по имени *имя_файла*
`boot system tftp` *имя_файла* `10.1.1.1`	IOS по имени *имя_файла* загружается с сервера TFTP по адресу 10.1.1.1

И наконец, помните процесс обновления IOS? После копирования нового файла IOS во флеш-память на маршрутизаторе процессу обновления остается еще несколько этапов: добавить команду `boot system`, ссылающуюся на правильный новый файл, сохранить конфигурацию и перезагрузить маршрутизатор. Маршрутизатор пройдет уже описанную в этом разделе последовательность загрузки и загрузит новый образ IOS. На этом процесс обновления IOS завершается. Представленный в примере 20.1 маршрутизатор копировал образ IOS во флеш; впоследствии ему понадобилось бы сохранить команду `boot system flash:c2900-universalk9-mz.SPA.152-4.M1.bin` в файле `startup-config`.

Восстановление при невозможности загрузки IOS

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.

Если к концу этапа 3 маршрутизатор не находит образ OS, он посылает широковещательное сообщение в поисках сервера TFTP. Он сообщает имя файла образа IOS и загружает его, если находит сервер TFTP. На практике этот процесс вряд ли сработает. В качестве последнего шанса маршрутизатор пытается загрузить операционную систему ROMMON, что является первым этапом процесса восстановления после отказа такого типа. Операционная система ROMMON предоставляет достаточно функций, чтобы скопировать новый файл IOS во флеш с сервера TFTP, если кто-то по ошибке стер прежний образ IOS во флеш-памяти.

Проверка образа IOS с использованием команды `show version`

Команда `show version` сообщает разнообразную информацию о маршрутизаторе. По образу IOS она выводит версию программного обеспечения, его источник и время его загрузки на маршрутизатор. В результате команда `show version` фактически идентифицирует ряд ключевых фактов о результатах предыдущего процесса загрузки.

Команда `show version` выводит много и других фактов, как показано в примере 20.3. Пример демонстрирует команду `show version` на маршрутизаторе R2; это тот же маршрутизатор, что и в примерах 20.1 и 20.2, где во флеш был скопирован новый образ IOS. С тех пор на маршрутизатор R2 была добавлена команда `boot system flash:c2900-universalk9-mz.SPA.152-4.M1.bin`, и он был перезагружен, чтобы завершить переход на использование новой версии IOS 15.2(4).

В примере команды выделено много элементов, демонстрирующих некоторые из наиболее важных фактов. Ниже описан каждый из элементов вывода в порядке их расположения в примере.

Ключевая тема

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 20.3 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 20.3. Вывод команды `show version`

```
R2# show version
Cisco IOS Software, C2900 Software (C2900-UNIVERSALK9-M), Version
15.2(4)M1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright 1986-2012 by Cisco Systems, Inc.
Compiled Thu 26-Jul-12 20:54 by prod_rel_team

ROM: System Bootstrap, Version 15.0(1r)M15, RELEASE SOFTWARE (fc1)

R2 uptime is 44 minutes
System returned to ROM by reload at 19:44:01 UTC Tue Feb 12 2013
System restarted at 19:45:53 UTC Tue Feb 12 2013
System image file is "flash:c2900-universalk9-mz.SPA.152-4.M1.bin"
Last reload type: Normal Reload
Last reload reason: Reload Command


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 CISCO2901/K9 (revision 1.0) with 483328K/40960K bytes of memory.
Processor board ID FTX1628837T
2 Gigabit Ethernet interfaces
4 Serial(sync/async) interfaces
1 terminal line
DRAM configuration is 64 bits wide with parity enabled.
255K bytes of non-volatile configuration memory.
3425968K bytes of USB Flash usbflash1 (Read/Write)
250880K bytes of ATA System CompactFlash 0 (Read/Write)


License Info:

License UDI:

-------------------------------------------------
Device#    PID                 SN
-------------------------------------------------
*0         CISCO2901/K9        FTX1628837T


Technology Package License Information for Module:'c2900'

-----------------------------------------------------------------
Technology    Technology-package          Technology-package
              Current       Type          Next reboot
-----------------------------------------------------------------
ipbase        ipbasek9      Permanent     ipbasek9
security      None          None          None
uc            None          None          None
data          None          None          None

Configuration register is 0x2102
```

Восстановление пароля

Предположим, администратор пытается подключиться со своего компьютера к маршрутизатору по протоколу SSH или Telnet, но у него ничего не получается. Либо он может войти в пользовательский режим, но не в привилегированный, поскольку он забыл пароль. Теперь необходимо восстановить или по крайней мере сбросить пароль, чтобы можно было войти в маршрутизатор и изменить конфигурацию. Как это сделать?

Можно сбросить пароль на маршрутизаторе Cisco, имея к нему физический доступ. Имея доступ к маршрутизатору с консоли и возможность отключить и снова включить его питание, любой мог бы сбросить все пароли на маршрутизаторе и заменить их новыми значениями.

Подробности зависят от модели маршрутизатора, но если зайти на `www.cisco.com` и поискать по ключевым словам "password recovery" (восстановления пароля), то среди нескольких первых ссылок можно найти главную страницу восстановления пароля с инструкциями по восстановлению пароля (фактически сбросу пароля) для практически любой модели изделия Cisco.

ВНИМАНИЕ!

В документации компании Cisco тема данного раздела упоминается как "восстановление пароля", но фактически речь идет не о возвращении или отображении забытого пароля, а о его замене новым значением.

Общие представления о восстановлении (сбросе) пароля Cisco

Хотя подробности зависят от конкретной модели, все процедуры восстановления пароля следуют тем же общим принципам. Первая задача процесса — заставить маршрутизатор загрузить операционную систему IOS, игнорируя файл `startup-config`, содержащий все пароли. Как только маршрутизатор загрузится, проигнорировав начальную конфигурацию, к консоли можно подключиться без ввода пароля и перенастроить все пароли.

Компания Cisco определяет бит конфигурационного регистра, установка которого в двоичную 1 указывает маршрутизатору игнорировать файл `startup-config` при следующей загрузке. Для установки этого значения стандартное значение конфигурационного регистра 0x2102 следует изменить на 0x2142.

К сожалению, для доступа к режиму, позволяющему изменить значение конфигурационного регистра, необходимо помнить пароль перехода в привилегированный режим. Однако необходимость восстановления пароля возникает, когда пароль неизвестен. Так как же изменить конфигурационный регистр? Решение — в использовании режима операционной системы ROMMON.

Операционная система ROMMON позволяет вводить команды, включая команды установки конфигурационного регистра. По сравнению с операционной системой IOS, набор команд CLI у операционной системы ROMMON несколько меньше. Эти команды также зависят от конкретной модели маршрутизатора, но программное обеспечение ROMMON каждого маршрутизатора имеет некую команду, обычно `confreg`, позволяющую установить значение конфигурационного регистра. Например, команда ROMMON `confreg 0x2142` установила бы соответствующий бит и указала бы маршрутизатору игнорировать файл `startup-config` при загрузке.

Так как же заставить маршрутизатор загрузиться в режиме ROMMON? Старые маршрутизаторы поддерживают традиционную возможность — кнопку сброса на консоли, а более новые могут потребовать удаления флеш-памяти.

- **Старые маршрутизаторы**. Подключившись к консоли, используйте эмулятор терминала для ввода команд в CLI. Питание маршрутизатора отключается, а затем снова включается. Затем, в течение первых 30 секунд, на клавиатуре удерживайте нажатой клавишу <break>. Это заставит маршрутизатор нарушить обычную последовательность загрузки и загрузить операционную систему ROMMON.
- **Более новые маршрутизаторы (с внешней флеш-памятью)**. Выньте все флеш-карты, выключите маршрутизатор, а затем включите его снова. Маршрутизатор не сможет загрузить операционную систему IOS и вместо нее загрузит ROMMON. (После загрузки ROMMON вставьте все вынутые флеш-карты на место.)

Таким образом, в основе восстановления пароля лежат следующие идеи.

Три ключевые концепции процесса восстановления пароля маршрутизатора Ключевая тема

Этап 1 Загрузить операционную систему ROMMON либо за счет вмешательства в процесс загрузки с консоли, либо предварительного удаления всей флеш-памяти

Этап 2 Заставить конфигурационный регистр игнорировать файл `startup-config` (например, командой `confreg 0x2142`)

Этап 3 Загрузить маршрутизатор уже с операционной системой IOS, чтобы консоль смогла перейти в привилегированный режим, не нуждаясь в паролях

Конкретный пример сброса пароля

Пример 20.4 демонстрирует процесс восстановления (сброса) пароля на маршрутизаторе модели 2901. В начале примера маршрутизатор R1 включен и пользователь подключен к консоли. У маршрутизатора 2901 есть слоты компактной флеш-памяти, а также слоты USB, подходящие для накопителей флеш, поэтому в данном примере автор удалял флеш-память, чтобы перевести процесс начальной загрузки маршрутизатора в режим ROMMON. Вначале маршрутизатор R1 включен. Вот этапы примера.

Этап 1 Отключите питание маршрутизатора

Этап 2 Осторожно извлеките компактную флеш-карту из маршрутизатора

Этап 3 Включите питание маршрутизатора

Этап 4 Просмотрите сообщения инициализации и дождитесь приглашения `ROMMON>`

Этап 5 Как только маршрутизатор перейдет в режим ROMMON и отобразится приглашение `ROMMON>`, осторожно вставьте флеш-карту на место

Этап 6 Используя команду ROMMON `confreg 0x2142`, установите в конфигурационном регистре значение 0x2142

Этап 7 Введите команду ROMMON `reset`, запускающую нормальный процесс перезагрузки маршрутизатора (включающий использование нового значения конфигурационного регистра)

Этап 8 Убедитесь, что операционная система IOS запросила переход в режим начальной конфигурации, поскольку она должна загрузиться без начальной конфигурации

Этап 9 Подключитесь с консоли (никакой пароль не нужен) и перейдите в привилегированный режим. Это потребует проверки пароля, но паролей уже нет

Этап 10 Введите команду `copy startup-config running-config`, чтобы вернуть всю конфигурацию в исходное состояние, чтобы маршрутизатор начал свою работу заново

Этап 11 Перейдите в режим конфигурации, сбросьте все забытые пароли и введите новые

Этап 12 Введите команду `copy running-config startup-config`, чтобы сохранить всю конфигурацию, включая измененные пароли

Этап 13 Верните конфигурационный регистр в его нормальное значение (обычно это 0x2102), чтобы при следующей загрузке маршрутизатор не загрузил снова операционную систему ROMMON

Пример 20.4. Восстановление/сброс пароля

```
R1#! 1) Пользователь подходит к маршрутизатору и отключает питание

! 2) Пользователь удаляет всю флеш-память

! 3) Пользователь снова включает питание

System Bootstrap, Version 15.0(1r)M15, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright 2011 by cisco Systems, Inc.
Total memory size = 512 MB - On-board = 512 MB, DIMM0 = 0 MB
CISCO2901/K9 platform with 524288 Kbytes of main memory
Main memory is configured to 72/-1(On-board/DIMM0) bit mode with ECC
enabled

! 4) Несколько строк инициализации ROMMON пропущено:

Readonly ROMMON initialized
rommon 1 > confreg 0x2142

You must reset or power cycle for new config to take effect
rommon 2 >
! 6) Пользователь подходит к маршрутизатору и возвращает флеш-память

rommon 3 > reset

System Bootstrap, Version 15.0(1r)M15, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright 2011 by cisco Systems, Inc.

Total memory size = 512 MB - On-board = 512 MB, DIMM0 = 0 MB
CISCO2901/K9 platform with 524288 Kbytes of main memory
Main memory is configured to 72/-1(On-board/DIMM0) bit mode with ECC ena-
bled

! Множество строк сообщений инициализации IOS пропущено

                --- System Configuration Dialog ---

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

```
Press RETURN to get started!

! 9) Пользователь подключился с консоли, для перехода в привилегированный
режим пароль не требуется

Router>
Router> enable

! 10) Пользователь копирует файл startup-config, чтобы вернуть маршрути-
затор к нормальной работе
Router# copy startup-config running-config
Destination filename [running-config]?
3297 bytes copied in 0.492 secs (6701 bytes/sec)

! 11) Пользователь заменяет забытый пароль
R1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)# enable secret cisco
R1(config)# ^Z
R1#

! 12) Пользователь сохраняет внесенные изменения
R1# copy running-config startup-config
Destination filename [startup-config]?
3297 bytes copied in 0.492 secs (6701 bytes/sec)

! 13) Пользователь возвращает конфигурационный регистр в его нормальное
значение 0x2102
R1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)# config-reg 0x2102
R1(config)# ^Z
R1#
```

Обратите внимание, что последние этапы весьма важны. Помните, что маршрутизатор загрузился без начальной конфигурации, поэтому явно не готов к нормальной работе. Команда `copy startup-config running-config` компенсирует тот факт, что маршрутизатор проигнорировал файл `startup-config` при загрузке IOS. Кроме того, для подготовки к следующей перезагрузке маршрутизатора верните значение конфигурационного регистра в нормальное состояние, обычно это шестнадцатеричное 2102.

ВНИМАНИЕ!

Команда `copy running-config startup-config` могла отключить некоторые из интерфейсов, в зависимости от текущего состояния кабельного соединения и состояния подключенных устройств. Поэтому проверьте и включите все необходимые интерфейсы подкомандой интерфейса `no shutdown`.

Управление файлами конфигурации

Маршрутизаторы и коммутаторы Cisco иногда используют два разных файла конфигурации: файл `startup-config` для сохранения конфигурации, используе-

мой при каждой загрузке устройства, и файл running-config, содержащий текущую конфигурацию, используемую в настоящее время и расположенную в оперативной памяти.

Этот последний из трех главных разделов главы посвящен обзору некоторых ключевых фактов об этих двух файлах конфигурации. В нем также обсуждается команда copy и ее использование для копирования содержимого файлов конфигурации. Завершается данный раздел кратким напоминанием диалога начальной загрузки, позволяющего маршрутизатору создать файл начальной конфигурации.

Основы файла конфигурации

Операционная система Cisco IOS хранит набор команд конфигурации в *файле конфигурации* (configuration file). Фактически маршрутизаторы используют несколько файлов конфигурации: один файл для начальной конфигурации, используемой при включении устройства; и другой файл для активной, используемой в настоящее время конфигурации, хранимой в оперативной памяти. В табл. 20.3 приведены имена этих двух файлов, их цель и область хранения.

Ключевая тема **Таблица 20.3. Имена и цели двух основных файлов конфигурации Cisco IOS**

Имя файла конфигурации	Цель	Место хранения
startup-config	Хранит начальную конфигурацию, используемую при каждой загрузке операционной системы Cisco IOS	NVRAM
running-config	Хранит команды конфигурации, используемые в настоящее время. При вводе команд в режиме конфигурации этот файл изменяется динамически	RAM

По существу, когда используется режим конфигурации, изменяется только файл running-config. Если эту конфигурацию необходимо сохранить, следует ввести команду copy running-config startup-config, чтобы переписать прежний файл startup-config.

В примере 20.5 показано, что используемые в режиме конфигурации команды изменяют только файл running-config в оперативной памяти. Пример демонстрирует следующие концепции и этапы.

Этап 1 Исходное имя хоста маршрутизатора, когда файл startup-config соответствует файлу running-config

Этап 2 Команда hostname изменяет имя хоста, но только в файле running-config

Этап 3 Команды show running-config и show startup-config демонстрируют, что команды hostname сделали два файла конфигурации различными

Пример 20.5. Изменение файла running-config, но не файла startup-config

```
! Этап 1 (две команды)
!
hannah# show running-config
! (строки пропущены)
```

```
hostname hannah
! (остальные строки пропущены)

hannah# show startup-config
! (строки пропущены)
hostname hannah
! (остальные строки пропущены)

! Этап 2. Обратите внимание, что приглашение к вводу команд изменилось
! немедленно после команды hostname.
!
hannah# configure terminal
hannah(config)# hostname kris
kris(config)# exit

! Этап 3 (две команды)
!
kris# show running-config
! (строки пропущены)
hostname kris
! (остальные строки пропущены - обратите внимание, что
! файл running-config отражает измененное имя хоста)

kris# show startup-config
! (строки пропущены)
hostname hannah
! (остальные строки пропущены - обратите внимание, что измененная
! конфигурация не отображается в файле startup-config)
```

Копирование и удаление файлов конфигурации

Если в конце примера 20.5 перезагрузить маршрутизатор, имя хоста снова станет `hannah`, поскольку файл `running-config` не был скопирован в файл `startup-config`. Но если необходимо сохранить новое имя хоста `kris`, то следует использовать команду `copy running-config startup-config`, перезаписывающую текущий файл `startup-config` текущим содержимым файла `running-config`.

Для копирования файлов на маршрутизаторе используется команда IOS `copy`. Файлы могут быть любыми, но чаще всего это либо образы IOS, либо файлы конфигурации.

Кроме копирования файла `running-config` в `startup-config` для сохранения изменений, команду `copy` чаще всего используют для резервного копирования файлов конфигурации. Файлы `startup-config` и `running-config` можно скопировать на сервер и с сервера назад на маршрутизатор, как показано на рис. 20.5.

В общем виде команды копирования конфигурации Cisco IOS на рисунке можно представить следующим образом:

```
copy {tftp | running-config | startup-config} {tftp | running-config |
  startup-config}
```

Первый набор заключенных в фигурные скобки ({}) параметров — это области источников файла, а следующий набор — области назначения.

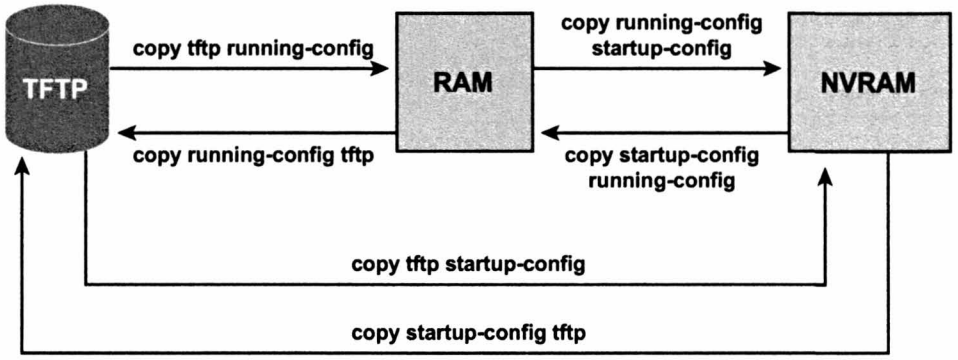


Рис. 20.5. Области и случаи копирования

Команда `copy` всегда заменяет существующий файл при копировании в NVRAM или на сервер TFTP. Другими словами, прежний файл как бы удаляется, а новый полностью заменяет его. Но когда команда `copy` копирует файл конфигурации в файл `running-config` в оперативной памяти, файл не заменяется, а объединяется. Фактически любое копирование в оперативную память работает так, как если бы команды из файла конфигурации вводились бы в том же порядке.

Зачем это сделано? Если текущая конфигурация была изменена, но затем возникает необходимость вернуться к тому, что было в файле `startup-config`, то результат команды `copy startup-config running-config` может и не сделать эти два файла фактически тождественными. Единственный способ гарантировать соответствие этих двух файлов конфигурации — использовать команду `reload`, которая перезагрузит маршрутизатор, стерев оперативную память, а затем скопирует файл `startup-config` в оперативную память в ходе процесса перезагрузки.

ВНИМАНИЕ!

Все образы IOS Cisco и все задачи управления файлами, включая команду `copy`, поддерживают также протокол IPv6. Поэтому, если установлены серверы IPv6 TFTP в сети IPv6, команда `copy` отлично сработает и с новым семейством протоколов.

В лабораторной работе с соседними маршрутизаторами удобней было бы копировать файлы со съемного носителя флеш и на него. Слоты USB на последних моделях маршрутизаторов Cisco позволяют вставлять и удалять носитель флеш для USB. Например, у маршрутизатора Cisco 2901 есть два слота USB (USBFlash0: и USBflash1:). Как показано в примере 20.6, инженер мог легко скопировать файл `running-config` на носитель флеш.

Пример 20.6. Копирование файла на носитель флеш для USB

```
R1# copy running-config usbflash1:temp-copy-of-config
Destination filename [temp-copy-of-config]?
3159 bytes copied in 0.944 secs (3346 bytes/sec)

R1# dir usbflash1:
Directory of usbflash1:/
```

```
 1  -rw-     4096 Feb 11 2013 17:17:00 +00:00 ._.Trashes
 2  drw-        0 Feb 11 2013 17:17:00 +00:00 .Trashes
 7  drw-        0 Feb 11 2013 17:17:00 +00:00 .Spotlight-V100
73  -rw- 97794040 Feb 12 2013 21:49:36 +00:00 c2900-universalk9-
mz.SPA.152-4.
M1.bin
74  -rw-     3159 Feb 12 2013 22:17:00 +00:00 temp-copy-of-config

7783804928 bytes total (7685111808 bytes free)
R1#
```

Помимо копирования, файлы можно также удалять. Например, операционная система IOS поддерживает три разных команды для удаления файла `startup-config` в NVRAM. Команды `write erase` и `erase startup-config` являются устаревшими, поэтому рекомендуется более новая команда `erase nvram`.

Обратите внимание, что у операционной системы Cisco IOS нет команды удаления содержимого файла `running-config`. Чтобы убрать файл `running-config`, достаточно удалить файл `startup-config` и перезагрузить маршрутизатор.

ВНИМАНИЕ!

Создание резервных копий всех текущих конфигураций маршрутизаторов должно быть частью общей стратегии защиты любой сети. Хранение копий конфигурации облегчит восстановление после ошибок или атак, изменяющих конфигурацию.

Обратите внимание на еще одну деталь в именах файлов конфигурации: большинство людей используют общепринятые имена `startup-config` и `running-config`, но операционная система Cisco IOS определяет несколько других, более формальных имен для этих файлов. Эти имена файлов используют формат, определенный *файловой системой Cisco IOS* (Cisco IOS File System — IFS), используемой операционной системой Cisco IOS для управления файлами. Например, команда `copy` может обратиться к файлу `startup-config` как к `nvram:startup-config`. Альтернативные имена этих двух файлов конфигурации приведены в табл. 20.4.

Таблица 20.4. Имена IFS файлов конфигурации

Общепринятое имя файла конфигурации	Альтернативное имя
`startup-config`	`nvram:startup-config`
`running-config`	`system:running-config`

Диалог начальной настройки

В операционной системе Cisco IOS есть два основных метода создания начальной конфигурации устройства: режим конфигурирования, который был подробно описан выше, и *диалог 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 ме-

ре, до тех пор, пока они не наберутся опыта работы с интерфейсом командной строки устройств компании Cisco.

На рис. 20.6 приведен диалог начальной настройки коммутатора. Этот диалог чаще всего используется после загрузки операционной системы устройства, когда в памяти NVRAM нет конфигурации. Перейти к диалогу начальной настройки можно с помощью команды **`setup`** в режиме привилегированного пользователя.

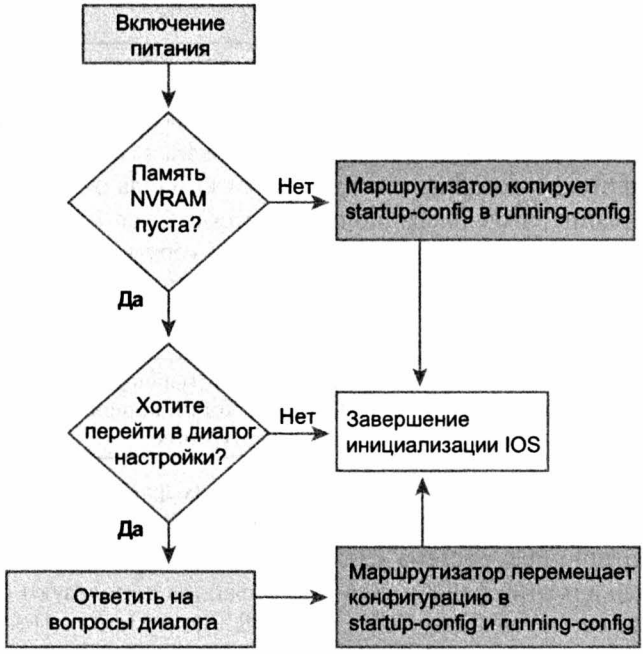


Рис. 20.6. Логика и описание диалога начальной загрузки после перезагрузки

ВНИМАНИЕ!

Процесс восстановления пароля представлен в примере 20.3. Этот процесс заставил маршрутизатор загрузиться, игнорируя начальную конфигурацию, задав пользователю вопрос, представленный на рис. 20.6.

Обзор

Резюме

- В качестве операционной системы (Operating System — OS) маршрутизаторы Cisco используют программное обеспечение Cisco IOS.
- Процесс обновления образа IOS включает такие этапы, как копирование более нового образа IOS во флеш-память, указание маршрутизатору, какой именно образ IOS использовать, и удаление прежнего образа IOS после проверки работоспособности новой версии.
- При включении процесс загрузки на маршрутизаторе должен быть готов выбрать правильный образ IOS для использования, а если этот процесс по какой-нибудь причине терпит неудачу, то иметь способ преодолеть или устранить эту проблему.
- В процессе загрузки маршрутизатор проходит следующие этапы.
  1. После включения или переключения питания маршрутизатор выполняет процедуру самотестирования при включении питания (POST), с помощью которой обнаруживает аппаратные компоненты и проверяет, что все они работают правильно.
  2. Далее маршрутизатор из постоянного запоминающего устройства (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`).
- 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.
- Маршрутизаторы используют конфигурационный регистр во время загрузки для получения неких параметров конфигурации прежде, чем будет загружена операционная система IOS и прочитан файл `startup-config`.
- Маршрутизатор выбирает загружаемую OS на основании двух факторов: последней шестнадцатеричной цифры значения конфигурационного регистра (загрузочного поля) и любых глобальных команд конфигурации `boot system` в файле `startup-config`.

- Команда `show version` сообщает разнообразную информацию о маршрутизаторе. По образу IOS она выводит версию программного обеспечения, его источник и время его загрузки на маршрутизатор.
- Имея доступ к маршрутизатору с консоли и возможность отключить и снова включить его питание, любой мог бы сбросить все пароли на маршрутизаторе и заменить их новыми значениями.
- Для копирования файлов на маршрутизаторе используется команда IOS copy. Файлы могут быть любыми, но чаще всего это либо образы IOS, либо файлы конфигурации.
- В операционной системе Cisco IOS есть два основных метода создания начальной конфигурации устройства: режим конфигурирования и диалог начальной настройки.
- Диалог начальной настройки в интерактивной форме запрашивает у системного администратора базовые параметры устройства.

Контрольные вопросы

Ответьте на эти вопросы. Ответы можно найти на последней странице главы. Полное объяснение ответов приведено в приложении B на веб-сайте.

1. Каков первый этап процесса загрузки маршрутизатора?

   А) Маршрутизатор находит файл конфигурации.

   Б) Процедура POST.

   В) Маршрутизатор находит образ Cisco IOS.

   Г) Маршрутизатор инициализирует код самозагрузки из ROM.

2. Каков первый этап процесса загрузки типичного маршрутизатора Cisco при попытке найти загружаемую операционную систему?

   А) Маршрутизатор ищет образ на сервере TFTP.

   Б) Маршрутизатор проверяет поле начальной загрузки конфигурационного регистра.

   В) Маршрутизатор загружает операционную систему ROMMON.

   Г) Маршрутизатор ищет файл образа Cisco IOS во флеш-памяти.

3. Какой командой после начальной загрузки маршрутизатора Cisco проще всего проверить загруженный образ Cisco IOS и выяснить место, откуда он был скопирован в оперативную память?

   А) `show running-config`.

   Б) `show boot`.

   В) `show cisco ios`.

   Г) `show version`.

4. Какое значение конфигурационного регистра контролирует загрузку маршрутизатора?

   А) Третий шестнадцатеричный символ.

   Б) Второй шестнадцатеричный символ.

В) Первый шестнадцатеричный символ.

Г) Последний шестнадцатеричный символ.

5. Пароль привилегированного режима забыт, и невозможно получить доступ к глобальному режиму конфигурации. Как в процессе восстановления пароля изменить конфигурационный регистр, если невозможно вспомнить пароль для перехода в режим конфигурации маршрутизатора?

   А) Использовать режим операционной системы ROMMON.

   Б) Использовать утилиту Setup.

   В) Настроить устройство, используя GUI.

   Г) Использовать режим сброса пароля.

6. Какая память маршрутизатора используется для хранения конфигурации, когда он включен и работает?

   А) RAM.

   Б) ROM.

   В) Flash.

   Г) NVRAM.

7. Что делает маршрутизатор Cisco, когда при загрузке с использованием файла образа во флеш-памяти он не имеет файла `startup-config`?

   А) Маршрутизатор переходит в режим ROMMON.

   Б) Маршрутизатор запрашивает у пользователя разрешение на запуск утилиты Setup.

   В) Маршрутизатор не загружает IOS.

   Г) Маршрутизатор запрашивает у пользователя URL файла начальной конфигурации.

Ключевые темы

Повторите все ключевые темы данной главы, отмеченные пиктограммой "Ключевая тема". Ключевые темы и соответствующие им страницы перечислены в табл. 20.5.

Таблица 20.5. Ключевые темы главы 20

Элемент	Описание	Страница
Список	Этапы загрузки маршрутизатора Cisco	638
Список	Этапы выбора источника операционной системы Cisco IOS в процессе загрузки устройства	641
Рис. 20.4	Варианты загрузки операционной системы в современных маршрутизаторах Cisco	642
Список	Список наиболее важной информации, которую можно получить с помощью команды show version	644
Список	Три ключевые концепции процесса восстановления пароля маршрутизатора	647
Табл. 20.3	Имена и цели двух основных файлов конфигурации Cisco IOS	650

Ключевые термины

После первого прочтения главы попытайтесь дать определения следующим ключевым терминам. Но не расстраивайтесь, если не все получится сразу, в главе 22 описано, как использовать эти термины на завершающем этапе подготовки к экзамену.

загрузочное поле (boot field), конфигурационный регистр (configuration register), образ IOS (IOS image), монитор ROM (ROM Monitor — ROMMON), файл `startup-config`, файл `running-config`, режим начальной конфигурации (setup mode), межсетевая операционная система (Internetwork Operating System — IOS), постоянное запоминающее устройство (Read-only memory — ROM), флеш-память (flash memory), энергонезависимая память (Nonvolatile RAM — NVRAM)

Таблицы команд

Ниже приведены краткие описания команд, использованных в этой главе.

Таблица 20.6. Конфигурационные команды главы 20

Команда	Описание
`config-register` *значение*	Глобальная команда, устанавливающая шестнадцатеричное значение конфигурационного регистра
`boot system {` *url_файла* `|` *имя_файла*`}`	Глобальная команда, задающая внешний источник образа IOS по его URL
`boot system flash [`*флеш_fs*`:] [`*имя_файла*`]`	Глобальная команда, задающая источник образа IOS во флеш-памяти
`boot system rom`	Глобальная команда, указывающая маршрутизатору, что нужно загрузить систему RxBoot из памяти ROM
`boot system {rcp	tftp	ftp}` *имя_файла* `[`*ip-адрес*`]`	Глобальная команда, указывающая внешний сервер, протокол и название файла, которые будут использоваться для загрузки операционной системы

Таблица 20.7. Команды EXEC главы 20

Команда	Описание
`reload`	Пользовательская команда привилегированного режима, перезагружающая коммутатор или маршрутизатор
`copy` *откуда куда*	Пользовательская команда привилегированного режима, копирующая файлы из одного места в другое. Копируются файлы `startup-config` и `running-config`, файлы на серверах TFTP и RPC, а также флеш-память
`copy running-config startup-config`	Пользовательская команда привилегированного режима, сохраняющая активную конфигурацию за счет замены файла `startup-config` при инициализации коммутатора
`copy startup-config running-config`	Пользовательская команда привилегированного режима, объединяющая файл `startup-config` с файлом конфигурации, активным в оперативной памяти в настоящее время

Окончание табл. 20.7

Команда	Описание
`show running-config`	Выводит содержимое файла `running-config`

`write erase`
`erase startup-config`
`erase nvram:`
	Три пользовательских команды привилегированного режима, удаляющих файл `startup-config`

`setup`	Пользовательская команда привилегированного режима, переводящая в режим начальной конфигурации, в котором операционная система Cisco IOS запрашивает у пользователя основные параметры конфигурации
`show flash`	Выводит имена и размер файлов во флеш-памяти, а также указывает объем использованной и доступной флеш-памяти

Ответы на контрольные вопросы:

1 Б. 2 Б. 3 Г. 4 Г. 5 А. 6 А. 7 Б.

Глава 21

Управление лицензиями IOS

Поскольку компания Cisco внесла серьезные изменения в способ создания программного обеспечения для маршрутизаторов Cisco, изменился и способ лицензирования программного обеспечения для частных лиц и организаций. В этой главе рассматриваются прежние методы и подробности внесенных изменений, а также фактический процесс проверки текущих лицензий, установки новых лицензий, активизации кода лицензии и даже резервное копирование и удаление лицензий с устройства.

В этой главе рассматриваются следующие экзаменационные темы
Технологии маршрутизации IP
Управление файлами Cisco IOS
Лицензии
Просмотр лицензии
Смена лицензии

Основные темы

Пакет IOS

Компания Cisco выпускает *межсетевую операционную систему* (Internetwork Operating System — IOS) в виде единого файла. Это упрощает инсталляцию новой версии IOS: достаточно загрузить с сервера Cisco один файл, скопировать его во флеш-памяти на маршрутизаторе, а затем выполнить действия, гарантирующие начальную загрузку маршрутизатора в следующий раз с использованием нового образа IOS (подробнее об этом процессе см. в главе 20).

Компания Cisco продолжает выпускать операционную систему IOS как единый файл, но содержимое этого файла изменилось. В данном разделе рассматриваются и старые, и новые способы создания образов, а также новые средства лицензирования IOS, разрешающие маршрутизатору использовать разные элементы IOS.

Образы IOS для каждой модели и серии, а также их версии и выпуски

Начиная с 1980-х годов и на протяжении следующего десятилетия компания Cisco выпускала каждый образ IOS для конкретной модели маршрутизатора, версии, выпуска и набора средств.

Во-первых, из-за аппаратных различий компания Cisco нуждалась в различных образах IOS для разных моделей маршрутизаторов или, по крайней мере, для их разных семейств. Минимальный маршрутизатор с ограниченными физическими интерфейсами нуждался в программном обеспечении, отличном от высокопроизводительного маршрутизатора, поддерживающего множество разных типов интерфейсных плат. Кроме того, разные модели маршрутизаторов зачастую использовали разные процессоры, поэтому компания Cisco компилировала различные образы IOS для использования на разных процессорах.

Во-вторых, компания Cisco нуждалась в разных образах IOS для каждой новой версии или выпуска операционной системы Cisco IOS. Для идентификации главных номеров выпусков программного обеспечения Cisco IOS используется термин *версия* (version), а для меньших изменений — *выпуск* (release). Однако компания Cisco не использует стратегию установки операционной системы IOS в виде одного файла с последующей установкой исправляющих ошибки дополнений в виде отдельных файлов. Вместо этого для исправления ошибок следует перейти на новый выпуск или новую версию, т.е. получить с сервера Cisco новый файл IOS целиком, а затем установить его на маршрутизаторы. Хотя этот процесс и не является особо трудным (см. главу 20), но требует дополнительных административных затрат и тщательного планирования.

На рис. 21.1 представлено концептуальное представление того, что получилось у компании Cisco при множестве образов IOS для каждого маршрутизатора. У маршрутизаторов были разные образы IOS для каждой модели (или серии моделей) маршрутизатора и различных файлов IOS для каждой версии программного обеспечения в пределах каждой серии моделей. Например, у маршрутизаторов Cisco серии 2800 был свой набор образов IOS для маршрутизатора 2801 и другой набор

для трех других маршрутизаторов той же серии. Для маршрутизатора 2801 и каждого нового выпуска компания Cisco создавала и делала доступным для загрузки на сервере Cisco.com целый новый файл образа IOS.



Рис. 21.1. Образы IOS для каждой модели и серии, а также их версии и выпуски

Прежний пакет: один образ IOS для каждой комбинации средств

Кроме того, для каждой комбинации наборов средств IOS, разрешенных на маршрутизаторе, компания Cisco также создавала по одному образу. *Набор средств* (feature set) — это группа взаимосвязанных средств IOS. Например, голосовые средства маршрутизатора находились бы в одном наборе средств, а средства защиты, такие как *система предотвращения вторжений* (Intrusion Prevention System — IPS), — в наборе средств защиты.

В концепции набора средств есть очень простой резон — цена. Клиенты, требующие меньше средств, хотят платить меньше. Компания Cisco обеспечила более гибкую политику цен в зависимости от потребностей клиента.

Использование наборов средств требует предоставить еще больше образов IOS. Мало того, что необходимо по одному образу IOS на каждую модель (или серию моделей), на каждую версию и даже на каждый выпуск, так нужен еще отдельный образ на каждую комбинацию наборов средств.

Чтобы было понятней, на рис. 21.2 концептуально представлено семь образов IOS. Каждый — для той же модели маршрутизатора, той же версии и выпуска. У всех образов есть те же базовые функции IP, а у некоторых есть и дополнительные наборы средств. И хотя на рисунке показано семь вариантов для выбора, это количество комбинаций намного скромнее, чем у реальных наборов средств для типичной модели маршрутизатора.



Рис. 21.2. Старый пакет образов IOS: разные образы с разными наборами средств

Предположим, например, что необходимо использовать определенное средство защиты, находящееся в наборе средств защиты. Можно купить любой из четырех образов IOS с выделенным набором средств защиты. Если не нужны никакие дополнительные средства IP или голосовые средства, то образы IOS справа можно отбросить, так как они слишком дороги из-за множества включенных наборов средств.

Новый пакет IOS: один универсальный образ со всеми наборами средств

В настоящее время компания Cisco начала выпуск пакета IOS с универсальным образом. Термин *универсальный образ* (universal image) подразумевает "все наборы средств". Вместо старой модели одного образа с определенной комбинацией наборов средств (см. рис. 21.2) компания Cisco выпускает один универсальный образ со всеми наборами средств. Однако для каждой модели (или серии моделей маршрутизаторов), а также версий выпусков, только не для разных наборов средств, все еще требуется отдельный универсальный образ.

Например, если маршрутизатор поддерживает базовые средства IP, голос, защиту и дополнительный набор средств IP, то компания Cisco создала бы один универсальный образ со всеми этими средствами для каждой модели (серии) маршрутизатора и для каждой версии (выпуска). На рис. 21.3 представлен пример одного образа, содержащего базовые средства IP, средства защиты, голоса, данных и видео.

Ключевая тема



Рис. 21.3. Универсальный образ: один образ содержит все средства

Активация программного обеспечения IOS при универсальном образе

Ранее компания Cisco позволяла любому загрузить любой образ IOS для любого маршрутизатора Cisco. Процесс загрузки обязывает установить флажок, подтверждающий, что вы согласны с условиями использования. Однако любой мог получить образы IOS для любых реальных устройств Cisco.

Политика Cisco хорошо работала с добросовестными клиентами, однако не трудно догадаться, что это открыло возможность злоупотребления программным обеспечением Cisco IOS. Например, компания вполне могла покупать подержанные аппаратные средства Cisco, загружать последнюю версию программного обеспечения Cisco IOS и использовать его, несмотря на явное нарушение условия пользования, ведь они не заплатили компании Cisco вообще ничего за программное обеспечение. Либо кли-

енты могли не платить за право загрузки новых версий Cisco IOS, вопреки соглашению об обслуживании Cisco (SMARTnet), поскольку прежняя система позволяла загружать более новое программное обеспечение практически каждому.

Со временем компания Cisco выпустила серии 1900, 2900 и 3900 маршрутизаторов Cisco — *второе поколение маршрутизаторов с интегрированными службами* (Integrated Services Routers Generation 2 — ISR G2). Для предотвращения краж компания Cisco внесла несколько существенных изменений в процесс поддержки программного обеспечения. В первую очередь, раздел загрузки программного обеспечения на веб-сайте Cisco.com требует теперь ввода аутентификационной информации. Профиль пользователя включает название компании, и если эта компания заключила текущее соглашение об обслуживании, то разрешается загрузка программного обеспечения для определенной модели устройств. В противном случае сайт загрузки Cisco пресечет попытку загрузки программного обеспечения.

Кроме того, новейшие маршрутизаторы, такие как ISR G2, используют универсальные образы IOS с программным процессом активации. Идея проста: чтобы использовать набор средств, встроенный в универсальный образ, достаточно разблокировать его, используя программный процесс активации, определенный компанией Cisco. В универсальном образе есть все наборы средств. Программный процесс активации имеет две главные цели.

Разрешение. Разрешить или активизировать средство на маршрутизаторе. Без программной активации средство не работает, и соответствующие команды не распознаются в CLI.

Проверка прав. Проверить и подтвердить, что клиент Cisco заплатил за право использования этого набора средств на данном маршрутизаторе.

Например, клиент мог купить маршрутизатор 2901, модель маршрутизатора ISR G2, использующий универсальный образ, и пройти процесс активации программного обеспечения Cisco. Все такие маршрутизаторы поставляются с уже разрешенным базовым набором средств (Базовые IP) и ключом лицензии для этого средства. Впоследствии клиент может решить использовать программную активацию для разрешения средств защиты, что требует установки ключа лицензии для набора средств защиты, как показано на рис. 21.4.

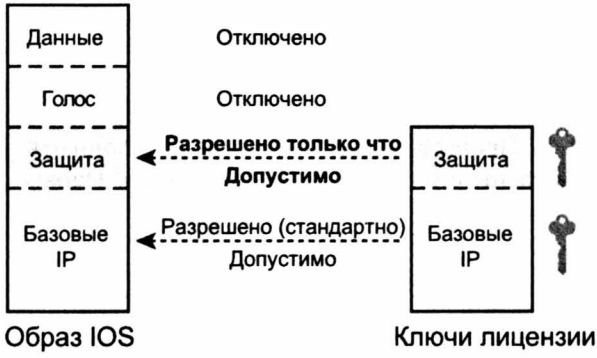


Рис. 21.4. Ключи лицензии на маршрутизаторе, разрешающие средства IOS

Компания Cisco предоставляет множество разных типов средств и лицензий. Наборы средств Cisco называются по наиболее значительному набору технологических средств. В табл. 21.1 представлены лицензии и технологии, доступные для платформ Cisco ISR G2 серий маршрутизаторов 1900, 2900 и 3900.

Таблица 21.1. Некоторые из лицензий пакетов технологий



Лицензия пакета технологий	Средства
ipbasek9 (Базовые IP)	Основные функциональные возможности IOS
datak9 (Данные)	MPLS, ATM, мультипротокольность, поддержка IBM
uck9 (Унифицированная коммуникация)	VoIP, IP-телефония
securityk9 (Защита)	IOS firewall, IPS, IPsec, 3DES, VPN

ВНИМАНИЕ!

Лицензия на базовые IP является предпосылкой для установки лицензий на защиту, данные и унифицированные коммуникации.

Управление программной активаций при помощи диспетчера лицензий Cisco

Клиенты Cisco могут заказать средства сразу при покупке маршрутизатора или добавить их позже. При заказе вместе с маршрутизатором компания Cisco установит лицензии на маршрутизатор еще на фабрике, и клиенту не придется заботиться об их добавлении. В качестве альтернативы клиент может купить лицензию для набора средств и позже, а затем, следуя процессу активации, разрешить этот набор средств на маршрутизаторе.

Большинство крупных компаний управляют лицензиями Cisco при помощи такого приложения, как *диспетчер лицензий Cisco* (Cisco License Manager — CLM). Этот бесплатный программный пакет может быть установлен на многих клиентах Windows, серверных операционных системах, а также на Sun Solaris и Red Hat Linux. Диспетчер CLM

- общается по Интернету с регистрационным порталом лицензий Cisco (Product License Registration Portal);
- получает информацию о лицензиях на средства, купленные у любого торгового представителя Cisco;
- общается с маршрутизаторами и коммутаторами компании, устанавливая ключи лицензий и разрешая средства на соответствующих устройствах.

На рис. 21.5 представлена роль диспетчера CLM в процессе лицензирования Cisco.

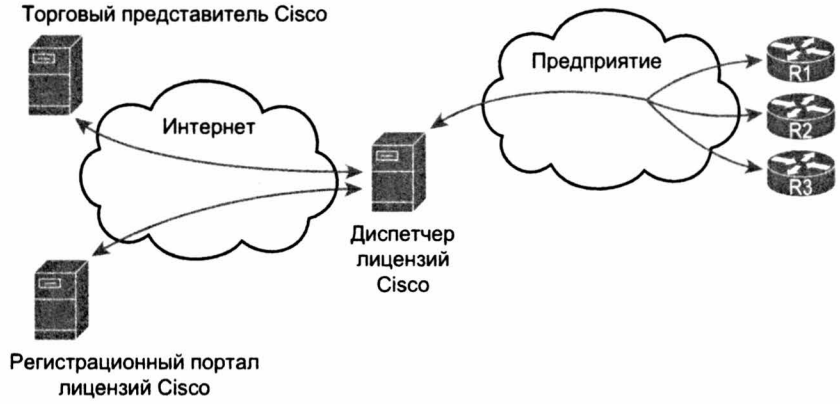


Рис. 21.5. Роль диспетчера лицензий Cisco в программной активации

Если используется диспетчер CLM, то достаточно знать лишь общие идеи лицензирования, а множество подробностей можно игнорировать, — ими займется диспетчер CLM. Лицензии можно купить у любого торгового представителя Cisco. Приложение позволяет просмотреть то, что уже куплено и что уже установлено на конкретных устройствах. Можно также выбрать определенные устройства для получения новых прав на использование новых наборов средств и разрешить эти средства в удобном графическом интерфейсе пользователя.

Использование лицензий для активации программного обеспечения вручную

Диспетчер CLM существенно упрощает весь процесс активации программного обеспечения Cisco, но его можно также осуществить и вручную. Процесс активации вручную требует найти на веб-сайте Cisco.com портал Cisco Product License Registration Portal и ввести несколько команд в CLI маршрутизатора. Кроме того, необходимо следовать многоэтапному процессу, чтобы объединить все части. Практически придется проделать всю работу, которую диспетчер CLM делает самостоятельно. В следующем разделе рассматривается самая простая версия процесса, в которой не используется ни одна из дополнительных возможностей.

У каждого маршрутизатора, модель которого поддерживает программное лицензирование, есть индивидуальный номер — *уникальный идентификатор устройства* (UDI). Идентификатор UDI имеет два основных компонента: идентификатор продукта (product ID — PID) и серийный номер (Serial Number — SN). В примере 21.1 показан вывод команды `show license udi`, демонстрирующий идентификатор продукта, серийный номер и UDI маршрутизатора.

Пример 21.1. Проверка идентификатора UDI на маршрутизаторе Cisco

```
R1# show license udi
Device#    PID                 SN              UDI
------------------------------------------------------------------------
*0         CISCO2901/K9        FTX162883H0     CISCO2901/K9:FTX162883H0
```

Затем процесс требует доказательства оплаты за лицензию на конкретное средство определенной модели маршрутизатора. В реальном мире доказательством покупки в магазине служит бумажная квитанция; квитанцией для наборов программных средств является *ключ авторизации продукта* (Product Authorization Key — PAK). Ключ PAK действует как квитанция, он имеет уникальный номер, который компания Cisco может найти в базе данных и подтвердить, лицензия на какой набор средств был фактически куплен.

Следующий этап — объединение лицензии, которую можно использовать на любом маршрутизаторе той же модели, с конкретным маршрутизатором. Для этого следует пройти процесс, объединяющий ключ PAK (обобщенные права на лицензию) с идентификатором UDI (присущим конкретному маршрутизатору), чтобы создать ключ лицензии. Для этого следует открыть в веб-браузере веб-страницу регистрационного портала лицензий Cisco и скопировать номера PAK и UDI. Сервер Cisco проверит принадлежность идентификатора UDI реальному маршрутизатору, реальность ключа PAK, что этот ключ PAK еще не использовался для разрешения этого средства на другом маршрутизаторе, и все остальные проверки, предотвращающие мошенничество. Если все проверки пройдены, компания Cisco перешлет в приложении по электронной почте файл ключа лицензии (доступный также для загрузки).

Первые три этапа приведены на рис. 21.6, а последующие — на рис. 21.7.

Этап 1 На странице регистрационного портала лицензий Cisco (доступного по адресу `www.cisco.com/go/license`) введите идентификатор UDI маршрутизатора, выданный командой `show license udi`

Этап 2 На той же странице введите ключ PAK для лицензии, купленной у торгового представителя или непосредственно у компании Cisco

Этап 3 Когда веб-сайт запросит, скопируйте файл ключа лицензии (загруженный или полученный по электронной почте)



Рис. 21.6. Значения PAK и UDI для получения уникального файла ключа лицензии от Cisco.com

ВНИМАНИЕ!

На момент написания этой книги страница регистрационного портала лицензий Cisco (`www.cisco.com/go/license`) содержала видео о выполнении этапов на рис. 21.6.

По завершении трех этапов, представленных на рис. 21.6, набор средств на маршрутизаторе все еще не разрешен. На настоящий момент, после этапа 3, ключ лицензии существует как файл. Этот ключ лицензии разблокировал один набор средств на одном маршрутизаторе, т.е. на том маршрутизаторе, UDI которого использовался для создания ключа. Остальная часть процесса разрешает лицензию на этом одном маршрутизаторе в ходе перемещения на него файла ключа лицензии и перезагрузки.

На следующем этапе файл ключа лицензии следует сделать доступным для маршрутизатора любым подходящим способом и ввести несколько команд. В лабораторной работе проще всего скопировать файл на носитель флеш для USB и вставить его в слот USB маршрутизатора. Для дистанционных маршрутизаторов скопируйте файл на доступный сервер TFTP, FTP, или HTTP. Эти этапы приведены в следующем списке как продолжение предыдущего.

Этап 4 Сделайте файл доступным для маршрутизатора при помощи USB или некоего сервера в сети

Этап 5 В интерфейсе CLI маршрутизатора введите команду `license install` *`url`*, чтобы установить файл ключа лицензии на маршрутизатор (URL указывает на файл)

Этап 6 Перезагрузите маршрутизатор, чтобы изменения вступили в силу

Следующие три этапа приведены на рис. 21.7.



Рис. 21.7. Копирование и установка лицензии на маршрутизаторе

Пример активации лицензии вручную

Чтобы перейти от общих концепций к частностям, рассмотрим пример установки лицензии данных на маршрутизаторе модели 2901. Пример начинается с просмотра текущего состояния лицензий на типичном маршрутизаторе, а затем переходит к их изменению.

Просмотр текущего состояния лицензий

Сначала на маршрутизаторе R1 разрешены только базовые средства IP. Никаких других лицензий на этом маршрутизаторе не было разрешено. Пример 21.2 демонстрирует состояние доступных средств, где выделены разрешенные базовые средства IP, а также еще три лицензии на пакеты технологий, включая защиту, голос и данные.

Пример 21.2. Первоначальные лицензии на маршрутизаторе R1

```
R1# show license
Index 1 Feature: ipbasek9
```

```
        Period left: Life time
        License Type: Permanent
        License State: Active, In Use
        License Count: Non-Counted
        License Priority: Medium
Index 2 Feature: securityk9
        Period left: Not Activated
        Period Used: 0 minute 0 second
        License Type: EvalRightToUse
        License State: Not in Use, EULA not accepted
        License Count: Non-Counted
        License Priority: None
Index 3 Feature: uck9
        Period left: Not Activated
        Period Used: 0 minute 0 second
        License Type: EvalRightToUse
        License State: Not in Use, EULA not accepted
        License Count: Non-Counted
        License Priority: None
Index 4 Feature: datak9
        Period left: Not Activated
        Period Used: 0 minute 0 second
        License Type: Permanent
        License State: Active, Not in Use
        License Count: Non-Counted
        License Priority: Medium
! Строки опущены для краткости; доступно еще 8 лицензий
```

Выделенные строки обстоятельно объясняют текущее состояние. Первая выделенная строка ссылается на базовый набор средств IP с неограниченной продолжительностью существования. (Обратите внимание, что компания Cisco разрешает набор базовых средств IP на всех маршрутизаторах, а другие наборы средств необязательны.) Следующие три выделенных раздела выводят наборы средств защиты, голоса (*унифицированная коммуникация* (Unified Communication — UC)) и данных как не активизированные. Кроме того, обратите внимание, что вывод команды `show license` на маршрутизаторе 2901 включает несколько дополнительных лицензионных средств, опущенных для краткости примера.

Команда `show license` демонстрирует несколько строк информации о состоянии средств, но, как показано в примере 21.3, команды `show version` и `show license feature` выводят более короткую информацию о состоянии. Каждая строка вывода команды `show license feature` демонстрирует в столбце `Enabled` справа текущее состояние. В конце вывода команды `show version` представлены сведения о лицензиях основных пакетов технологий.

Пример 21.3. Первоначальное состояние лицензий на маршрутизаторе R1

```
R1# show license feature
Feature name    Enforcement  Evaluation  Subscription  Enabled  RightToUse
ipbasek9        no           no          no            yes      no
securityk9      yes          yes         no            no       yes
uck9            yes          yes         no            no       yes
datak9          yes          yes         no            no       yes
gatekeeper      yes          yes         no            no       yes
```

```
SSL_VPN          yes          yes          no           no        yes
ios-ips-update   yes          yes          yes          no        yes
SNASw            yes          yes          no           no        yes
hseck9           yes          no           no           no        no
cme-srst         yes          yes          no           no        yes
WAAS_Express     yes          yes          no           no        yes
UCVideo          yes          yes          no           no        yes

R1# show version
Cisco IOS Software, C2900 Software (C2900-UNIVERSALK9-M), Version
15.1(4)M4, RELEASE SOFTWARE (fc1)

! Строки опущены для краткости

License UDI:
-------------------------------------------------
Device#    PID              SN
-------------------------------------------------
*0         CISCO2901/K9     FTX1628838P

Technology Package License Information for Module:'c2900'

-----------------------------------------------------------------
Tecnology    Technology-package       Technology-package
             Current      Type        Next reboot
-----------------------------------------------------------------
ipbase       ipbasek9     Permanent   ipbasek9
security     None         None        None
uc           None         None        None
data         None         None        None

Configuration register is 0x2102
```

Добавление лицензии на пакет технологий

Далее, в примере 21.4, показана установка на маршрутизаторе R1 лицензии для набора средств данных. Файл лицензий уже получен с регистрационного портала лицензий продуктов Cisco, помещен на носитель USB и включен в маршрутизатор R1. Таким образом, этапы 1–4, показанные на рис. 21.6 и 21.7, завершены.

Пример 21.4 демонстрирует заключительные этапы установки файла лицензии на маршрутизаторе R1. Здесь приведено содержимое носителя флеш для USB с выделенным файлом лицензии. Далее следует команда, изменяющая лицензии на маршрутизаторе.

Пример 21.4. Установка лицензии на маршрутизаторе Cisco

```
R1# dir usbflash1:
Directory of usbflash1:/
  1   -rw-    4096 Feb 11 2013 17:17:00 FTX1628838P_201302111432454180.lic

7783804928 bytes total (7782912000 bytes free)

R1# license install usbflash1:FTX1628838P_201302111432454180.lic

Installing...Feature:datak9...Successful:Supported
```

```
1/1 licenses were successfully installed
0/1 licenses were existing licenses
0/1 licenses were failed to install

R1#
Feb 11 22:35:20.786: %LICENSE-6-INSTALL: Feature datak9 1.0 was installed
in this device.
UDI=CISCO2901/K9:FTX1628838P; StoreIndex=1:Primary License Storage

Feb 11 22:35:21.038: %IOS_LICENSE_IMAGE_APPLICATION-6-LICENSE_LEVEL: Mod-
ule name = c2900 Next reboot level = datak9 and License = datak9
```

После команды `reload` (не представленной здесь) на маршрутизаторе будут поддерживаться средства набора данных. Пример 21.5 подтверждает изменение в состоянии лицензий — лицензия данных теперь отображается как активная.

Пример 21.5. Проверка установленной лицензии на маршрутизаторе

```
R1# show license
Index 1 Feature: ipbasek9
        Period left: Life time
        License Type: Permanent
        License State: Active, In Use
        License Count: Non-Counted
        License Priority: Medium
Index 2 Feature: securityk9
        Period left: Not Activated
        Period Used: 0 minute 0 second
        License Type: EvalRightToUse
        License State: Not in Use, EULA not accepted
        License Count: Non-Counted
        License Priority: None
Index 3 Feature: uck9
        Period left: Not Activated
        Period Used: 0 minute 0 second
        License Type: EvalRightToUse
        License State: Not in Use, EULA not accepted
        License Count: Non-Counted
        License Priority: None
Index 4 Feature: datak9
        Period left: Life time
        License Type: Permanent
        License State: Active, In Use
        License Count: Non-Counted
        License Priority: Medium
! Строки опущены для краткости
```

Установленную лицензию можно также проверить с помощью команды `show version`, как показано в примере 21.6.

Пример 21.6. Использование команды `show version` для проверки информации о лицензиях

```
R1# show version | begin Technology Package
Technology Package License Information for Module:'c2900'
```

```
-------------------------------------------------------------------
Tecnology    Technology-package        Technology-package
             Current      Type         Next reboot
-------------------------------------------------------------------
ipbase       ipbasek9     Permanent    ipbasek9
security     securityk9   None         None
uc           None         None         None
data         datak9       Permanent    datak9

Configuration register is 0x2102
```

Лицензии на право использования

Хотя в одних случаях стратегия лицензирования программного обеспечения для законных клиентов Cisco работает хорошо, в других случаях это может быть не так. Например, когда законный клиент Cisco хочет проверить средство маршрутизатора прежде, чем примет решение о покупке лицензии для всех своих маршрутизаторов, компания Cisco не желает, чтобы механизм лицензирования помешал этой продаже. Поэтому лицензирование Cisco достаточно гибко, чтобы позволить использование лицензии без покупки ключа PAK.

За прошедшие несколько лет компания Cisco внесла несколько изменений, позволив клиентам использовать средства без оплаты лицензии. Ныне большинство средств доступно для использования клиентом на протяжении 60-дневного пробного периода без платы за ключ PAK. А что потом? Средство остается разрешенным бессрочно. Лицензирующее программное обеспечение рассчитывает на честность пользователя и просит не злоупотреблять доверием.

ВНИМАНИЕ!

Со временем компания Cisco может изменить стратегию лицензирования программного обеспечения, чтобы поддержать правовой баланс.

Сегодня компания Cisco позволяет использовать эти средства без ключа PAK — достаточно *лицензии на право использования* (right-to-use license). Для ее использования следует ввести команду `license boot module` и перезагрузить маршрутизатор, чтобы позволить ему использовать новое средство. В примере 21.7 показано добавление набора средств защиты на маршрутизатор R1 с использованием пробной лицензии на право использования.

Пример 21.7. Активация лицензии на право использования

```
R1(config)# license boot module c2900 technology-package securityk9
PLEASE READ THE FOLLOWING TERMS CAREFULLY. INSTALLING THE LICENSE OR
LICENSE KEY PROVIDED FOR ANY CISCO PRODUCT FEATURE OR USING SUCH
PRODUCT FEATURE CONSTITUTES YOUR FULL ACCEPTANCE OF THE FOLLOWING
TERMS. YOU MUST NOT PROCEED FURTHER IF YOU ARE NOT WILLING TO BE BOUND
BY ALL THE TERMS SET FORTH HEREIN.

! Остальная часть EULA опущена …

Activation of the software command line interface will be evidence of
your acceptance of this agreement.
```

```
ACCEPT? [yes/no]: yes
% use 'write' command to make license boot config take effect on next
boot

Feb 12 01:35:45.060: %IOS_LICENSE_IMAGE_APPLICATION-6-LICENSE_LEVEL: Mod-
ule name = c2900 Next reboot level = securityk9 and License = securityk9
Feb 12 01:35:45.524: %LICENSE-6-EULA_ACCEPTED: EULA for feature securi-
tyk9 1.0 has been accepted. UDI=CISCO2901/K9:FTX1628838P; StoreIn-
dex=0:Built-In License Storage
R1(config)# ^Z
```

После перезагрузки маршрутизатора набор средств станет доступен и будет работать точно так же, как при покупке ключа PAK и загрузке файла лицензии с сервера Cisco.com. Пример 21.8 снова приводит вывод команды `show license`, демонстрируя различия результатов установки лицензии на право использования.

Пример 21.8. Результат активации лицензии на право использования

```
R1# show license
Index 1 Feature: ipbasek9
        Period left: Life time
        License Type: Permanent
        License State: Active, In Use
        License Count: Non-Counted
        License Priority: Medium
Index 2 Feature: securityk9
        Period left: 8 weeks 4 days
        Period Used: 0 minute 0 second
        License Type: EvalRightToUse
        License State: Active, In Use
        License Count: Non-Counted
        License Priority: Low
Index 3 Feature: uck9
        Period left: Not Activated
        Period Used: 0 minute 0 second
        License Type: EvalRightToUse
        License State: Not in Use, EULA not accepted
        License Count: Non-Counted
        License Priority: None
Index 4 Feature: datak9
        Period left: Life time
        License Type: Permanent
        License State: Active, In Use
        License Count: Non-Counted
        License Priority: Medium
! Строки опущены для краткости
```

В этом примере лицензии базовых IP и данных являются постоянными, а лицензия на право использования имеет только 60 дней в запасе (8 недель и 4 дня). Первые 60 дней считаются пробным периодом. Со временем вывод будет меняться, отсчитывая время назад до 0 дней, когда, согласно текущим правилам на момент публикации этой книги, наступает период постоянного существования.

Обзор

Резюме

- Ранее компания Cisco позволяла любому загрузить любой образ IOS для любого маршрутизатора Cisco.
- Разные модели маршрутизаторов зачастую использовали разные процессоры, поэтому компания Cisco компилировала различные образы IOS для использования на разных процессорах.
- Для идентификации главных номеров выпусков программного обеспечения Cisco IOS используется термин *версия*, а для меньших изменений — термин *выпуск*.
- Набор средств — это группа взаимосвязанных средств IOS.
- Компания Cisco использует пакет IOS с универсальным образом. Вместо старой модели одного образа с определенной комбинацией наборов средств компания Cisco выпускает один универсальный образ со всеми наборами средств.
- Раздел загрузки программного обеспечения на веб-сайте `Cisco.com` требует теперь ввода аутентификационной информации; в противном случае сайт загрузки Cisco пресечет попытку загрузки программного обеспечения.
- Клиенты Cisco могут заказать средства сразу при покупке маршрутизатора или добавить их позже. При заказе вместе с маршрутизатором компания Cisco установит лицензии на маршрутизатор еще на фабрике, и клиенту не придется заботиться об их добавлении. В качестве альтернативы клиент может купить лицензию для набора средств и позже, а затем, следуя процессу активации, разрешить этот набор средств на маршрутизаторе.
- Процесс активации вручную требует найти на веб-сайте `Cisco.com` портал Cisco Product License Registration Portal и ввести несколько команд в CLI маршрутизатора.
- За прошедшие несколько лет компания Cisco внесла несколько изменений, позволив клиентам использовать средства, не платя за лицензию. Ныне большинство средств доступно для использования клиентом на протяжении 60-дневного пробного периода без платы за ключ PAK.

Контрольные вопросы

Ответьте на эти вопросы. Ответы можно найти на последней странице главы. Полное объяснение ответов приведено в приложении B на веб-сайте.

1. Предположим, есть маршрутизатор Cisco модели X. Компания Cisco выпустила для этой модели программное обеспечение IOS таким образом, что клиент может заплатить за базовые средства и дополнительно за средства данных, голоса и защиты. Сколько образов IOS одной версии было бы доступно для этой моде-

ли X маршрутизатора при традиционном способе выпуска программного обеспечения Cisco IOS?

А) 1.

Б) 2.

В) 3.

Г) >3.

2. Как называется новый файл образа Cisco IOS, предоставляющий доступ ко всем основным средствам IOS?

А) Universal.

Б) Full.

В) Complete.

Г) Enhanced.

3. Как называется лицензия, разрешающая средства защиты на маршрутизаторе Cisco?

А) Security.

Б) VPN.

В) Securityk9.

Г) Encrypted.

4. Какая команда позволяет просмотреть идентификатор UDI маршрутизатора Cisco?

А) `show udi`.

Б) `show license udi`.

В) `show base udi`.

Г) `show udi base`.

5. В каком из следующих ответов приведена команда CLI на маршрутизаторе, применяемая при установке лицензии оплаченного пакета технологий для маршрутизатора 2901, использующего лицензированную операционную систему Cisco IOS и универсальный образ IOS?

А) `license boot module c2900 technology-package` *`пакет_технологий`*.

Б) `license boot module technology-package` *`пакет_технологий`* `install`.

В) `license install` *`url пакет_технологий`*.

Г) `license install` *`url`*.

6. В каком из следующих ответов приведена команда CLI на маршрутизаторе, используемая при установке лицензии на право использования для маршрутизатора 2901, использующего лицензированную операционную систему Cisco IOS и универсальный образ IOS?

А) `license boot module c2900 technology-package` *`пакет_технологий`*.

Б) `license boot module technology-package` *`пакет_технологий`* `install`.

В) `license install` *`url пакет_технологий`*.

Г) `license install` *`url`*.

Ключевые темы

Повторите все ключевые темы данной главы, отмеченные пиктограммой "Ключевая тема". Ключевые темы и соответствующие им страницы перечислены в табл. 21.2.

Таблица 21.2. Ключевые темы главы 21

Элемент	Описание	Страница
Рис. 21.3	Универсальный образ: один образ содержит все средства	663
Табл. 21.1	Некоторые из лицензий пакетов технологий	665
Рис. 21.6	Значения PAK и UDI для получения уникального файла ключа лицензии от Cisco.com	667

Заполните таблицы и списки по памяти

Распечатайте приложение Г с веб-сайта или его раздел, относящийся к этой главе, и заполните таблицы и списки по памяти. В приложении Д приведены заполненные таблицы и списки для самоконтроля.

Ключевые термины

После первого прочтения главы попытайтесь дать определения следующим ключевым терминам. Но не расстраивайтесь, если не все получится сразу, в главе 22 описано, как использовать эти термины на завершающем этапе подготовки к экзамену.

набор средств IOS (IOS feature set), универсальный образ (universal image), ключ активации продукта (Product Activation Key — PAK), универсальный идентификатор устройства (Universal Device Identifier — UDI)

Таблицы команд

Хоть и не обязательно заучивать информацию из таблиц данного раздела, ниже приведен список команд конфигурации и пользовательских команд главы. Фактически команды стоит запомнить, чтобы лучше понять содержимое главы и выполнить задания по подготовке к экзамену. Чтобы проверить, насколько хорошо вы запомнили команды, закройте левую сторону таблицы листом бумаги, читайте описания с правой стороны и пытайтесь вспомнить команду.

Таблица 21.3. Конфигурационные команды главы 21

Команда	Описание
`license boot module c2900 technology-package` *`имя_пакета`*	Глобальная команда, устанавливающая на маршрутизатор лицензию на право использования

Таблица 21.4. Команды EXEC главы 21

Команда	Описание
`show license`	Отображает группу строк для каждого средства в текущем образе IOS наряду с несколькими переменными состояния, связанными с программой активации и лицензирования
`show license feature`	Отображает по одной строке для каждого средства в текущем образе IOS наряду с несколькими переменными состояния, связанными с программой активации и лицензирования
`show license udi`	Отображает UDI маршрутизатора
`dir` *`файловая_система`*	Отображает файлы указанной файловой системы. Например, команда `dir usbflash1` выводит файлы в одном из слотов USB на маршрутизаторе 2901
`show version`	Отображает различную информацию о текущей версии IOS, включая подробности о лицензии в конце вывода команды
`license install` *`url`*	Устанавливает на маршрутизатор файл ключа лицензии

Ответы на контрольные вопросы:

1 Г. 2 А. 3 В. 4 Б. 5 Г. 6 А.

Обзор части VI

Проследите свой прогресс изучения материала части по контрольному списку в следующей таблице. Подробно задачи описаны ниже.

Контрольный список обзора части VI

Задача	Первая дата завершения	Вторая дата завершения
Повторите вопросы из обзоров глав		
Ответьте на вопросы обзора части		
Повторите ключевые темы		

Повторите вопросы из обзоров глав

Ответьте снова на вопросы обзоров глав этой части книги, используя программное обеспечение PCPT. Инструкция по запуску программного обеспечения PCPT с вопросами обзоров глав только этой части приведена в разделе "Как просмотреть вопросы только обзоров глав конкретной части" введения к книге.

Ответьте на вопросы обзора части

Ответьте на вопросы обзора этой части книги, используя программное обеспечение PCPT. Инструкция по запуску программного обеспечения PCPT с вопросами обзоров только этой части приведена в разделе "Как просмотреть вопросы только обзоров частей" введения к книге.

Повторите ключевые темы

Снова просмотрите темы прочитанных глав, отмеченные пиктограммой "Ключевая тема". Если понятны не все их подробности, уделите время повторному изучению

Часть VII. Подготовка к экзамену

Глава 22. “Подготовка к сертификационному экзамену”

Глава 22

Подготовка к сертификационному экзамену

Поздравляем! Вы сделали это: книга прочитана. Теперь пришло время заканчивать подготовку к экзамену. Эта глава поможет подготовиться и сдавать экзамен двумя способами.

Глава начинается с описания самого экзамена. Содержимое и темы уже известны. Теперь необходимо подумать, что будет во время экзамена и что необходимо сделать за несколько недель до его сдачи. На настоящий момент все, что вы делаете, должно быть сосредоточено на подготовке к сдаче, чтобы можно было закончить наконец это грандиозное предприятие.

Второй раздел этой главы дает некоторое представление об экзаменационных задачах и окончательной подготовке к экзаменам ICND1, ICND2 или CCNA.

Советы о самом экзамене

Завершив чтение этой книги, можно зарегистрироваться для сдачи экзамена Cisco ICND1, ICND2 или CCNA, придти и сдать экзамен. Но если уделить немного времени обдумыванию самого события экзамена, узнать чуть больше о пользовательском интерфейсе реальных экзаменов Cisco и окружении в сертификационных центрах, то подготовка будет гораздо лучше, особенно если это первый экзамен Cisco. Этот первый из трех главных разделов главы предоставляет несколько советов об экзаменах Cisco и самом событии экзамена.

Изучите типы вопросов, используя руководство по сертификационным экзаменам Cisco

За оставшиеся до экзамена недели стоит подумать о различных типах экзаменационных вопросов и выработать план ответа на них. Один из наилучших способов изучения экзаменационных вопросов — это воспользоваться руководством по сертификационным экзаменам Cisco (Cisco Exam Tutorial).

Руководство доступно на сайте `www.cisco.com` (достаточно поискать "exam tutorial"). На веб-странице руководства есть также сделанное во Flash представление пользовательского интерфейса экзамена, позволяющее попрактиковаться в сдаче экзамена. В пользовательском интерфейсе экзамена стоит опробовать следующее.

- Щелкните на кнопке Next (Далее) на вопросе с многовариантным выбором одного ответа, и вы убедитесь, что экзаменационное программное обеспечение укажет на слишком большое количество ответов.

- В вопросе с многовариантным выбором нескольких ответов выберите слишком мало ответов и, щелкнув на кнопке Next (Далее), посмотрите ответ пользовательского интерфейса.
- В вопросе с перетаскиванием перетащите ответы в некую область, а затем перетащите их назад в первоначальную область. (Это может произойти на реальном экзамене, если вы передумаете при ответе на вопрос.)
- В вопросе с имитацией (Simulation question) сначала удостоверьтесь, что можете получить доступ к интерфейсу командной строки (CLI) на одном из маршрутизаторов. Для этого следует щелкнуть на пиктограмме компьютера, подключенного к консоли маршрутизатора; консольный кабель представлен пунктирной линией, а сетевые кабели — сплошными линиями.
- В вопросе с имитацией удостоверьтесь также, что смотрите на область прокрутки вверху, а не сбоку, и видите окно эмулятора терминала.
- В вопросе с имитацией удостоверьтесь, что можете переключаться между окном топологии и окном эмулятора терминала щелчком на кнопках Show Topology (Показать топологию) и Hide Topology (Скрыть топологию).
- В тестлете (Testlet question) ответьте на один вопрос с многовариантным выбором, перейдите ко второму, ответьте на него, а затем вернитесь к первому вопросу, подтвердив, что в тестлете можно перемещаться между вопросами.
- Снова в тестлете щелкните на кнопке Next (Далее), чтобы появилось всплывающее окно, используемое Cisco для подтверждения перехода далее. Тестлеты фактически позволяют дать меньше ответов и все равно перейти далее. После щелчка для выхода из тестлета уже нельзя вернуться, чтобы изменить ответ на любой из этих вопросов.

Рассчитывайте время, чтобы успеть ответить на все вопросы

На экзамене необходимо следить за временем. Продвигаясь слишком медленно, можно упустить время и не успеть ответить на все вопросы. Слишком быстрое продвижение тоже вредно, поскольку, быстро отвечая на вопросы, легко не понять вопрос полностью или допустить ошибку. Поэтому необходимо знать, достаточно ли быстро идет процесс, чтобы ответить на все вопросы без спешки.

Пользовательский интерфейс экзамена демонстрирует немало полезной информации, в том числе таймер обратного отсчета и счетчик вопросов. Счетчик вопросов демонстрирует количество вопросов, на который даны ответы, а также все количество вопросов на экзамене.

К сожалению, все вопросы нельзя считать равными, поэтому это не дает точной оценки времени. Например, если экзамен занимает 90 минут и насчитывает 45 вопросов, то на каждый вопрос приходится по две минуты. Если ответ на 20 вопросов занял 40 минут, вполне можно уложиться в срок. Однако такую оценку затрудняет несколько факторов.

В первую очередь, корпорация Cisco не указывает заранее точного количества вопросов для каждого экзамена. Например, на веб-сайте Cisco экзамен CCNA может быть указан как насчитывающий от 45 до 55 вопросов. (У экзаменов ICND1 и ICND2 подобные диапазоны.) Но вы не узнаете, сколько вопросов будет на вашем

экзамене, пока он не начнется, точнее, пока вы не щелкнете на кнопке Start Exam (Начать экзамен).

Кроме того, некоторые вопросы (их называют *прожигателями времени* (time burners)) явно требуют много больше времени на ответ.

- **Вопросы нормального времени**. Вопрос с многовариантным выбором и перетаскиванием, приблизительно по минуте на каждый.
- **Прожигатели времени**. Симлеты и тестлеты, примерно по 6–8 минут каждый.

И наконец, при наличии 45–55 вопросов на одном экзамене тестлеты и симлеты могут содержать несколько вопросов с многовариантным выбором, а в счетчике вопросов они считаются как один вопрос. Например, если тестлет содержит четыре встроенных вопроса с многовариантным выбором, то счетчик вопросов покажет его как один вопрос.

ВНИМАНИЕ!

Хотя компания Cisco никак не объясняет, почему одним может достаться 45 вопросов, а другим 55 на том же экзамене, это, возможно, связано с тем, что в наборе из 45 вопросов могло бы быть больше прожигателей времени, делающих эти два набора эквивалентными.

Необходим план распределения времени, не отвлекающий от экзамена. Он мог бы включать примерно следующие предположения:

50 вопросов за 90 минут — это немного меньше, чем две минуты на вопрос, и на основании этого можно предположить, сколько вопросов прожигателей времени еще не встретилось.

Независимо от того, как планировалось распределить время, подумайте об этом перед экзаменом. Вполне можно использовать метод, приведенный в следующем разделе.

Предлагаемый метод распределения времени

Для распределения времени с учетом вероятного наличия прожигателей времени применим следующий метод. Вы не обязаны использовать его, но он прост, использует только целые числа и дает, по мнению автора, достаточно близкую оценку времени.

Концепция проста. Вот простое вычисление, позволяющее оценить использованное до сих пор время.

Количество пройденных вопросов + 7 на каждого прожигателя времени

Потраченное время покажет таймер, а на основании его значения можно выяснить следующее.

- Использовано именно столько времени или немного больше — хронометраж в порядке.
- Использовано меньше времени — вы опережаете график.
- Использовано заметно больше времени — вы отстаете от графика.

Например, если уже даны ответы на 17 вопросов, 2 из которых были прожигателями, оценка времени составит 17 + 7 + 7 = 31 минуту. Если ваше фактическое вре-

мя составляет 31 минуту или 32-33 минуты, то вы укладываетесь в расписание. Если же потрачено меньше 31-й минуты, вы опережаете график.

Математика довольно проста: пройденные вопросы плюс 7 на каждого прожигателя, и ощущение того, укладываетесь ли вы в срок.

ВНИМАНИЕ!

Этот метод приблизителен; автор не дает никаких гарантий, что этот подход даст точный прогноз на каждом экзамене.

Другие рекомендации

Вот еще несколько рекомендаций по подготовке к экзамену.

- Купите беруши. В некоторых сертификационных центрах они есть, но чтобы не рисковать, лучше быть подготовленным. Сертификационные центры, как правило, располагаются в помещениях неких компаний, где работают люди, или в учебных центрах. Поэтому в соседних помещениях есть говорящие люди и другой офисный шум. Беруши здесь будут весьма кстати. (Наушники, как электронные устройства, запрещены.)
- Некоторым нравится в первые минуты экзамена сделать несколько заметок для справки. Например, записать таблицу магических чисел для поиска идентификаторов подсети IPv4. Если вы планируете делать это, попрактикуйтесь в составлении таких заметок. Перед каждым тренировочным экзаменом практикуйтесь в создании таких заметок, точно так же, как собираетесь сделать это на реальном экзамене.
- Спланируйте свой визит в сертификационный центр с достаточным запасом времени, чтобы не спешить и сделать все вовремя.
- Если вы нервничаете перед экзаменами, применяйте свои любимые методики расслабления за несколько минут перед каждым тренировочным экзаменом, чтобы быть готовым использовать их.

Советы на день экзамена

Я надеюсь, экзамен пройдет успешно. Конечно, чем лучше готов, тем выше шансы преуспеть на экзамене. Но и эти небольшие советы помогут сосредоточить все усилия в день экзамена.

- Перед экзаменом лягте спать пораньше, не учите допоздна. Ясность мысли важней, чем один дополнительный факт, особенно потому, что экзамен требует больше анализа и размышлений, а не просто запоминания фактов.
- Если вы не принесли беруши, спросите их в сертификационном центре, даже если не предполагаете использовать их. Никогда не знаешь, что может пригодиться.
- Вы можете принести личные вещи в здание и помещение сертификационного центра, но не в то, где проходит сдача экзамена. Поэтому не берите с собой по возможности ничего лишнего. Если у вас есть безопасное место, чтобы оставить портфель, кошелек, электронные приборы и т.д., оставьте их там.

Но в сертификационном центре также должно быть место для хранения вещей. Короче говоря, чем меньше принесете, тем меньше придется волноваться о сохранности. (Автора, например, попросили снять даже механические наручные часы, причем не раз.)

- Сертификационный центр выдаст ламинированный лист и карандаш, чтобы делать заметки. (Персонал центра, как правило, не позволяет приносить бумагу и ручки в помещение, даже если они взяты в самом центре.)
- Отправляйтесь в сертификационный центр с запасом времени, чтобы не торопиться.
- Планируйте сходить в уборную перед визитом в сертификационный центр. Если не получится, то можно воспользоваться туалетом в сертификационном центре (персонал, конечно, поможет его найти и предоставит время перед началом экзамена).
- Не пейте литр сока перед визитом в сертификационный центр. После начала экзамена таймер не будет останавливаться, пока вы бегаете в уборную.
- В день экзамена используйте любые методики расслабления, которые практикуете, чтобы сосредоточиться, пока ожидаете сдачи экзамена.

Обзор экзамена

Этот обзор завершает материалы плана изучения, предложенного в данной книге. На настоящий момент уже прочитаны все главы и выполнены упражнения обзоров глав и частей. Теперь необходимо выполнить завершающие упражнения и действия, прежде чем переходить к сдаче экзамена, как описано в данном разделе.

В данном разделе предлагается несколько новых действий, а также повторяется несколько старых. Но и новые и старые действия сосредоточены на заполнении пробелов в знаниях и закреплении навыков, что завершает процесс изучения. Повторение некоторых задач из обзоров глав и частей поможет подготовиться к сдаче экзамена; таким образом, данный раздел требует уделить время ответам на экзаменационные вопросы.

Здесь рекомендуется несколько типов задач и предоставляется несколько таблиц для отслеживания каждого действия. Ниже приведены основные категории.

- Практика на скорость.
- Пробная сдача экзаменов.
- Поиск пробелов в знаниях (слабых мест).
- Настройка и проверка функций из CLI.
- Повторение задач из обзоров глав и частей.

Практика создания подсетей и другие навыки, связанные с математикой

Нравится вам это или нет, но некоторые из вопросов на экзаменах Cisco ICND1, ICND2 и CCNA требуют выполнения некоторых математических действий. Для сдачи следует знать математику, а также какой процесс и когда использовать.

Интересно, что экзамены ICND1 и ICND2 требуют знания математических механизмов, но компания Cisco поместила обучающий материал по этим навыкам в темы экзамена ICND1. В результате считается, что сдающий экзамен ICND2 уже обладает всеми этими навыками (и они действительно должны быть). В частности, в экзамен ICND2 входит много тем по поиску и устранению неисправностей, и почти все они требуют навыков математических вычислений по созданию подсетей.

Независимо от того, где и как вы изучали механизм создания подсетей, перед сдачей экзамена ICND2 или CCNA имеет смысл изучить математические концепции, изложенные в этой книге.

В табл. 22.1 приведен список тем этой главы, требующих как математических вычислений, так и скорости. В табл. 22.2 приведен список элементов, для которых математические вычисления или процессы более важны, чем скорость. На этом этапе обучения следует уже уверено находить правильный ответ на эти виды задач. Теперь самое время закрепить свои навыки в получении правильных ответов, чтобы сократить нехватку времени на экзаменах.

ВНИМАНИЕ!

Время на решение задач в таблице выбрано автором, чтобы дать общее представление. Если некоторые задачи выполняются немного медленнее, это вовсе не означает, что на экзамене будет провал. Но если почти каждая задача занимает в несколько раз больше времени, то проблемы со временем будут.

Таблица 22.1. Математические действия, требующие скорости вычисления

Глава	Действие	Отличная скорость (секунды)	Дата/время самопроверки	Дата/время самопроверки
12	Найти ключевые факты о классовой сети по одноадресатному IPv4-адресу	10		
13	Преобразование любой маски в одном формате в два других формата маски	10		
13	По IPv4-адресу и маске найти номер сети, биты подсети и хоста, а также количество подсетей и хостов в подсети	15		
14	По IPv4-адресу и маске найдите резидентскую подсеть, широковещательный адрес подсети и диапазон пригодных для использования адресов	20–30		
19	По набору требований к маске выберите наилучшую маску подсети	15		
19	По классовой сети и одной маске найдите все идентификаторы подсети	45		

Таблица 22.2. Математические действия, для которых скорость вычислений не столь важна

Глава	Действие	Дата/время самопроверки	Дата/время самопроверки
20	Найдите перекрытия VLSM, затрагивающие 5-6 подсетей		
20	Добавьте подсети VLSM, затрагивающие 5-6 подсетей		
21	Найдите наилучший суммарный маршрут, затрагивающий четыре маршрута		
22	Создайте команду ACL, соответствующую адресу подсети		
22	Перечислите адреса, соответствующие одной команде ACL		
25	Найдите наилучшее сокращение одного IPv6-адреса		
27	Найдите IPv6-адрес одного интерфейса маршрутизатора в формате EUI-64		

Практические задачи перечисленных в табл. 22.1 и 22.2 математических действий приведены в конце соответствующих глав. Например, для многих вопросов создания подсетей можно составить собственные задачи и проверить свою работу с любым калькулятором подсетей. Кроме того, для всех этих глав есть соответствующие приложения на веб-сайте с дополнительными практическими заданиями. И наконец, дополнительные практические задания можно найти в блоге автора.

Пробная сдача экзаменов

Поскольку однажды вам придется сдавать реальный экзамен Cisco в сертификационном центре, пришло время попрактиковаться в пробной сдаче с максимально возможным подобием.

Пробный экзамен использует программное обеспечение Pearson IT Certification Practice Test (PCPT), позволяющее опробовать большинство тех же задач реального экзамена Cisco. Это программное обеспечение задает вопросы, предоставляя в окне таймер обратного отсчета. После ответа на вопрос к нему больше нельзя вернуться (как и на экзаменах Cisco). Если время закончилось, вопросы без ответа будут считаться неправильными.

Процесс сдачи пробного экзамена на время поможет подготовиться в трех ключевых направлениях.

- Само событие пробного экзамена, включая нехватку времени, научит внимательно читать и сохранять концентрацию на протяжении длительного периода.
- Позволит выработать критически важные интеллектуальные навыки анализа и исследования сетевого сценария.
- Обнаружить пробелы в знаниях сети, чтобы можно было изучить эти темы перед реальным экзаменом.

В максимально возможной степени отработайте событие пробного экзамена, как будто сдаете реальный экзамен Cisco в сертификационном центре Vue. Ниже приве-

дено несколько советов, позволяющих сделать пробную сдачу экзамена более значащей, а не просто еще одним рутинным событием перед днем экзамена.

- Выделите два часа на сдачу 90-минутного пробного экзамена с ограничением по времени.
- Создайте список того, что предполагаете сделать на протяжении десяти минут перед реальным событием экзамена. Затем представьте себя выполняющим эти действия. Перед сдачей каждого пробного экзамена попрактикуйтесь в этих действиях. (См. предыдущий раздел "Советы на день экзамена", в котором приведены рекомендации о том, что делать в эти предшествующие десять минут.)
- В экзаменационное помещение ничего приносить нельзя, поэтому уберите все заметки и вспомогательные материалы с рабочего места перед пробной сдачей экзамена. Использовать можно только чистый лист бумаги, ручку и свои знания. Не используйте на своем компьютере ни калькулятор, ни блокнот, ни веб-браузеры, ни любые другие приложения.
- В реальной жизни вам могут мешать, но если это возможно, попросите окружающих оставить вас в покое на время сдачи пробного экзамена. Если все же придется сдавать пробный экзамен в шумной обстановке, наушники или беруши позволят снизить раздражающее воздействие.
- Не полагайтесь на удачу. Отвечайте только тогда, когда уверены. Если вопрос непонятен, к нему можно вернуться и обдумать впоследствии.

Пробная сдача экзамена ICND2

Поскольку вы читаете эту главу во втором томе, то, вероятней всего, готовитесь либо к экзамену ICND2, либо к экзамену CCNA. Экзаменационное программное обеспечение PCPT и предоставляемые вместе с книгой экзамены позволяют сдавать пробные экзамены и ICND2, и CCNA.

При сдаче пробного экзамена ICND2 необходимо выбрать один или несколько экзаменов ICND2 в программном обеспечении PCPT. Если вы следовали плану изучения этой книги, то еще не видели ни одного из вопросов в этих базах данных экзаменов. После выбора одного из этих экзаменов достаточно выбрать параметр Practice Exam (Пробный экзамен) вверху справа и запустить экзамен.

Пробные экзамены можно использовать несколькими способами. Если выбран одиночный пробный экзамен, то можно провести четыре пробных сдачи, не встретив повторяющихся вопросов. В этом случае можно выделить все четыре экзамена, и программное обеспечение PCPT случайно выберет комплект вопросов из всех четырех. При таком подходе можно сделать очень много попыток сдачи пробного экзамена, прежде чем вы начнете запоминать конкретные вопросы.

В табл. 22.3 приведен контрольный список для записи событий пробного экзамена. Обратите внимание, что примечания и дата в таблице кадров весьма полезны для некоторых других действий, поэтому заполняйте оба поля. Кроме того, в столбце примечаний, если задание выполнено раньше времени, отметьте количество оставшегося времени; если времени не хватило, отметьте количество вопросов, на которые не хватило времени.

Таблица 22.3. Контрольный список пробного экзамена ICND2

Экзамен	Дата	Результат	Примечания, время
ICND2			
ICND2			
ICND2			
ICND2			

Пробная сдача экзамена CCNA

Если решено сдать только экзамен CCNA, то и пробные экзамены нужно сдавать CCNA, а не ICND1 или ICND2. Комплект вопросов пробного экзамена CCNA используется пробными экзаменами ICND1 и ICND2, но лучше отвечать на те вопросы, которые будут на вашем экзамене.

И книга по ICND1, и книга по ICND2 предоставляет по четыре комплекта экзаменационных вопросов CCNA каждый. Если имеется только одна из этих двух книг, просто используйте четыре экзамена раздела "CCNA Full Exam" (Полный экзамен CCNA). Если есть обе книги, то имеется два комплекта по четыре экзамена CCNA, т.е. в общей сложности восемь индивидуальных экзаменов CCNA. На рис. 22.1 приведены названия и значение экзаменов в программном обеспечении PCPT.

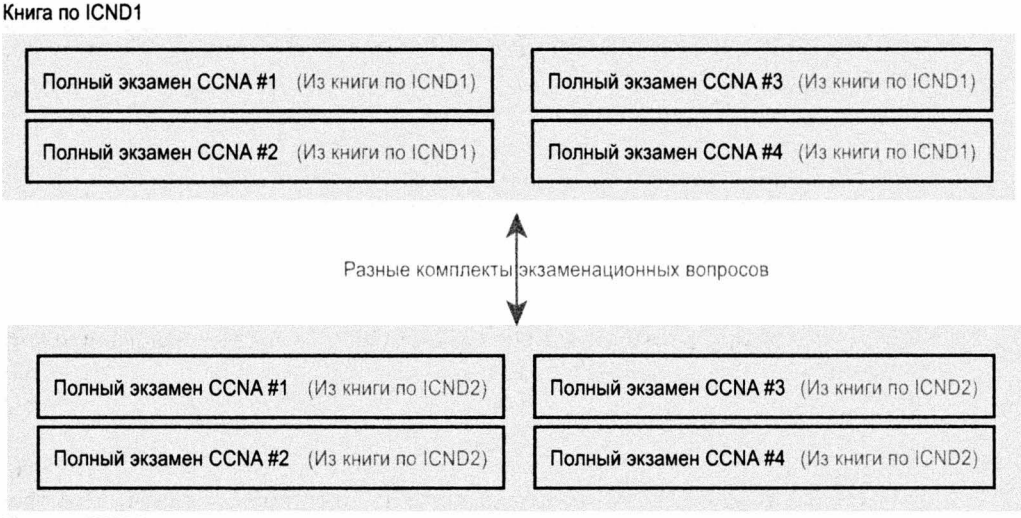


Рис. 22.1. Комплекты экзаменационных вопросов CCNA в книгах ICND1 и ICND2

Для сдачи экзамена CCNA выберите в окне PCPT одну из экзаменационных баз данных CCNA. Затем в разделе Practice Exam (Пробный экзамен) выберите параметр Mode (Режим) и запустите экзамен.

В табл. 22.4 приведен контрольный список для записи событий пробного экзамена. Обратите внимание, что примечания и дата в таблице кадров весьма полезны для некоторых других действий, поэтому заполняйте оба поля. Кроме того, в столбце примечаний, если задание выполнено раньше времени, отметьте количество

оставшегося времени; если времени не хватило, отметьте количество вопросов, на которые не хватило времени.

Таблица 22.4. Контрольный список пробного экзамена CCNA

Название экзаменационной базы данных	Дата	Результат	Примечания, время
Экзамен CCNA 1 (из книги по ICND1)			
Экзамен CCNA 2 (из книги по ICND1)			
Экзамен CCNA 3 (из книги по ICND1)			
Экзамен CCNA 4 (из книги по ICND1)			
Экзамен CCNA 1 (из книги по ICND2)			
Экзамен CCNA 2 (из книги по ICND2)			
Экзамен CCNA 3 (из книги по ICND2)			
Экзамен CCNA 4 (из книги по ICND2)			

ВНИМАНИЕ!

Программное обеспечение PCPT, прилагаемое к книге ICND2, содержит четыре экзаменационных базы данных: по две для ICND2 и по две для CCNA. Вопросы в этих базах частично совпадают с таковыми для экзаменов CCNA, поэтому имеет смысл сдавать либо пробные экзамены ICND2, либо пробные экзамены CCNA, в зависимости от того, к чему вы готовитесь, но не оба.

Как отвечать на экзаменационные вопросы

Откройте веб-браузер. Да, отдохните и откройте веб-браузер на любом устройстве. Найдите интересную тему. Затем, прежде чем щелкнуть на ссылке, проследите, куда устремятся ваши глаза в течение первых 5–10 секунд после щелчка на ссылке. Затем щелкните на ссылке и посмотрите на страницу. Куда вы смотрите?

Интересно, что дизайн веб-браузеров и содержимого веб-страниц приучили всех к определенному стилю просмотра. Дизайнеры веб-страниц разрабатывают содержимое с учетом того, что люди просматривают страницы по разным шаблонам. Независимо от шаблона чтения веб-страниц, почти никто не читает их последовательно и полностью. Сначала люди просматривают интересующие их рисунки и заголовки, а затем то, что находится вокруг этих элементов.

Остальные средства электронной культуры также повлияли на способ восприятия информации средним человеком. Например, большинство людей, пользуясь социальными сетями и средствами текстовых сообщений, привыкли отсеивать интересное из сотен или тысяч сообщений.

Эти каждодневные привычки повлияли на то, как все мы читаем и думаем перед экраном. К сожалению, те же привычки зачастую служат плохую службу при сдаче машинных экзаменов.

Если вы будете просматривать экзаменационные вопросы так же, как читаете веб-страницы, электронные письма и сообщения социальных сетей, то, вероятно, пропустите ключевой факт в вопросе, ответе или рисунке. Учитесь внимательно читать все слова с начала и до конца, что для многих людей стало на удивление противоестественным.

ВНИМАНИЕ!

Автор говорил со многими университетскими профессорами по разным дисциплинам и с преподавателями академии Cisco Networking Academy, и все они в один голос заявляли, что главной проблемой на экзаменах является то, что люди не читают вопросы достаточно внимательно, чтобы вникнуть в суть.

Позвольте автору дать две рекомендации о сдаче пробных экзаменов и ответе на отдельные вопросы. Во-первых, перед пробным экзаменом обдумайте собственную стратегию чтения вопросов. Выработайте собственный подход к вопросам, в особенности к вопросам с многовариантным выбором нескольких ответов. Во-вторых, если хотите несколько рекомендаций о чтении экзаменационного вопроса, используйте следующую стратегию.

Этап 1 Прочитайте вопрос полностью, от начала до конца

Этап 2 Просмотрите все дополнения (обычно вывод команды) и рисунки

Этап 3 Просмотрите ответы, чтобы понять тип информации. (Числа? Термины? Отдельные слова? Фразы?)

Этап 4 Еще раз перечитайте вопрос полностью, от начала до конца, чтобы удостовериться в его понимании

Этап 5 Прочитайте каждый ответ полностью, обращая внимание на рисунки, если они есть. После чтения каждого ответа, прежде чем приступить к чтению следующего ответа:
A. Если точно правильный, выберите его.
B. Если ответ наверняка неправилен, мысленно исключите его.
C. Если не уверены, мысленно отметьте ответ как возможно правильный.

ВНИМАНИЕ!

Количество правильных ответов на экзамене Cisco указано. Экзаменационное программное обеспечение также поможет закончить вопрос с правильным количеством ответов. Оно не позволит выбрать слишком много ответов. Кроме того, если попытаться перейти к следующему вопросу, выделив слишком мало ответов, экзаменационное программное обеспечение переспросит, действительно ли вы хотите перейти.

Используйте пробные экзамены, чтобы опробовать свой подход к чтению. Переходя к каждому следующему вопросу, попытайтесь читать его согласно выбранному подходу. Если чувствуете нехватку времени, то нужно продолжить практиковать свой подход, сокращая количество вопросов, пропущенных только из-за просмотра, а не полного чтения.

Обзор вопросов поможет найти пробелы в знаниях

Вы только что прошли несколько пробных экзаменов и вероятно многому научились, извлекли некоторую пользу для себя, приобрели навыки и улучшили знание сети. Но если вернуться и просмотреть все вопросы без правильных ответов, то можно обнаружить несколько небольших пробелов в знании.

Одной из труднейших задач при окончательной подготовке к экзамену является обнаружение пробелов в знаниях и навыках. Другими словами, необходимо узнать, какими темами и навыками вы владеете слабо. Или какие темы вы полагаете известными, но неправильно понимаете некоторые важные факты. Поиск пробелов

в знаниях на данном последнем рабочем этапе требует больше, чем просто знания своих сильных и слабых сторон.

Программное обеспечение PCPT поможет найти эти пробелы, оно отслеживает каждый сданный пробный экзамен, запоминая ответ на каждый вопрос и правильность ответа. Просматривая результаты, можно перемещаться между вопросами и просматривать страницы с результатами. Для поиска пробелов в своих знаниях следуйте таким этапам.

Этап 1 Выберите и просмотрите один из пробных экзаменов

Этап 2 Просматривайте все вопросы с неправильными ответами, пока не будете уверены, что правильно понимаете вопросы

Этап 3 Завершив обзор вопроса, отметьте его

Этап 4 Продолжайте обзор всех вопросов с неправильными ответами, пока все они не будут отмечены

Этап 5 Переходите к следующему пробному экзамену

На рис. 22.2 приведена типичная страница из обзора вопросов, все вопросы которой имеют неправильные ответы. Результаты приведены в столбце Correct (Правильно), отсутствие флажка означает неправильный ответ.

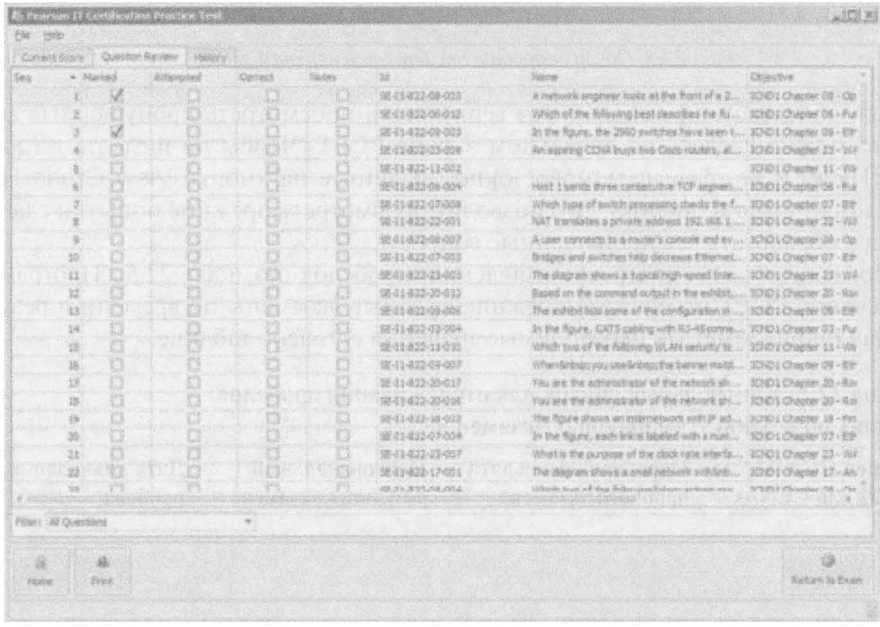


Рис. 22.2. Аттестационная страница PCPT с результатами

В процессе обзора вопросов и отметки их выполненными можно перемещаться между страницей обзора всех вопросов и индивидуальными вопросами. Достаточно дважды щелкнуть на вопросе, чтобы отобразить его. В окне вопроса можно щелкнуть на кнопке Grade Exam (Оценка экзамена), чтобы перейти к результатам аттестации на странице обзора вопросов, представленной на рис. 22.2. В окне вопроса (рис. 22.3) есть также возможность отметить вопрос (в верхнем левом углу) .

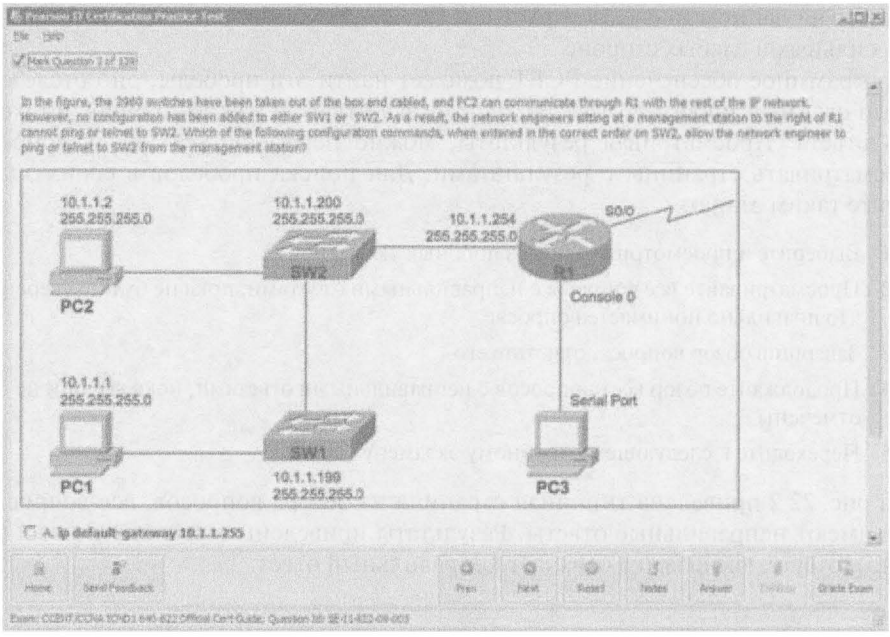


Рис. 22.3. Обзор вопроса с отметкой в верхнем левом углу

Если впоследствии понадобится вернуться и просмотреть пропущенные вопросы, это можно сделать на начальном экране PCPT. Чтобы не щелкать на кнопке Start (Пуск) и не открывать новое окно, щелкните на кнопке View Grade History (Просмотр истории оценок). Это позволит просмотреть прежние попытки сдачи экзамена и обработать все пропущенные вопросы.

Проследите свой прогресс выявления пробелов по табл. 22.5. Программное обеспечение PCPT отображает прежние пробные экзамены по времени и результату — так проще заметить необходимые значения согласно таблице.

Таблица 22.5. Контрольный список для отслеживания пробелов в знаниях по результатам пробных экзаменов

Экзамен (ICND1, ICND2 или CCNA)	Первоначальная дата пробного экзамена	Первоначальный результат экзамена	Дата ликвидации пробела

Практические навыки CLI

Для успешного ответа на вопросы с симлетами необходимы навыки работы с командами маршрутизаторов и коммутаторов Cisco, а также использования CLI Cisco. Как было сказано во введении к этой книге, вопросы симлетов требуют при-

нятия решения, какие команды конфигурации следует ввести, чтобы решить проблему или закончить рабочую конфигурацию. Симлеты требуют ответа на вопросы с множественным выбором, используя предварительно CLI для ввода команды `show`, позволяющей просмотреть состояние маршрутизаторов и коммутаторов в небольшой сети.

При подготовке к экзамену необходимо владеть следующими видами информации.

- **Навигация CLI**. Базовый механизм CLI перемещения между режимами пользователя, привилегированным режимом и режимом конфигурации.
- **Индивидуальная конфигурация**. Смысл параметров каждой команды конфигурации.
- **Конфигурация средства**. Набор команд конфигурации, обязательных и необязательных, для каждого средства.
- **Проверка конфигурации**. Команды `show`, непосредственно идентифицирующие параметры конфигурации.
- **Проверка состояния**. Команды `show`, выводящие текущее состояние.

Чтобы лучше запомнить и усвоить эти знания и навыки, можно выполнить задания, предложенные в нескольких следующих разделах.

Диаграммы связей из обзоров частей

В упражнениях обзоров частей вы создавали разные диаграммы связей и по конфигурации, и по командам проверки. Чтобы запомнить конкретные диаграммы связей, вернитесь к разделам обзоров каждой части.

Выполнение лабораторных работ

Независимо от выбранного метода приобретения практических навыков работы с CLI, уделите время обзору и выполнению лабораторных работ по командам. На настоящий момент вы имеете немного практических навыков ввода команд конфигурации, полученных при тренировке на эмуляторе, реальном механизме и даже на бумаге. Хотя повторение всех лабораторных работ могло бы быть и непрактично, тренировка с любыми командами и средствами, в которых вы чувствуете себя немного неуверенным, а также по темам из обзора диаграмм связей имела бы смысл. Контрольный список лабораторных работ приведен в табл. 22.6.

Наилучший способ приобретения практических навыков заключается в использовании эмулятора Pearson Network Simulator (или Sim) (см. `http://pearsonitcertification.com/networksimulator`).

В качестве бесплатной альтернативы можно выполнить на бумаге несколько коротких, на 5–10 минут, лабораторных работ по конфигурации, приведенных в блогах автора. Найдите их в разделе Config Museum блогов (один блог по ICND1, другой по ICND2) и выберите те лабораторные работы, которые хотите использовать. Можете попробовать выполнить их на бумаге или собственном средстве выполнения лабораторной работы. Начать поиск блогов можно по адресу `www.certskills.com/blogs`.

Таблица 22.6. Контрольный список лабораторных работ

Тема	Глава	Дата выполнения лабораторной работы
Протокол STP	2	
Сети VLAN	3	
Протоколы HSRP и GLBP	6	
Протокол OSPFv2 (для IPv4)	8	
Протокол EIGRP (для IPv4)	10	
Протоколы HDLC и PPP	12	
Стандарт Frame Relay	14	
Протокол OSPFv3 (для IPv6)	16	
Протокол EIGRPv6 (для IPv6)	17	
Протокол SNMP, системный журнал и NetFlow	19	
Лицензирование	21	

Другие учебные задачи

Если, дойдя до этого места, вы все еще чувствуете потребность в некой подготовке, то в этом последнем разделе предоставлены еще две рекомендации.

Во-первых, некоторые полезные задачи приведены в разделах обзоров глав и частей. Во-вторых, примите участие в обсуждениях учебной сети Cisco Learning Network. Попробуйте отвечать на вопросы, задаваемые другими участниками; процесс ответа заставляет обдумать тему намного глубже. Когда некто публикует ответ, с которым вы не согласны, обдумайте причину и выскажите свое мнение. Это отличный способ узнать больше и ощутить атмосферу доверия.

Заключительные соображения

Вы много учились, упорно трудились и потратили время и деньги на подготовку к экзамену. Надеюсь, экзамен пройдет успешно, поскольку вы действительно знаете материал и преуспеете в карьере сетевого специалиста.

Празднуйте успех и не расстраивайтесь в противном случае. Учебная сеть Cisco Learning Network является прекрасным местом, чтобы публиковать сообщения и просить советы на следующий раз. Автор лично хотел бы услышать о вашем успехе через Twitter (`@wendellodom`) или на его странице в Facebook (`http://facebook.com/wendellodom`). Желаю вам успеха и поздравляю с завершением работы над книгой!

Часть VIII. Приложения (в книге)

Приложение А. “Справочные числовые таблицы”

Приложение Б. “Обновление экзамена ICND2”

Список терминов

Справочные числовые таблицы

Это приложение содержит несколько полезных справочных таблиц, в которых приведены числа, используемые всюду в этой книге. Например, табл. А.1 полезна при преобразовании десятичных чисел в двоичные, и наоборот.

Таблица А.1. Десятичные и двоичные числа в диапазоне от 0 до 255

Десятичное число	Двоичное число	Десятичное число	Двоичное число	Десятичное число	Двоичное число	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. А.1

Десятичное число	Двоичное число	Десятичное число	Двоичное число	Десятичное число	Двоичное число	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. А.2 приведены шестнадцатеричные и двоичные числа. Она полезна при преобразовании шестнадцатеричных чисел в двоичные, и наоборот.

Таблица А.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. А.3 содержит степени числа 2, от 2^1 до 2^{32}.

Таблица А.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	1024	26	67 108 864
11	2048	27	134 217 728
12	4096	28	268 435 456
13	8192	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. А.4 приведены все 33 возможные маски подсетей, во всех трех форматах.

Таблица А.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

Обновление экзамена ICND2

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 объяснены трудные моменты каких-либо технологий и новых тем экзамена.

Данное приложение имеет версию 1.0 и не содержит никаких обновлений. Проверить модифицированную версию можно по адресу `http://www.ciscopress.com/title/9781587144882`.

Список терминов

3G/4G Интернет (3G/4G Internet). Технология доступа к Интернету, использующая беспроводную радиосвязь через вышки мобильных телефонов. Как правило, используется мобильными телефонами, планшетами и некоторыми другими устройствами мобильной связи.

Ethernet WAN. Любая служба WAN, использующая любой тип канала связи Ethernet как канал доступа между клиентом и службой WAN.

EUI-64. Буквально — *стандарт расширенного уникального идентификатора длиной 64 бита* (extended unique identifier that is 64 bits long). Специфический для протокола IPv6 набор правил формирования 64-битового идентификатора, используемого как идентификатор интерфейса в IPv6-адресах, начинающийся с 48-битового MAC-адреса, шестнадцатеричной части FFFE в середине и инвертированного седьмого бита.

Абонентское оконечное оборудование (Customer Premise Equipment — CPE). Телефонный термин, обозначающий оборудование, расположенное на территории клиента телефонной компании (площадке предприятия), но подключенное к службе WAN, предоставляемой телефонной компанией.

Автоматическая настройка адреса без фиксации состояния (Stateless Address Autoconfiguration — SLAAC). Функция протокола IPv6, позволяющая назначить одноадресатный адрес хосту или маршрутизатору без использования сервера DHCP с фиксацией состояния.

Автоматическое суммирование (autosummarization). Функция протоколов маршрутизации, позволяющая маршрутизатору, к которому подключены подсети из одной классовой сети, анонсировать суммарный маршрут только к полной классовой сети в обновлениях маршрутов.

Агент SNMP (SNMP agent). Агент простого протокола управления сетью располагается на управляемом устройстве. Это программное обеспечение обрабатывает сообщения SNMP, передаваемые *станцией управления сетью* (NMS).

Административное расстояние (administrative distance). Параметр, используемый маршрутизаторами компании Cisco для выбора маршрута, который будет установлен в таблицу маршрутизации. Каждому из протоколов маршрутизации присвоено свое значение административного расстояния. Чем меньше административное расстояние, тем более предпочтительным и доверительным является источник маршрутной информации.

Административный режим магистрали (trunking administrative mode). Параметр магистрального соединения на интерфейсе коммутатора Cisco, заданный командой `switchport mode`.

Активный виртуальный шлюз (Active Virtual Gateway — AVG). Совместно с протоколом балансировки нагрузки шлюза (GLBP), обеспечивающим ответы на запросы ARP у маршрутизатора виртуальных IP-адресов, выдает соответствующие виртуальные MAC-адреса, чтобы сбалансировать пользовательский трафик для каждого хоста.

Алгоритм выбора первого кратчайшего маршрута Дейкстры (Dijkstra Shortest Path First Algorithm — SPF). Алгоритм, используемый протоколами маршрутизации по

состоянию канала для анализа баз LSDB и поиска маршрутов наименьшей стоимости от маршрутизатора к каждой подсети.

Алгоритм поиска кратчайших маршрутов (Shortest Path First — SPF). Алгоритм, используемый протоколом OSPF, для поиска всех возможных маршрутов и последующего выбора маршрута с самой низкой метрикой для каждой подсети.

Алгоритм распределенных обновлений (Diffusing Update Algorithm — DUAL). Алгоритм сходимости, используемый в протоколе EIGRP. Обеспечивает отсутствие циклов на протяжении всего маршрута. Позволяет маршрутизаторам, задействованным в изменении топологии, одновременно выполнять синхронизацию, не затрагивая маршрутизаторы, на которые не повлияли изменения.

Анонс inter-area prefix LSA (inter-area prefix LSA). В OSPFv6 — тип анонса LSA, подобный анонсу summary LSA типа 3 в OSPFv2, создаваемый *граничным маршрутизатором области* (ABR), для описания префикса IPv6 одной области в базе данных другой области.

Анонс network LSA (network LSA). В OSPF — тип анонса LSA, создаваемого *выделенным маршрутизатором* (Designated Router — DR) сети (подсети), для которой DR помогает распространять анонсы LSA.

Анонс router LSA (router LSA). В OSPF — тип анонса LSA, создаваемый маршрутизатором для описания самого себя.

Анонс summary LSA (summary LSA). В OSPFv2 — тип анонса LSA, создаваемого *граничным маршрутизатором области* (ABR), для описания подсети одной области в базе данных другой области.

Анонс маршрутизатора (Router Advertisement — RA). Сообщение, определенное протоколом обнаружения соседних устройств (NDP) IPv6 и используемое маршрутизаторами для объявления об их готовности действовать как маршрутизатор IPv6 на канале связи. Сообщение может быть также послано в ответ на полученный ранее запрос информации о наличии маршрутизатора NDP (RS).

Анонс соседа (Neighbor Advertisement — NA). Сообщение, определенное протоколом обнаружения соседних устройств IPv6 (NDP) и используемое для объявления соседям MAC-адреса хоста. Иногда передается в ответ на полученное ранее сообщение запроса соседа NDP (NS).

Анонс состояния канала (Link-State Advertisement — LSA). Название структуры данных в протоколе OSPF, размещаемой в базе LSDB, в которой описаны детали разных компонентов сети, в том числе маршрутизаторов и каналов (подсетей).

Анонсируемое расстояние (reported distance). Метрика маршрута к какой-либо известной маршрутизатору подсети с точки зрения смежных устройств.

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.

Аутентификация (authentication). В технологиях безопасности — проверка идентификатора пользователя или процесса.

База данных состояний каналов (Link-State Database — LSDB). Структура данных в оперативной памяти маршрутизатора OSPF, в которой хранятся анонсы LSA, используемые для построения полной топологии сети.

База топологии (topology database). Специализированная структурированная база данных, в которой описана сетевая топология для протокола маршрутизации.

База управляющей информации (Management Information Base — MIB). Используемая протоколом SNMP стандартная структура базы данных, расположенная на управляемом устройстве и содержащая переменные, которые можно читать, а иногда и записывать при управлении устройством.

Балансировка нагрузки с неодинаковыми стоимостями (unequal-cost load balancing). Концепция протокола EIGRP, согласно которой маршрутизатор добавляет в таблицу маршрутизации маршруты с несколькими неодинаковыми стоимостями (разными метриками), позволяя в то же время использовать маршруты с одинаковыми метриками.

Бесклассовая адресация (classless addressing). Концепция IPv4-адресации, определяющая IP-адреса подсетей как состоящие из двух частей: префикса (или подсети) и хоста.

Бесклассовая маршрутизация (classless routing). Разновидность маршрутизации IPv4, в которой описано, как именно должны использоваться стандартный (default) маршрут и маршруты к сетям. Стандартный маршрут используется в том случае, когда сеть — получатель пакета не указан в таблице маршрутизации в явном виде.

Бесклассовый протокол маршрутизации (classless routing protocol). Более новый протокол маршрутизации, пересылающий в своих обновлениях таблиц маршрутизации адрес подсети и маску. Такой протокол маршрутизации не ориентирован на класс сети и поддерживает маски VLSM и суммирование маршрутов вручную.

Бесконечность (infinity). В контексте протокола IP маршрутизации некоторое значение, представляющее собой максимально возможную метрику маршрута для данного протокола, сигнализирующую о том, что маршрут не может быть использован.

Блокированный порт (disabled port). Порт, который с точки зрения протокола STP выключен, т.е. не находится в рабочем или подключенном состоянии (`up/up`).

Вариация (variance). Значение, умножаемое на наименьшую метрику одного из маршрутов к сети получателя. Если полученное число больше метрик остальных маршрутов, то такие маршруты будут установлены в таблицу маршрутизации и будет выполняться балансировка нагрузки по нескольким путям согласно метрикам этих маршрутов. Используется в протоколах EIGRP и IGRP, поскольку метрики маршрутов к одной и той же подсети редко бывают одинаковыми.

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 они 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 глобальная сеть Интернет. В сетях VPN пакеты шифруются, поэтому обеспечивается конфиденциальность передаваемых данных, а оконечные точки сети аутентифицируются, что обеспечивает их идентичность.

Виртуальный IP-адрес (virtual IP address). IP-адрес, используемый протоколом FHRP для нескольких маршрутизаторов, чтобы для хостов в этой подсети они выглядели как единый стандартный маршрутизатор.

Виртуальный MAC-адрес (virtual MAC address). MAC-адрес, используемый протоколом FHRP для получения фреймов от хостов.

Виртуальный канал (Virtual Circuit — VC). Логический канал, обеспечивающий надежное соединение между двумя сетевыми устройствами. Определяется парой VPI/VCI или идентификатором DLCI и может быть постоянным (permanent PVC) или коммутируемым (switched SVC). Виртуальные каналы применяются в сетях Frame Relay, X.25 и ATM.

Внеполосный (Out-Of-Band — OOB). Сетевой управляющий трафик зачастую передается как внеполосный. Это означает, что управляющий трафик не использует те же сетевые пути, что и трафик пользовательских данных.

Внутренний маршрутизатор (internal router). В OSPF — маршрутизатор со всеми интерфейсами в той же не опорной области.

Вторичный IP-адрес (secondary IP address). Дополнительный адрес (или адреса), настроенный на интерфейсе маршрутизатора с указанием ключа `secondary` в команде `ip address`.

Выделенный маршрутизатор (designated router). Побеждающий на выборах маршрутизатор OSPF в сети с множественным доступом, отвечающий за управление процессом обмена информацией по топологии OSPF между всеми подключенными к данной сети маршрутизаторами.

Выделенный порт (designated port). Один из интерфейсов коммутатора (или коммутаторов), подключенного к одному и тому же сегменту или домену коллизий в протоколах STP и RSTP, находящийся в режиме передачи фреймов. Порт коммутатора, анонсирующий сообщение BPDU с самым низким значением стоимости, становится выделенным.

Высокоуровневый протокол управления каналом (High-Level Data Link Control — HDLC). Бит-ориентированный синхронный протокол канального уровня, разработанный организацией ISO. Основан на протоколе SDLC и определяет метод инкапсуляции данных в синхронных последовательных каналах с помощью символов кадрирования и контрольных сумм.

Глобальный одноадресатный адрес (global unicast address). Разновидность одноадресатного IPv6-адреса, относящегося к диапазону открытых глобально уникальных IP-адресов, зарегистрированному в Ассоциации ICANN, ее региональных представительствах или у крупных провайдерах услуг Интернета.

Глобальный префикс маршрутизации (global routing prefix). Префикс IPv6, определяющий блок IPv6-адресов, состоящий из глобальных одноадресатных адресов, присвоенный одной организации, чтобы у нее был блок глобально уникальных IPv6-адресов для использования в собственной сети.

Граничный маршрутизатор автономной системы (Autonomous System Border Router — ASBR). Маршрутизатор OSPF, получающий маршруты из альтернативного источника, т.е. другого протокола маршрутизации, который является внешним по отношению к домену маршрутизации OSPF.

Граничный маршрутизатор зоны (Area Border Router — ABR). Маршрутизатор в протоколе OSPF, интерфейсы которого относятся к разным зонам.

Двойной стек (dual stack). Метод работы устройства в протоколе IPv6, когда на маршрутизаторе одновременно запущены протоколы IPv6 и IPv4.

Двусторонний канал (2-way state). В OSPF — состояние соседнего устройства, подразумевающее, что маршрутизатор обменялся сообщениями Hello с соседом и что все обязательные параметры совпали.

Деинкапсуляция (deencapsulation). Процесс на компьютере, получающем данные по сети, в ходе которого устройство интерпретирует, а по завершении удаляет заголовки нижнего уровня, открывая следующий, более высокий уровень PDU.

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 рассылал 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). Примерами протоколов этого класса являются RIP и IGRP.

Доступ по телефону (dial access). Общий термин, относящийся к любому виду коммутируемой службы WAN, использующей сеть телефонной компании, в которой перед началом передачи данных устройство должно установить соединение (эквивалент набора номера по телефону).

Дуплексная передача (full duplex). Возможность одновременной передачи данных между отправляющей и принимающей станциями в двух направлениях.

Единая точка отказа (single point of failure). Одиночное устройство в сети или на канале связи, отказ которого приведет к отключению данной совокупности пользователей.

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.

Задержка передачи (forward delay). Таймер протокола STP, равный 15 секундам, используемый для указания того, как долго интерфейс будет находиться в состоянии прослушивания (listening) или самообучения (learning).

Закрытый (частный) ключ (private key). Закрытый идентификатор в системах шифрования с парой "закрытый–открытый ключ". Используется для расшифровки данных, которые могут быть зашифрованы открытым ключом.

Запрет (deny). Правило в списке управления доступом (ACL), указывающее, что пакет должен быть отброшен.

Запрос на получение информации о наличии маршрутизатора (Router Solicitation — RS). Сообщение, определенное протоколом обнаружения соседних устройств (NDP) IPv6 и используемое для запроса любых маршрутизаторов канала связи об их идентификаторах и других параметрах конфигурации (префиксе и его длине).

Запрос соседа (Neighbor Solicitation — NS). Сообщение, определенное протоколом обнаружения соседних устройств IPv6 (NDP) и используемое для запроса у соседа ответного сообщения анонса соседа, содержащего его MAC-адрес.

Запрос состояния канала (link-state request). Пакет OSPF, используемый для отправки запроса соседнему маршрутизатору на получение определенного анонса LSA.

Идентификатор канального подключения (Data-Link Connection Identifier — DLCI). Значение, которое определяет канал PVC или SVC в сети Frame Relay. В базовой спецификации Frame Relay идентификаторы DLCI являются локальными (для указания одного и того же соединения подключенные устройства могут использовать разные значения).

Идентификатор маршрутизатора (Router ID — RID). 32-битовое число в протоколе OSPF, которое уникальным образом идентифицирует маршрутизатор.

Идентификатор моста (Bridge ID — BID). 8-байтовый идентификатор мостов и коммутаторов, используемый в протоколах STP и RSTP. Состоит из поля приоритета размером два байта и поля идентификатора системы (System ID) длиной шесть байтов, в качестве которого обычно используется MAC-адрес.

Идентификатор объекта (Object Identifier — OID). Используется для уникального описания переменной MIB в базе данных SNMP. Это строка чисел, уникально идентифицирующая переменную, а также описывающая положение переменной в древовидной структуре MIB.

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.

Интервал Dead (Dead interval). Таймер OSPF, используемый для каждого соседнего устройства. Маршрутизатор полагает, что сосед отключен, если он не получает от него никаких сообщений Hello за период времени, определенный этим таймером.

Интервал Hello (Hello interval). Таймер интерфейса в протоколах EIGRP и OSPF, указывающий, как часто маршрутизатор должен пересылать сообщения Hello.

Интерфейс базового уровня (Basic Rate Interface — BRI). Интерфейс сети ISDN, состоящий из двух каналов B и одного канала D в сети с коммутацией каналов для передачи голоса, видео и данных.

Интерфейс локального управления (Local Management Interface — LMI). Набор усовершенствований основной спецификации Frame Relay. Включает в себя механизм извещений об активности, который проверяет состояние канала передачи данных, механизм широковещательных рассылок, который позволяет работать с широковещательными интерфейсами DLCI, механизм глобальной адресации, который дает интерфейсам DLCI глобальное, а не локальное значение в сетях Frame Relay, а также механизм определения состояния виртуального канала, который предоставляет отчет о текущем состоянии известных коммутатору интерфейсов DLCI.

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 (T1) или 30 (E1) каналов B для передачи голоса либо данных.

Кабельный Интернет (cable Internet). Технология доступа к Интернету по телевизионному кабелю, обычно используемому для передачи видео.

Канал EtherChannel (EtherChannel). Созданная компанией Cisco Systems спецификация логического набора нескольких интерфейсов Ethernet, которые используются для образования единой конечной точки маршрутизации или организации мостового соединения с высокой пропускной способностью.

Канал доступа (access link). В технологии Frame Relay последовательный канал, соединяющий устройство DTE (обычно — маршрутизатор) с коммутатором Frame Relay. В каналах доступа используются те же стандарты физического уровня, что и в выделенных двухточечных каналах.

Канал связи WAN (WAN link). Другое название *выделенной линии* (leased line).

Классовая адресация (classful addressing). Концепция IPv4-адресации, предполагающая, что адрес состоит из трех частей: сети, подсети и хоста; всегда относится к какой-либо классовой сети.

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 VPN (VPN client). Программное обеспечение устанавливаемое на компьютерах и ноутбуках для подключения к дистанционным сетевым устройствам по технологии VPN.

Ключ активации продукта (Product Activation Key — PAK). Число, предоставляемое компанией Cisco в процессе лицензирования IOS. Оно дает клиенту Cisco право использовать набор функций IOS на одном из маршрутизаторов этого клиента определенной модели и серии (выбранный при покупке PAK).

Кодирование (encoding). Метод представления электрических или световых сигналов в линии, осуществляющий кодирование битов. Например, устройство может закодировать двоичную единицу и нуль сигналами с разной частотой.

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, на канальном уровне эталонной модели OSI.

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 технологической 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 друг с другом пакетами данных по одному разделяемому каналу связи.

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.

Корневая стоимость (root cost). Стоимость STP от некорневого коммутатора до корневого. Представляет собой сумму всех стоимостей STP для всех портов, которые фрейм прошел бы до достижения корневого коммутатора.

Корневой коммутатор (root switch). Устройство, которое выиграло выборы в локальной коммутируемой сети из-за того, что имеет наименьший идентификатор моста (Bridge ID). В протоколе STP периодически рассылает сообщения Hello BPDU (каждые 2 секунды).

Корневой мост (root bridge). То же самое, что корневой коммутатор.

Корневой порт (root port). Один из портов некорневого коммутатора, стоимость маршрута для которого к корневому коммутатору минимальна в протоколе STP. Должен находиться в режиме передачи (forwarding).

Линия T1 (T1). Линия от телефонной компании, допускающая передачу данных на скорости 1,544 Мбит/с, позволяющая организовать 24 отдельных канала DS0 по 64 Кбит/с (плюс дополнительный служебной канал на 8 Кбит/с).

Линия T3 (T3). Линия от телефонной компании, допускающая передачу данных на скорости 44,736 Мбит/с, позволяющая организовать 28 отдельных каналов DS1 (T1) по 1,544 Мбит/с (плюс дополнительный служебной канал).

Локализация проблемы (problem isolation). Этап процесса поиска и устранения неисправностей, на котором сетевой инженер пытается выделить основные причины отказа.

Локальное имя пользователя (local username). Имя пользователя (с паролем), заданное на маршрутизаторе или коммутаторе. Оно считается локальным, поскольку существует на маршрутизаторе или коммутаторе, а не на дистанционном сервере.

Магистральное соединение (trunking). Или магистральное соединение VLAN. Метод (использующий или протокол межсистемной связи Cisco, или протокол IEEE 802.1Q) поддержки нескольких VLAN, имеющих члены на нескольких коммутаторах.

Магистральный канал (trunk). Физическое и логическое соединение между двумя коммутаторами, по которому передается сетевой трафик. В современных коммутаторах используются магистральные соединения стандартов 802.1Q и ISL.

Максимальный блок передачи (Maximum Transmission Unit — MTU). Максимальный размер (в байтах) пакета данных, который можно передать через данный интерфейс.

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 частей сети и хоста в адресе подсети. Части сети адреса соответствуют двоичные единицы в маске, а части хоста — нули.

Маска подсети переменной длины (Variable-Length Subnet Mask — VLSM). Возможность задавать различные маски для одной и той же сети класса A, B или C в различных подсетях. Позволяет оптимизировать доступное адресное пространство.

Маски подсети постоянной длины (Static-Length Subnet Mask — SLSM). Дизайн сети, в котором одна и та же маска используется для разделения классовой сети A, B или C на подсети.

Мгновенное обновление (triggered update). Обновление маршрутов, создаваемое в ответ на изменение топологии сети и отправляемое сразу же, а не по истечении какого-либо времени.

Межкоммутаторный канал (Inter-Switch Link — ISL). Собственный протокол компании Cisco, сохраняющий информацию виртуальной LAN при обмене трафиком между коммутаторами и маршрутизаторами.

Межсетевая операционная система (Internetwork Operating System — IOS). Программное обеспечение операционной системы Cisco, поддерживающее большинство функциональных возможностей маршрутизатора или коммутатора, а остальное обеспечивают сами аппаратные средства.

Метрика (metric). Числовое значение, вырабатываемое каким-либо алгоритмом для каждого маршрута в сети. Обычно чем меньше метрика, тем предпочтительнее маршрут.

Многообластной (multi-area). Проект OSPFv2 и OSPFv3, использующий несколько областей.

Модем (modem). *Мо*дулятор-*дем*одулятор. Устройство, преобразующее цифровой сигнал в аналоговый, и наоборот, чтобы компьютер мог отправлять данные другому компьютеру по аналоговой телефонной линии. На стороне отправителя модем преобразует цифровые сигналы в форму, подходящую для передачи по аналоговым линиям связи. На стороне получателя аналоговые сигналы снова преобразуются в цифровую форму.

Модем DSL (DSL modem). Устройство, подключенное к телефонной линии и использующее стандарты DSL для передачи и получения данных через телефонную компанию.

Модуль данных протокола моста (Bridge Protocol Data Unit — BPDU). Служебное сообщение протокола распределенного связующего дерева (Spanning-Tree Protocol), которое посылается через заданные интервалы для обмена информацией между мостами и коммутаторами сети.

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.

Монитор ROM (ROM Monitor — ROMMON). Низкоуровневая операционной система, допускающая загрузку на маршрутизаторы Cisco для выполнения некоторых редко необходимых задач обслуживания, включая восстановление пароля и загрузку новый операционной системы IOS, после отказа флеш-памяти.

Мультипротокольная коммутация по меткам (Multiprotocol Label Switching — MPLS). Метод перенаправления пакетов на основании маркеров, а не заголовков IP. Может быть объединена с другими средствами провайдера служб для оказания клиентам услуг WAN.

Набор средств IOS (IOS feature set). Набор взаимосвязанных средств, которые можно разрешить на маршрутизаторе для выполнения определенных функций. Например, набор средств безопасности позволяет маршрутизатору выступать в роли сетевого брандмауэра.

Направленный широковещательный адрес (directed broadcast address). Широковещательный адрес подсети.

Не широковещательный множественный доступ (Nonbroadcast Multiaccess — NBMA). Определенный тип сети уровня 2, в которой к сети подключено больше двух устройств, но они не могут обмениваться широковещательными фреймами.

Неполносвязная топология (partial-mesh topology). Топология сети, в которой 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.

Неправильное сообщение Hello (inferior Hello). Сообщение, содержащее больший в числовом выражении идентификатор корневого моста, чем у локального устройства, или сообщение Hello, в котором указан тот же идентификатор корневого моста, но с большей стоимостью.

Несмежная сеть (discontiguous network). Вариант дизайна сети IPv4, в котором подсети одной и той же классовой сети разделены подсетью другой классовой сети.

Номер автономной системы (Autonomous System Number — ASN). Номера, используемые протоколом BGP для идентификации домена маршрутизации, зачастую единого предприятия или организации. В контексте этой книги, при использовании с протоколом EIGRP, это номера, идентифицирующие процессы маршрутизации на маршрутизаторах, желающих обмениваться информацией о маршрутизации EIGRP друг с другом.

Нулевая подсеть (zero subnet). Подсеть в классовой сети IPv4, в части подсети адреса которой стоят двоичные нули. В десятичном виде нулевая подсеть может быть легко идентифицирована, поскольку ее адрес совпадает с адресом сети.

Обновление состояния канала (link-state update). Пакет OSPF, используемый для передачи анонса LSA соседнему маршрутизатору.

Обобщенная маршрутная инкапсуляция (Generic Routing Encapsulation — GRE). Определенный документом RFC 2784 протокол, определяющий заголовки, используемые при создании туннеля VPN между сетевыми площадками. Протокол определяет использование обычного заголовка IP, называемого *заголовком передачи* (delivery header), и заголовка GRE, используемых конечными точками для создания и управления трафиком по туннелю GRE.

Образ IOS (IOS image). Файл, содержащий операционную систему IOS.

Обратный маршрут (reverse route). С точки зрения хоста маршрут, по которому к нему пересылаются пакеты от дистанционного устройства.

Оконечное оборудование канала передачи данных (Data Circuit-terminating Equipment — DCE). Устройство, используемое для конвертирования данных поль-

зователя из цифрового формата DTE в форму, приемлемую для оборудования служб распределенной сети.

Оперативная память (Random-Access Memory — RAM). Тип энергозависимой памяти для чтения и записи микропроцессором.

Опорная область (backbone area). В протоколах OSPFv2 и OSPFv3 специальная область в проекте с несколькими областями, со всеми не опорными областями, нуждающимися в подключении к опорной области, область 0.

Оптимальное расстояние (Feasible Distance — FD). Метрика наилучшего маршрута к подсети.

Оптимальный маршрут (successor). Наилучший маршрут (с наименьшей метрикой) в протоколе EIGRP, который устанавливается в таблицу маршрутизации.

Открытый ключ (public key). Открытый идентификатор в системах шифрования с парой "закрытый–открытый ключ". Используется для шифрования данных, которые могут быть зашифрованы закрытым ключом.

Открытый протокол поиска первого кратчайшего маршрута (Open Shortest Path First — OSPF). Популярный протокол внутреннего шлюза, в котором используются база данных состояния каналов и алгоритм *первого кратчайшего маршрута* (Shortest Path First — SPF) для расчета оптимальных маршрутов к подсетям.

Очень маленький спутниковый терминал (Very Small Aperture Terminal — VSAT). Термин, описывающий оба типа WAN, использующих спутники и тип очень маленькой спутниковой антенны, обычно используемой для обмена данными через спутник.

Пакет описания базы данных (database description). Специализированный пакет OSPF, в котором содержатся краткие описания анонсов LSA базы LSDB.

Передача (forward). Процесс доставки фрейма к получателю с помощью маршрутизирующего устройства.

Передача голоса по сети IP (Voice over IP — VoIP). Передача, позволяющая 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.

Перекрывающиеся подсети (overlapping subnets). Результат неправильного дизайна подсетей IP, когда диапазон адресов одной подсети перекрывается диапазоном другой.

Периодическое обновление маршрутов (periodic update). Обновление, рассылаемое протоколами маршрутизации через равные интервалы времени. Характерны для дистанционно-векторных протоколов маршрутизации.

Подсеть (subnet). Некоторая часть сети класса A, B или C, выделенная сетевым инженером. С помощью подсетей можно сэкономить адресное пространство и создать группы IP-адресов.

Поле типа протокола (protocol type field). Поле в заголовке фрейма 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.

Полная синхронизация (full state). Состояние соседнего маршрутизатора в протоколе OSPF, когда два устройства полностью закончили обмен своими базами LSDB.

Полное обновление маршрутов (full update). Вариант обновления маршрутов в протоколах маршрутизации, в котором перечислены все известные устройству маршруты.

Полностью смежный (fully adjacent). В OSPF — характеристика состояния соседа, при котором два соседа достигли полной синхронизации.

Порт (port). В терминологии IP процесс верхнего уровня, который принимает данные от нижних уровней. Представляет собой поле в заголовке TCP или UDP, идентифицирующее приложение, которое пересылает (порт отправителя) или принимает (порт получателя) поток сегментов данных. В коммутируемых локальных сетях портом называют интерфейс коммутатора.

Последовательный кабель (serial cable). Тип кабеля со многими разными видами разъемов, обычно соединяющий маршрутизатор с внешним модулем CSU/DSU на выделенной линии.

Последовательный канал (serial link). Другое название *выделенной линии* (leased line).

Постоянное запоминающее устройство (Read-only memory — ROM). Тип энергонезависимой памяти для чтения и записи микропроцессором.

Постоянный виртуальный канал (Permanent Virtual Circuit — PVC). Постоянно действующий виртуальный канал между устройством DTE сети Frame Relay, идентифицируемый значением DLCI в канале доступа к провайдеру услуги. Каналы PVC экономят полосу пропускания, необходимую для установки и разрыва соединения, если виртуальный канал должен существовать постоянно. Постоянные виртуальные каналы являются логическим аналогом физического выделенного канала.

Префикс подсети (subnet prefix). Префикс, назначенный каждому из каналов в технологии IPv6. Является аналогом подсети в протоколе IPv4.

Префикс провайдера (ISP prefix). Префикс, описывающий блок адресов, присвоенный какому-либо провайдеру одним из регистраторов IP-адресов технологии IPv6.

Префикс регистратора (registry prefix). Префикс IPv6, описывающий блок открытых глобально уникальных адресов в протоколе IP версии 6, выделенный региональному регистратору Интернета Ассоциацией ICANN.

Префикс сайта (site prefix). Префикс, описывающий открытый глобально уникальный блок IPv6-адресов, который был присвоен какой-либо организации, например компании, предприятию или государственному учреждению. Такой блок обычно присваивается специализированным регистратором Интернета или провайдером.

Префиксная запись (prefix notation). Краткий формат записи маски подсети, в котором указывается только количество единичных битов в маске после косой черты. Например, /24 описывает маску с 24 единичными битами, т.е. маску сети класса C. Зачастую количество единичных битов в маске сети называют длиной префикса.

Привилегированный 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 конфигурировать устройство.

Привязка адреса в технологии Frame Relay (Frame Relay mapping). Информация, связывающая локальный идентификатор DLCI с адресом уровня 3 на другом конце виртуального канала.

Приложение Cisco Prime. Обладающее графическим интерфейсом пользователя (GUI) программное обеспечение управления устройствами сети Cisco, использующее протокол SNMP. Термин *Cisco Prime* — это общее название набора разнообразных индивидуальных программных продуктов.

Простейший протокол передачи файлов (Trivial File Transfer Protocol — TFTP). Упрощенная версия протокола FTP, позволяющая компьютерам обмениваться файлами по сети и использующая в качестве транспортного механизма дейтаграммы.

Простой протокол управления сетью (Simple Network Management Protocol — SNMP). Стандартный для Интернета протокол управления устройствами в сетях IP. К поддерживающим протокол SNMP устройствам обычно относятся маршрутизаторы, коммутаторы и серверы. Главным образом он используется в системах управления сетью для контроля сетевых устройств, требующих административного внимания. Как определено Инженерной группой по развитию Интернета (IETF), протокол SNMP входит в *комплект протоколов Интернета* (Internet Protocol Suite), состоящий из набора стандартов для управления сетью, включая протокол уровня приложений, схему базы данных и ряда объектов данных.

Протокол EIGRP для IPv6 (EIGRP for IPv6 — EIGRPv6). Версия протокола EIGRP, поддерживающая анонсы маршрутов для префиксов IPv6, а не подсетей IPv4.

Протокол NetFlow (NetFlow). Позволяет осуществлять мониторинг трафика IP в сети. Эту информацию можно использовать для расчетов, оповещения, планирования пропускной способности, защиты и общего мониторинга дистанционный сети.

Протокол PPPoE (PPP over Ethernet — *PPP по Ethernet*). Протокол, специально разработанный для инкапсуляции фреймов PPP во фреймах Ethernet с целью передачи фреймов PPP между двумя устройствами. Это фактически создает туннель с двухточечным соединением между двумя этими устройствами.

Протокол аутентификации по паролю (Password Authentication Protocol — PAP). Механизм аутентификации в протоколе PPP, в котором используется двухэтапный процесс проверки идентичности устройств и пароль передается в незашифрованном виде.

Протокол аутентификации с предварительным согласованием вызова (Challenge Handshake Authentication Protocol — CHAP). Протокол, предназначенный для обеспечения безопасности в линиях с инкапсуляцией PPP, которая предотвращает несанкционированный доступ в ходе идентификации дистанционного хоста. Затем маршрутизатор или сервер доступа определяет полномочия доступа данного пользователя.

Протокол балансировки нагрузки шлюза (Gateway Load Balancing Protocol — GLBP). Собственный протокол Cisco, позволяющий двум (или более) маршрутизаторам совместно использовать режимы стандартного маршрутизатора подсети и модели активной/активной, со всеми маршрутизаторами, активно перенаправляющими трафик вне подсетей для некоторых из их хостов.

Протокол двухточечного соединения (Point-to-Point Protocol — PPP). Преемник протокола SLIP, обеспечивающий соединения "маршрутизатор–маршрутизатор" и "хост–сеть" по синхронным и асинхронным каналам. Протокол SLIP был разработан для работы с протоколом IP, но протокол PPP может работать с несколькими протоколами сетевого уровня, такими как IP, IPX и ARA.

Протокол защищенных сокетов (Secure Socket Layer — SSL). Протокол, используемый в средствах безопасности. Интегрирован в наиболее распространенные веб-

браузеры и обеспечивает функции шифрования и аутентификации для браузера и веб-сайта.

Протокол маршрутизации (routing protocol). Протокол, осуществляющий реализацию какого-либо алгоритма маршрутизации. Примерами протоколов маршрутизации могут служить протоколы IGRP, OSPF и RIP.

Протокол маршрутизации внутреннего шлюза (Interior Gateway Protocol — IGP). Протокол, использующийся для обмена маршрутной информацией в автономных системах. Примерами широко используемых протоколов класса IGP являются IGRP, OSPF и RIP.

Протокол маршрутизации внутреннего шлюза (Interior Gateway Routing Protocol — IGRP). Устаревший, более не поддерживаемый протокол внутреннего шлюза (Interior Gateway Protocol — IGP) компании Cisco.

Протокол маршрутной информации (Routing Information Protocol — RIP). Протокол типа IGP, поставлявшийся с системами BSD UNIX. Самый 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 обнаружения соседних устройств (Neighbor Discovery Protocol — NDP). Часть стека протоколов IPv6, используемая для обнаружения соседних устройств и обмена информацией о них в той же подсети. Заменяет протокол ARP технологии IPv4.

Протокол обратного преобразования адресов (Inverse Address Resolution Protocol — Inverse ARP). Метод создания динамических маршрутов в сети. Позволяет серверу обнаружить сетевой адрес устройства, связанного с виртуальным каналом.

Протокол передачи файлов (File Transfer Protocol — FTP). Протокол уровня приложений, который является частью стека протоколов TCP/IP и предназначен для передачи файлов между сетевыми хостами. Описан в документе RFC 959.

Протокол преобразования адресов (Address Resolution Protocol — ARP). Интернет-протокол, используемый для определения привязки IP-адреса к MAC-адресу. Описан в документе RFC 826.

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 за счет отключения отдельных интерфейсов.

Протокол резервирования виртуального маршрутизатора (Virtual Router Redundancy Protocol — VRRP). Протокол стека TCP/IP, позволяющий двум (или более) маршрутизаторам совместно работать как стандартный маршрутизатор подсети в модели активный/резервный при одном маршрутизаторе, действующим как стандартный маршрутизатор, и другом, ожидающим на случай, если откажет первый.

Протокол резервирования первого транзитного участка (First Hop Redundancy Protocol — FHRP). Класс протоколов, включающий протоколы HSRP, VRRP и GLBP, позволяющий нескольким избыточным маршрутизаторам в той же подсети действовать как единый стандартный маршрутизатор (маршрутизатор первого транзитного участка).

Протокол резервного маршрутизатора (Hot Standby Router Protocol — HSRP). Собственный протокол компании Cisco, позволяющий двум (или более) маршрутизаторам совместно работать как стандартный маршрутизатор подсети в модели активный/активный, при одном маршрутизаторе, действующим как стандартный маршрутизатор, и другом, ожидающим на случай, если откажет первый.

Протокол создания магистралей VLAN (VLAN Trunking Protocol — VTP). Собственный протокол компании Cisco, используемый для обмена сообщениями коммутаторов компании Cisco, содержащих информацию о том, какие сети VLAN есть в устройствах и каковы их идентификаторы и имена.

Протокол управления IP (IP Control Protocol — IPCP). Протокол, обеспечивающий включение и выключение, а также конфигурирование протокола IP для канала с двухточечным соединением PPP.

Процедура доступа к каналу для служб передачи фреймов (Link Access Procedure Frame Bearer Services — LAPF). Стандарт, согласно которому формируются заголовок и концевик Frame Relay. Согласно стандарту в заголовке содержатся идентификатор DLCI, биты FECN, BECN и DE.

Прямой маршрут (forward route). С точки зрения какого-либо хоста маршрут, по которому данный хост пересылает пакеты дистанционному устройству.

Рабочий режим магистрали (trunking operational mode). Текущее поведение интерфейса коммутатора Cisco для магистрального соединения VLAN.

Разделение диапазона (split horizon). Технология, используемая в дистанционно-векторных протоколах маршрутизации для предотвращения кольцевых маршрутов. Принцип ее работы заключается в том, что если какая-либо подсеть присутствует в анонсе от смежного маршрутизатора, то в обратном направлении смежному устройству информация о такой подсети не пересылается.

Разрешение (permit). Правило списка управления доступом (ACL), гласящее, что пакет с указанными параметрами должен быть передан дальше маршрутизатором.

Расширенный вариант команды `ping` (extended ping). Вариант команды, в котором можно задать множество параметров, а не только IP-адрес получателя.

Расширенный протокол маршрутизации внутреннего шлюза (Enhanced Interior Gateway Routing Protocol — EIGRP). Обновленная версия протокола IGRP, разработанная компанией Cisco. Для этого протокола характерна очень быстрая конвергенция, высокая эффективность и экономия полосы пропускания сети. Сочетает в себе самые лучшие функции дистанционно-векторных протоколов и протоколов с учетом состояния каналов.

Расширенный список управления доступом (extended access list). Набор команд `access-list` в глобальной конфигурации системы IOS, при помощи которого проверяются различные характеристики пакета IP, например, IP-адрес отправителя и получателя, а также порты TCP и UDP, чтобы принять решение о том, следует ли такой пакет отбросить или передать дальше.

Региональный реестр Интернета (Regional Internet Registry — RIR). Одна из пяти организаций, распределяющих глобально уникальные открытые адреса в адресных пространствах протоколов IPv4 и IPv6.

Режим начальной конфигурации (setup mode). Средство операционной системы Cisco IOS коммутаторов и маршрутизаторов, запрашивающее у пользователя ин-

формацию о базовой конфигурации при создании новых файлов `running-config` и `startup-config`.

Резервный выделенный маршрутизатор (backup designated router). Маршрутизатор OSPF в многостанционной сети, отслеживающий работоспособность *выделенного маршрутизатора* (Designated Router — DR) и перехватывающий его роль в случае отказа устройства DR.

Самообучение (learn). Процесс, в ходе которого прозрачные мосты и коммутаторы обнаруживают MAC-адреса, инспектируя поле адреса отправителя во фреймах, и каждый новый MAC-адрес, а также номер порта, через который он был получен, заносится в таблицу коммутации.

Сбалансированный гибридный класс (balanced hybrid). Термин, описывающий комбинацию средств дистанционно-векторных протоколов маршрутизации и протоколов маршрутизации по состоянию канала, реализованных протоколом EIGRP.

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*.

Сервер DHCP без фиксации состояния (stateless DHCP). Термин из технологии IPv6, описывающий ситуацию, когда сервер не выдает адреса клиентским устройствам, а поставляет вспомогательную информацию, например IP-адрес сервера DNS, и не отслеживает информацию о клиентах.

Сервер DHCP с фиксацией состояния (stateful DHCP). Термин из технологии IPv6, описывающий ситуацию, когда сервер отслеживает, каким именно клиентским устройствам какие IP-адреса были выданы.

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.

Системный журнал (syslog). Сервер системного журнала получает системные сообщения от сетевых устройств и сохраняет их в базе данных. Сервер системного журнала позволяет также составлять отчеты об этих системных сообщениях. Некоторые способны даже отвечать на системные сообщения select определенными действиями, такими как сообщение на электронную почту или пейджер.

Скорость доступа (Access Rate — AR). Скорость передачи битов через канал связи Frame Relay.

Служба BPDU Guard. Специализированная служба коммутаторов локальных сетей компании Cisco, прослушивающая входящие сообщения BPDU протокола STP и выключающая пользовательский интерфейс, если через него получено такое сообщение. Основная функция этой службы — предотвращение кольцевых маршрутов в ситуации, когда к порту коммутатора подключается другой коммутатор вместо пользовательской станции.

Смежная сеть (contiguous network). В IPv4-адресации сеть, в которой при пересылке пакетов между двумя любыми подсетями классовой сети данные передаются только через смежные сети, относящиеся к той же классовой сети.

Совместно используемый ключ (shared key). Ключ для шифрования, известный как отправителю, так и получателю.

Сообщение GET (GET message). Сообщение, используемое протоколом SNMP для чтения переменных в MIB.

Сообщение inform (inform). Сообщение, похожее на сообщение trap в протоколе SNMP. Это упреждающее сообщение создается управляемым устройством на основании порогового значения, заданного сетевым администратором. Различие между сообщениями inform и trap в том, что сообщение inform должно быть подтверждено сетевой управляющей станцией.

Сообщение SET (SET message). Сообщение, используемое протоколом SNMP для установки значений переменных в MIB. Эти сообщения позволяют администратору настраивать управляемое устройство, используя протокол SNMP.

Сообщение trap (trap). Тип сообщения протокола SNMP. Это упреждающее сообщение создается управляемым устройством на основании порогового значения, заданного сетевым администратором.

Сообщения Hello (Hello). Сообщения, используемые в протоколе OSPF для обнаружения соседних маршрутизаторов и установления связи с ними. В протоколе EIGRP используются для обнаружения соседних маршрутизаторов и установления связи с ними. В протоколе STP данным термином называют периодические уведомления от корневого моста в распределенном дереве.

Соседний маршрутизатор (neighbor). В протоколах маршрутизации устройство, с которым данный маршрутизатор обменивается маршрутной информацией.

Составная метрика (composite metric). Термин протокола EIGRP, описывающий результат вычисления метрики EIGRP для маршрута.

Состояние GLBP active (GLBP active). Состояние *протокола балансировки нагрузки шлюза* (GLBP), при котором маршрутизатор выступает в роли *активного виртуального шлюза* (AVG), или состояние *ретранслятора GLBP* (GLBP forwarder) — маршрутизатора, активно поддерживающего перенаправление пакетов вне подсети для хостов данной подсети.

Состояние GLBP listen (GLBP listen). Состояние *протокола балансировки нагрузки шлюза* (GLBP) для *ретранслятора*, при котором маршрутизатор в настоящее время не поддерживает перенаправление пакетов вне подсети для хостов данной подсети заданного виртуального MAC-адреса. Вместо этого он ожидает перехода в режим активного в настоящее время *ретранслятора*.

Состояние GLBP standby (GLBP standby). Состояние *протокола балансировки нагрузки шлюза* (GLBP), при котором маршрутизатор не выступает в роли *активного виртуального шлюза* (AVG), а вместо этого контролирует текущий шлюз AVG на случай его отказа.

Состояние HSRP active (HSRP active). Состояние протокола резервного маршрутизатора (HSRP), при котором маршрутизатор активно поддерживает перенаправление пакетов вне подсети для хостов данной подсети.

Состояние HSRP standby (HSRP standby). Состояние протокола резервного маршрутизатора (HSRP), при котором маршрутизатор не поддерживает в настоящее

время перенаправление пакетов вне подсети для хостов данной подсети, а ожидает на случай отказа активного в настоящее время маршрутизатора, чтобы взять на себя его роль.

Состояние блокировки (blocking state). В протоколе стандарта 802.1D состояние порта, в котором он не обрабатывает принимаемые фреймы с данными и не пересылает их дальше, но обрабатывает сообщения протокола STP.

Состояние игнорирования (discarding state). Состояние порта в протоколе RSTP, в котором принимаемые интерфейсом фреймы с данными не обрабатываются и не передаются дальше; обрабатываются и пересылаются только служебные сообщения протокола.

Состояние канала (link state). Один из классов алгоритмов, используемых в протоколах маршрутизации. Протоколы с учетом состояния каналов строят базу данных с множеством деталей о каналах (подсетях) и их состоянии (работает, выключен), на основании которой строится таблица оптимальных маршрутов.

Состояние передачи (forwarding state). Состояние порта в протоколе STP, при котором передаются пользовательские фреймы.

Состояние прослушивания (listening state). Временное состояние порта в протоколе STP, в которое он переходит сразу же из заблокированного состояния. Коммутатор очищает таблицу MAC-адресов в этом состоянии и игнорирует фреймы, полученные через интерфейс.

Состояние самообучения (learning state). Временное состояние порта в протоколе STP, в котором через интерфейс не передаются фреймы, но устройство обнаруживает MAC-адреса во входящих фреймах и заносит их в таблицу коммутации.

Список управления доступом (Access Control List — ACL). Список правил, используемых маршрутизатором да контроля потока пакетов через маршрутизатор, например, чтобы закрыть потоки пакетов с определенных IP-адресов для определенных интерфейсов.

Стандарт IEEE 802.11. Основной стандарт беспроводных локальных сетей.

Стандарт IEEE 802.1AD. Стандарт IEEE, являющийся аналогом фирменной технологии EtherChannel компании Cisco.

Стандарт IEEE 802.1D. Стандарт IEEE для протокола распределенного связующего дерева.

Стандарт IEEE 802.1Q. Стандарт IEEE для магистрального протокола сетей VLAN. В нем присутствует концепция собственной сети VLAN (native), в которой в заголовок не добавляются дополнительные данные, а во все остальные виртуальные сети добавляется дополнительный 4-байтовый заголовок после стандартного поля типа или длины фрейма.

Стандарт IEEE 802.1S. Стандарт IEEE для связующего дерева из нескольких экземпляров (Multiple Instances of Spanning Tree — MIST), позволяющего выполнять балансировку нагрузки для нескольких сетей VLAN.

Стандарт IEEE 802.1W. Стандарт IEEE для улучшенной версии протокола STP, называемой быстрым протоколом STP (Rapide STP), конвергенция которого лучше, чем у обычно протокола STP.

Стандарт IEEE 802.3. Стандарт IEEE для сетей Ethernet.

Стандартный список доступа (standard access list). Список доступа, в котором может быть проверен только IP-адрес отправителя и по нему принято решение передавать пакет дальше или отбросить его.

Стандартный шлюз/стандартный маршрутизатор (default gateway/default router). В конфигурации хоста IP — IP-адрес маршрутизатора, которому узел будет пересылать пакеты в том случае, если IP-адрес получателя пакета относится к другой подсети.

Станция управления сетью (Network Management Station — NMS). Устройство, выполняющее программное обеспечение управления сетью. Между станциями NMS и управляемыми устройствами зачастую используется протокол управления сетью SNMP.

Субинтерфейс (subinterface). Один из виртуальных интерфейсов на общем физическом интерфейсе.

Суммарный маршрут (summary route). Маршрут, созданный с помощью конфигурационных команд и объединяющий в себе несколько подсетей в виде одной записи таблицы маршрутизации, что заметно уменьшает ее размер.

Суммирование маршрутов (route summarization). Процесс объединения нескольких маршрутов в один, анонсируемый соседним устройствам. Суммирование используется для уменьшения размера таблиц маршрутизации устройств.

Таблица соседних устройств (neighbor table). Список обнаруженных соседних маршрутизаторов в протоколах EIGRP и OSPF.

Таймер Hello (Hello timer). Интервал времени в *протоколе связующего дерева* (Spanning-Tree Protocol), используемый для рассылки сообщений Hello BPDU.

Таймер MaxAge (MaxAge). Таймер STP, задающий, как долго коммутатор должен ждать, если он больше не получает сообщений Hello от корневого коммутатора, прежде чем приступить к повторной конвергенции топологии STP.

Таймер обновлений маршрутизации (update timer). Таймер, период которого задает частоту рассылки обновлений маршрутизации. Дистанционно-векторные протоколы маршрутизации рассылают обновления маршрутов с использованием таймеров.

Телефонная компания (telco). Общепринятое сокращение для телефонной компании.

Терминальное оборудование (Data Terminal Equipment — DTE). Устройство, расположенное на пользовательском конце интерфейса "пользователь–сеть", которое может выступать в качестве источника данных, получателя данных или того и другого. Устройство DTE подключается к сети данных через устройства DCE (например, модем), а для синхронизации зачастую использует создаваемые ими сигналы времени. Терминальное оборудование включает в себя такие устройства, как компьютеры, трансляторы протоколов и мультиплексоры. С точки зрения провайдера устройство DTE находится вне сети провайдера услуги и обычно представляет собой маршрутизатор.

Тестовый пакет (keepalive). Сообщение, отправляемое одним сетевым устройством, которое сигнализирует другому сетевому устройству о работоспособности виртуального канала между ними.

Технология CIDR (Classless Interdomain Routing — CIDR). Бесклассовая междоменная маршрутизация, основанная на открытом стандарте RFC. Позволяет маршрутизаторам группировать маршруты для сокращения объема маршрутной информации, передаваемой основными маршрутизаторами. С ее помощью несколько се-

тей IP выглядят для внешних сетей как одна сеть. Классовыми называют сети, относящиеся к сетям классов A, B и C в адресном пространстве протокола IPv4.

Технология Frame Relay (Frame Relay). Международный стандартный протокол канального уровня, с помощью которого реализуется служба коммутации фреймов, позволяющая устройствам DTE (обычно маршрутизаторам) пересылать данные многим устройствам-получателям через один физический канал.

Технология IPSec (IP Security). Набор открытых стандартов обеспечения конфиденциальности и целостности данных, а также аутентификации данных между равноправными участниками обмена данными. Предоставляет эти виды обеспечения безопасности на уровне IP. Использует IKE для согласования протоколов и алгоритмов, основанных на локальной политике, и для генерации ключей шифрования и аутентификации, используемых IPSec. Может защищать один или более поток данных между двумя хостами, между двумя шлюзами обеспечения безопасности или между хостом и шлюзом обеспечения безопасности.

Технология PortFast. Функция STP коммутаторов, позволяющая переключить порт в режим передачи сразу же после включения порта, минуя этапы прослушивания и самообучения (listening and learning). Конфигурируется в портах, к которым подключены пользователи.

Туннель GRE (GRE tunnel). Концепция соединения VPN между площадками, согласно которой конечные точки действуют как двухточечный канал связи (туннель) между площадками, при фактической инкапсуляции пакетов с использованием стандартов GRE.

Универсальный идентификатор устройства (Universal Device Identifier — UDI). Номер, присваиваемый каждому маршрутизатору Cisco, для однозначной идентификации типа маршрутизатора и индивидуального серийного номера. Используется в процессе лицензирования программного обеспечения IOS.

Универсальный образ (universal image). Универсальный образ операционной системы Cisco IOS, содержащий все наборы функций для конкретного устройства, для которого он был создан. Администратору достаточно лицензировать и разрешить выбранные средства.

Уникальный локальный адрес (unique local address). Тип одноадресатных IPv6-адресов, предназначенных для замены частных IPv4-адресов.

Ускоренный протокол распределенного связующего дерева (Rapid Spanning Tree Protocol — RSTP). Улучшенная версия протокола STP с улучшенной конвергенцией, работающая быстрее стандартного протокола STP(IEEE 802.1d). Описан в стандарте IEEE 802.1w.

Условие резервирования (feasibility condition). Условие, заключающееся в следующем: если в протоколе EIGRP маршрутизатор обнаружил несколько маршрутов к одной подсети, а метрика оптимального маршрута равна X, то маршруты соответствуют условию резервирования, когда их анонсируемая метрика меньше или равна X.

Устройство DCE Frame Relay (Frame Relay DCE). Коммутатор в технологии Frame Relay.

Устройство DTE Frame Relay (Frame Relay DTE). Оборудование пользователя, подключенное к каналу доступа среды Frame Relay; обычно — маршрутизатор.

Утилита `ping` (Packet Internet Groper — *проверка доступности адресата*). Протокол управляющих сообщений Интернета (ICMP) поддерживает эхо-запрос и воз-

вращение ответа на него; утилита `ping` зачастую используется в сетях IP для проверки доступности сетевого устройства.

Утилита `traceroute` (traceroute). Программа, доступная на многих операционных системах, позволяющая отслеживать путь пакета от отправителя до получателя. Используется главным образом при решении проблем маршрутизации между хостами.

Файл `running-config`. Имя располагающегося в оперативной памяти файла операционной системы Cisco IOS коммутаторов и маршрутизаторов, содержащего текущую конфигурацию устройства.

Файл `startup-config`. Имя располагающегося в памяти NVRAM файла операционной системы Cisco IOS коммутаторов и маршрутизаторов, содержащего ту конфигурацию устройства, которая будет загружена в оперативную память как файл конфигурации `running-config`, когда устройство будет перезагружено или включено.

Фильтр (filter). Обычно процесс или устройство, которое определяет, передавать ли трафик дальше на основе заданных критериев, таких как адрес отправителя, адрес получателя или протокол.

Флеш-память (flash memory). Специализированный тип электронно-перепрограммируемой постоянной памяти, 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.

Фреймирование (framing). Соглашение уровня 2 о том, как устройства интерпретируют биты, пересылаемые на уровне 1. Например, если электрические сигналы были приняты из кабеля и преобразованы в двоичный код, фреймирование позволяет определить информационные поля в блоке данных.

Целостность (integrity). Целостность передачах данных означает, что информация в пути не изменилась.

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 данных. Часто используется в качестве сети доступа к Интернету и 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.

Цифровой сигнальный уровень 3 (Digital Signal level 3 — DS3). Канал на 44,736 Мбит/с от телефонной компании имеет 28 каналов DS1 плюс дополнительные служебные. Называется также T3.

Частичное обновление маршрутов (partial update). Обновление, содержащее некоторое подмножество из известных устройству маршрутов.

Частная сеть IP (private IP network). Один из нескольких номеров классовых сетей IPv4, которые никогда не присваиваются при использовании в Интернете, а значит, используются в одном предприятии.

Частный адрес (private address). Зарезервированные IP-адреса в классах сетей A, B и C, предназначенные для использования только в локальной сети какой-либо организации. Описаны в документе RFC 1918 и не маршрутизируются в Интернете.

Шаблон маски (wildcard mask). Маска, используемая в списках ACL операционной системы Cisco IOS, а также в протоколах маршрутизации OSPF и EIGRP.

Широковещательный адрес подсети (broadcast subnet address). Адрес, который должен выделить инженер, разделяя сеть класса A, B или C на подсети, в части хоста которого все биты равны единице. Широковещательный адрес последней подсети совпадает с широковещательным адресом классовой сети. Последнюю подсеть классовой сети зачастую называют широковещательной.

Широковещательный адрес подсети, широковещательный адрес (subnet broadcast address, broadcast address). Специальный адрес в каждой подсети (наибольший). Посланные на него пакеты доставляются на все хосты в данной подсети.

Широковещательный домен (broadcast domain). Множество устройств, которые получают широковещательные фреймы, исходящие от любого устройства из этого множества. Обычно широковещательные домены ограничены маршрутизаторами, так как маршрутизаторы не передают широковещательные фреймы.

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.

Энергонезависимая память (Nonvolatile RAM — NVRAM). Тип *оперативной памяти* (RAM), сохраняющей свое содержимое даже при отключении питания.

Эхо-запрос ICMP (ICMP Echo Request). Один из типов сообщений ICMP, специально предназначенный для использования командой `ping` при проверке подключения к сети. Команда `ping` посылает эти сообщения другим хостам и ожидает в ответ сообщение эхо-ответа ICMP.

Эхо-ответ ICMP (ICMP Echo Reply). Один из типов сообщений ICMP, специально предназначенный для использования командой `ping` при проверке подключения к сети. Команда `ping` ожидает получения этих сообщений от других хостов в ответ на сообщение эхо-запроса ICMP.

Предметный указатель

3

3G/4G Wireless, 513

A

ABR, 288, 555
Access
  Control List, 140
  link, 441
  VPN, 257
ACL, 140, 226
Active Virtual Gateway, 240
AD, 297
Adaptive Security Appliance, 255
Address Resolution Protocol, 125, 537
Adjacent, 286
Administrative Distance, 297
ADSL, 511
Agent, 613
Area, 288
Area Border Router, 288, 555
ARP, 182, 466, 537
AS number, 327
ASA, 255
ASBR, 291
Asymmetric DSL, 511
Authentication, 423
Autonomous System Border Router, 291
Autosummarization, 364
AVG, 240

B

Backbone
  area, 288
  router, 288
Backup DR, 284
Basic Rate Interface, 509
BDR, 284
BID, 66
Blocking, 60
Boot field, 641
BPDU, 66, 104
BRI, 509
Bridge, 65
  ID, 66
  Protocol Data Unit, 66, 104
Broadcast, 398
  storm, 61

C

CDP, 422
Challenge Handshake Authentication Protocol, 421, 514
CHAP, 421, 514
CIR, 444
Cisco
  Discovery Protocol, 121, 422
  IOS, 635
  License Manager, 665
CLI, 185
CLM, 665
Clocking, 411
Command-Line Interface, 185
Community string, 616
Contiguous network, 365
Control
  plane, 121
  Protocol, 422
Cost, 70
CP, 422
CPE, 411
Crossover cable, 135
CSU/DSU, 411
Customer Premise Equipment, 411

D

Data
  Circuit-Terminating Equipment, 414
  Link Connection Identifier, 502
  plane, 121
  Terminal Equipment, 414
DCE, 414
Delivery header, 264
Designated
  Port, 65, 71, 107
  Router, 284
  switch, 65
DHCP Relay, 213
  Agent, 529
Digital Subscriber Line, 510
Discarding state, 80
Discontiguous network, 366
Distance, 320
  Vector, 315
DLCI, 502
DP, 65, 71, 107
DR, 284

DROther, 285
DS1, 413
DSL, 510
DTE, 414, 441
  cable, 415
Dual-stack, 531
Duplex mismatch, 138
DV, 315

E

EIGRP, 315, 532, 584
Encryption key, 258
Enhanced Interior Gateway Routing Protocol, 315, 532, 584
EoMPLS, 502
Equal-cost load balancing, 354
EtherChannel, 98
Ethernet
  emulation, 502
  over MPLS, 502
  WAN, 502
  поверх MPLS, 502
Extranet VPN, 257

F

FCS, 416
FD, 334
Feasible
  distance, 335
  Distance, 334
  successor, 335
  Successor, 352
FHRP, 231, 232, 236
First Hop Redundancy Protocol, 231, 232, 236
Flow, 625
Forward route, 198
Forwarding, 60
Frame Check Sequence, 416
FS, 352
Full update, 321
Fully adjacent, 286

G

Gateway Load Balancing Protocol, 236
Generic Routing Encapsulation, 261
GLBP, 236
GRE, 261

H

Hello Interval, 325
Hold Interval, 325
Hot Standby Router Protocol, 236
HSRP, 236

I

ICMP, 184
IEEE, 77
IGRP, 316
Inferior Hello, 68
Institute of Electrical and Electronic Engineers, 77
Integrated Services Digital Network, 508
Interarea
  route, 289
  subnet, 571
Interface bandwidth, 307
Interior Gateway Routing Protocol, 316
Internal router, 288
Internet
  Control Message Protocol, 184
  Service Provider, 500
Internetwork Operating System, 661
Intra-area route, 289
Intranet VPN, 257
IOS, 661
IP Address Resolution Protocol, 466
IP Control Protocol, 422
IP Security, 254
IPCP, 422
IPsec, 254
IPSec, 258
IPv4 routing table, 345
ISDN, 508
ISP, 500
ISR G2, 664

K

Keepalive, 429
  interval, 429
K-value, 390

L

LACP, 101
Layer 3 switch, 210
LCP, 422
Learning, 76
Leased line, 410
Link
  Aggregation Control Protocol, 101
  Control Protocol, 422
Link-local address, 527
Link-quality monitoring, 423
Link-State, 315
  Advertisement, 278, 283, 570
  Database, 279
  Update, 282, 320
Listening, 76
Local loop, 507
LQM, 423

LS, 315
LSA, 278, 283, 570
LSDB, 279
LSU, 282, 320

M

Management Information Base, 613, 615
Manager, 613
Mapping, 466
  information, 480
MIB, 613, 615
MPLS, 504
MST, 87
Multilayer switch, 210
Multiple Spanning Tree, 87
Multiprotocol Label Switching, 504

N

Native, 162
NBMA, 443
NCP, 422
NDP, 528
Neighbor
  Discovery Protocol, 528
  requirements, 388
  table, 306, 345
NetFlow collector, 623
Network
  Control Protocol, 422
  Management Station, 613
  type, 398
NMS, 613
Nonbroadcast Multiaccess, 441

O

Object ID, 615
OID, 615
Open Shortest Path First Version 3, 532
OSPF Database Description, 282
OSPFv3, 532

P

PAgP, 101
PAK, 667
PAP, 421
Password Authentication Protocol, 421
Permanent Virtual Circuit, 502
PID, 666
Point-to-point, 398
Point-to-Point
  Protocol, 421
Port Aggregation Protocol, 101
PPP, 421
  over Ethernet, 513
  поверх Ethernet, 513
PPPoE, 513
PRI, 509
Primary Rate Interface, 509
Priority, 66
Problem isolation, 125
Product Authorization Key, 667
Product ID, 666
PVC, 502
PVST+, 87
PVSTP, 87

R

RA, 544
Rapid
  Spanning Tree Protocol, 77
  STP, 87
RD, 334
Real-time Transport Protocol, 328
Reference bandwidth, 307
Release, 661
Reliable Transport Protocol, 328
Reported Distance, 334
Reverse route, 198
RID, 280
ROAS, 210
Root
  cost, 65
  Port, 65, 69
Route
  poisoning, 323
  redistribution, 297
Router
  Advertisement, 544
  ID, 280
  on a Stick, 210
  Solicitation, 544
Routing table, 306
RP, 65, 69
RPVST+, 87
RS, 544
RSTP, 77
RTP, 328
Runt, 139

S

Secure
  Shell, 183
  Socket Layer, 260
  Sockets Layer, 254
Serial cable, 411
Serial Number, 666
Service provider, 410
Shortest Path First, 279, 333
Simple Network Management Protocol, 613
Single point of failure, 232

SLAAC, 529
SN, 666
SNMP, 613
Spanning Tree Protocol, 60, 232
Speed mismatch, 138
SPF, 279, 333
Split horizon, 322
SSH, 183
SSL, 254, 260
Stateless Address Autoconfiguration, 529
STP, 60, 232
STP convergence, 65
Stream, 625
Successor, 352
Superior Hello, 68
Switch, 65
Syslog, 619
System ID, 66
  extension, 88

T

TAC, 639
TDM, 413
Telco, 410
Time-Division Multiplexing, 413
Topology table, 306, 345
Tunnel interface, 262

U

UC, 669
UDI, 666
Unequal-cost load balancing, 361
Unified Communication, 669
Universal image, 663
Unshielded Twisted-Pair, 135
Update message, 320
UTP, 135

V

Variance, 361
Vector, 320
Version, 661
Very Small Aperture Terminal, 505
Virtual
  Private Network, 254
  Router Redundancy Protocol, 236
VPN, 254
  tunnel, 255
VRRP, 236
VSAT, 505

W

WAN interface card, 412
WIC, 412
Wireless Internet, 513
Working port, 66

А

Абонентский канал, 507
Абонентское оконечное оборудование, 411
Автоматическая настройка адресов без
  фиксации состояния, 529
Автоматическое суммирование, 364
Агент, 613
  пересылки DHCP, 529
Адаптивное устройство безопасности, 255, 257
Административное расстояние, 297
Адрес
  глобальный одноадресатный, 525
  локальный в пределах канала связи, 527
  уникальный локальный одноадресатный, 525
Активный виртуальный шлюз, 240
Алгоритм
  DUAL, 337
  поиска первого кратчайшего маршрута, 333
  распределенных обновлений, 337
Анонс
  LSA, 283
  network LSA, 290
  router LSA, 290
  summary LSA, 290
  маршрутизатора, 544
  состояния канала, 278, 282, 570
Анонсируемое расстояние, 334
Ассиметричная цифровая абонентская
  линия, 511
Аутентификация, 255, 423, 618

Б

База
  данных состояния каналов, 279
  управляющей информации, 613, 615
Балансировка нагрузки, 309
Балансировки нагрузки
  с неодинаковыми стоимостями, 361
Беспроводной
  3G/4G, 513
  Интернет, 513

В

Вариация, 361
Вектор, 320
Версия, 661
Виртуальная частная сеть, 254
Внутренний маршрутизатор, 288
Внутриобластной маршрут, 289
Выделенная линия, 410
Выделенный
  коммутатор, 65
  маршрутизатор, 284
  порт, 65, 71, 107

Выпуск, 661
Вытеснение маршрута, 323

Г

Граничный маршрутизатор
  автономной системы, 291
  области, 288, 555

Д

Двойной стек, 531
Диалог начальной настройки, 653
Диспетчер
  SNMP, 613
  лицензий Cisco, 665
Дистанционно-векторная логика, 315
Дистанция, 320
Дуплексная передача, 409

Е

Единая точка отказа, 232

З

Заголовок
  Frame Relay, 442
  LAPF, 447
Заголовок передачи, 264
Загрузочное поле, 641
Задержка, 330
Запрос, 337
Запрос на получение информации о наличии маршрутизатора, 544
Защита от повторного использования, 255
Защищенное удаленное соединение, 183
Защищенный протокол IP, 254

И

Идентификатор
  DLCI, 442, 443
    локальный, 449
  канального подключения, 442, 443, 502
  маршрутизатора, 280
  моста, 66
  продукта, 666
Избыточность, 232
Инкапсуляция
  GRE, 261
  IETF, 462
  сквозная, 493
Институт
  ANSI, 442
  инженеров по электротехнике и электронике, 77
Интервал
  Hello, 325
  Hold, 325
  keepalive, 429
  задержки, 325
Интерфейс, 487
  LMI, 441
  LMI, 443
  базового уровня, 509
  командной строки, 185
  многостанционный, 455
  основного уровня, 509
  управления, 443
    локального, 441
Интерфейсная плата WAN, 412
Информация сопоставления, 480
Исходная полоса пропускания, 307

К

Кабель DTE, 415
Кабельный Интернет, 511
Канал
EtherChannel, 78, 98
PVC, 442
  активный, 488
  виртуальный, 443, 444
  коммутируемый, 443
  постоянный, 442, 443
  доступа, 441, 443
  неактивный, 488
  статический, 488
  удаленный, 488
Карликовый фрейм, 139
Клиент VPN, 257
Ключ
  авторизации продукта, 667
  шифрования, 258
Коллектор NetFlow, 623, 628
Команда
  ping, 183
  traceroute, 194
Коммутатор, 65
  уровня 3, 210
Конвергенция STP, 65
Контроль качества канала, 423
Конфигурационный регистр, 640
Конфиденциальность, 255
Концевик Frame Relay, 442
Корневая стоимость, 65
Корневой порт, 65, 69
Коэффициент K, 390

Л

Лицензия на право использования, 672
Локализация проблемы, 125

М

Магистраль 802.1Q, 149
Магистральная область, 288

Магистральный маршрутизатор, 288
Маршрут
  оптимальный, 335
  хоста, 433
Маршрутизатор, 257
  на палочке, 210
Маски VLSM, 222
Межобластная подсеть, 571
Межобластной маршрут, 289
Межсетевая операционная система, 661
Многоуровневый коммутатор, 210
Множественное связующее дерево, 87
Модель
  активный/активный, 240
  активный/пассивный, 237
  активный/резервный, 237
Модем, 507
  ISDN, 509
Модуль
  CPE, 411
  CSU/DSU, 411
  данных протокола моста, 66, 104
Мост, 65
Мультиплексирование с разделением времени, 413
Мультипротокольная коммутация по меткам, 504

Н

Надежный транспортный протокол, 328
Наилучшее сообщение Hello, 68
Не наилучшее сообщение Hello, 68
Невыделенный маршрутизатор, 285
Несмежная сеть, 366
Нешироковещательная среда с многостанционным доступом, 441
Нешироковещательный множественный доступ, 443
Неэкранированная витая пара, 135
Номер
  ASN, 328
  автономной системы, 327

О

Область, 288
OSPF, 287
Обновление состояния канала, 282, 320
Обобщенная маршрутная инкапсуляция, 261
Оборудование
DCE, 443
DTE, 443
терминальное, 441, 443
Образ IOS, 635
Обратный маршрут, 198
Общая строка SNMP, 616
Объектный идентификатор, 615
Оптимальное расстояние, 334
Оптимальный маршрут, 352
Ответ, 337
Открытый протокол поиска первого кратчайшего маршрута версии 3, 532
Очень маленький спутниковый терминал, 505

П

Пакет
  DD, 282
  LSU, 282
Перекрестный кабель, 135
Перераспределение маршрутов, 297
Поиск первого кратчайшего маршрута, 279
Поле
  Type, 416
  контрольной суммы фрейма, 416
  типа протокола, 447
Полное обновление маршрутов, 321
Полностью согласованный, 286
Полоса пропускания интерфейса, 307
Последовательный кабель, 411
Постоянный виртуальный канал, 502
Поток, 625
Приоритет, 66
Провайдер служб, 410
  Интернета, 500
Прослушивание, 76
Простой протокол управления сетью, 613
Протокол
  ARP, 125, 182
  CDP, 121, 131
  DHCPv6 с фиксацией состояния, 528
  GLBP, 240
  HSRP, 239
  Inverse ARP, 469
  LAPF, 447
  Rapid STP, 80
  аутентификации
    по паролю, 421
    с предварительным согласованием, 421, 514
  балансировки нагрузки шлюза, 236
  двухточечного соединения, 421
  доступа к каналу, 447
  защищенных сокетов, 260
  интерфейса локального управления, 441
  маршрутизации, 376
    внутреннего шлюза, 316
  обнаружения
    соседних устройств, 528
    устройств Cisco, 121, 131, 422
  объединения портов, 101
  преобразования адресов, 125, 182, 466, 537

распределенного связующего дерева, 60, 232
резервирования виртуального маршрутизатора, 236
резервирования первого транзитного участка, 231, 232, 236
резервного маршрутизатора, 236
системного журнала, 619
управления, 422
IP, 422
каналом, 422
объединением каналов, 101
сетью, 422
управляющих сообщений Интернета, 184
Прямой маршрут, 198
Путь, 625

Р

Рабочий порт, 66
Разделение диапазона, 322
Размер блока MTU, 573
Распределение нагрузки с учетом равной стоимости, 354
Рассогласование
дуплекса, 138
скорости, 138
Расстояние
FD, 335
оптимальное, 335
Расширение системного идентификатора, 88
Расширенный протокол маршрутизации внутреннего шлюза, 315, 532, 584
Режим PortFast, 79
Резервный
DR, 284
выделенный маршрутизатор, 285
маршрут, 335, 352
Ретранслятор DHCP, 213

С

Самообучение, 76
Связанная сеть VLAN, 210
Серийный номер, 666
Сеть
VPN, 257
неполносвязная, 453
собственная, 162
Синхронизация, 411
Системный
журнал, 619
идентификатор, 66
Скорость
доступа, 443
согласованная, 443
Служба BPDU Guard, 79
Смежная сеть, 365
Согласованный, 286
Сообщение
keepalive, 429
об обновлении, 320
Сопоставление, 466
Соседи EIGRP, 327
Составная метрика, 329
Состояние
down, 573
err-disabled, 143
exchange, 573
exstart, 573
secure-up, 144
блокировки, 60
игнорирования, 80
канала, 315
перенаправления, 60
Список управления доступом, 140, 226
Среда NBMA, 441
Стандарт PVST+, 88
Станция управления сетью, 613
Стоимость, 70
Субинтерфейс, 454, 487, 490

Т

Таблица
маршрутизации, 306
IPv4, 345
соседних устройств, 306, 345
топологии, 306, 345
Телефонная компания, 410
Терминальное оборудование, 414
канала, 443
канала передачи данных, 414
Технология
Frame Relay, 441, 501
LTE, 513
Тип сети, 398
двухточечный, 398
широковещательный, 398
Топология
неполносвязная, 445
полносвязная, 445
Транспортный протокол реального времени, 328
Требования к соседям, 388
Туннель, 256
VPN, 255
Туннельный интерфейс, 262

У

Универсальный образ, 663
Уникальный идентификатор устройства, 666
Унифицированная коммуникация, 669
Уровень

данных, 121
защищенных сокетов, 254
управления, 121
Ускоренный протокол распределенного связующего дерева, 77

Ф

Файл конфигурации, 650
Флеш-память, 635

Ц

Целостность
данных, 255
сообщения, 618
Цифровая сеть с комплексным обслуживанием, 508
Цифровой
абонентский канал, 510
сигнальный уровень 1, 413

Ч

Частичные обновления маршрутов EIGRP, 324

Ш

Широковещательный шторм, 61
Шифрование, 618
Шлюз
AVG, 240
стандартный, 122

Э

Эмуляция Ethernet, 502

ОФИЦИАЛЬНОЕ РУКОВОДСТВО CISCO
по подготовке к сертификационным экзаменам
CISCO CCENT/CCNA ICND1 100-101
АКАДЕМИЧЕСКОЕ ИЗДАНИЕ

Уэнделл Одом



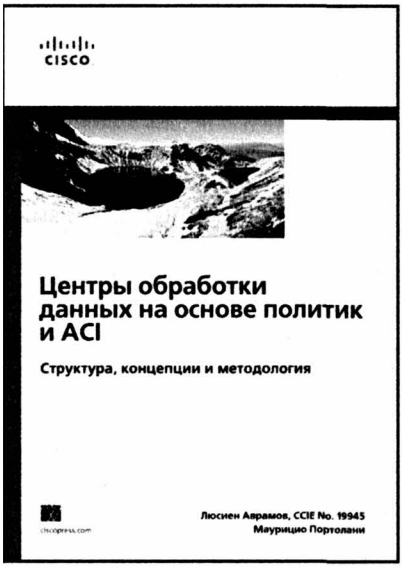
Нынешнее академическое издание — исчерпывающий справочник и учебное пособие по фундаментальным концепциям работы с сетями и вспомогательным приложениям. Книги этой серии являются официальным первоисточником для подготовки к экзамену. Они предоставляют теоретические и практические материалы, помогут кандидатам на сертификат Cisco Career Certification сконцентрировать усилия по изучению и повысить уверенность в себе по мере приближения дня экзамена. Хорошо выверенный по уровню детализации, оснащенный средствами оценки, вопросами и упражнениями, этот официальный учебник поможет вам преуспеть на экзамене.

www.williamspublishing.com

ISBN 978-5-8459-1906-9 **в продаже**

ЦЕНТРЫ ОБРАБОТКИ ДАННЫХ НА ОСНОВЕ ПОЛИТИК И ACI: структура, концепции и методология

Люсиен Аврамов, Маурицио Портолани



www.williamspublishing.com

Справочное руководство посвящено проектированию центров обработки данных на основе политик и инфраструктуры с акцентом на приложениях.
В книге изложены преимущества, архитектура, теория, концепции и методология центров обработки данных на основе политик. Демонстрируется использование сценариев Python и REST для автоматизации управления сетями и упрощения настройки сред ACI. Описываются аспекты проектирования виртуализированных центров обработки данных, систем для высокопроизводительных вычислений, сред со сверхмалыми задержками и крупномасштабных центров обработки данных. Рассматриваются вопросы, связанные с созданием гипервизоров и инфраструктур без виртуализации, демонстрируется интеграция служб, а также усовершенствованные методы телеметрии для выявления и устранения проблем.

ISBN 978-5-8459-2001-0 **в продаже**

Официальное руководство
по подготовке к сертификационным экзаменам

Cisco CCNA ICND2 200-101
Маршрутизация и коммутация
Академическое издание

Официальное руководство поможет освоить нужные темы по подготовке к сертификационным экзаменам CCNA ICND2, в частности:

- **протокол распределенного связующего дерева (STP)**
- **поиск и устранение неисправностей коммутации LAN**
- **маршрутизация IPv4**
- **сети VPN**
- **настройка, поиск и устранение неисправностей протоколов OSPF и EIGRP**
- **распределенные сети и Frame Relay**
- **реализация, поиск и устранение неисправностей протокола IPv6**

На веб-сайте!

На странице книги по адресу `http://www.williamspublishing.com/Books/978-5-8459-1907-6.html` находятся: образ DVD, содержащий больше 500 экзаменационных вопросов и практических задач, эмулятор *ICND2 Network Simulator Lite* и 60 минут обучающего видео на английском языке, а также дополнительные приложения из книги на русском языке.

Минимальные системные требования для практических сертификационных тестов: операционная система Windows XP (SP3), Windows Vista (SP2), Windows 7 или Windows 8; наличие Microsoft .NET Framework 4.0 Client; процессор 1 ГГц класса Pentium (или эквивалентный); оперативная память 512 Мбайт; дисковое пространство 650 Мбайт плюс по 50 Мбайт для каждого загруженного практического экзамена; доступ к Интернету для регистрации и загрузки экзаменационных баз данных.

Настоящая книга входит в серию *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.

Нынешнее академическое издание — исчерпывающий справочник и учебное пособие, знакомящие с фундаментальными концепциями настройки сетей, поиска и устранения неисправностей. Автор бестселлеров и опытный преподаватель Уэнделл Одом делится советами по подготовке к экзамену, помогая вам выявить свои слабые стороны, улучшить концептуальные знания и практические навыки.

ОСОБЕННОСТИ КНИГИ

- Описание процесса обучения, призванное помочь приобрести знания.
- Резюме в конце каждой главы, содержащие краткий обзор ключевых тем.
- Масса упражнений, включая справочные таблицы, краткий обзор основных команд, определения ключевых терминов, контрольные вопросы и многое другое, способное улучшить понимание тем и закрепить знания.
- Разделы по поиску и устранению неисправностей, помогающие разобраться в сложных реальных ситуациях.
- Бесплатный экземпляр электронной версии книги в форматах PDF, EPUB и Mobi (Kindle) на английском языке.
- Мощный процессор Pearson IT Certification Practice Test Premium Edition, укомплектованный сотнями выверенных реалистичных экзаменационных вопросов, увязывающий все вопросы с текстом книги и предоставляющий подробные отчеты об уровне подготовки.
- Бесплатный экземпляр эмулятора CCNA ICND2 200-101 Network Simulator Lite, укомплектованный лабораторными работами, позволяющими отточить практические навыки работы с пользовательским интерфейсом маршрутизаторов и коммутаторов.
- Более чем 60-минутная видеолекция автора книги на английском языке.
- Заключительная глава, содержащая дополнительные советы и описания ресурсов для подготовки к сертификационному экзамену.
- Ориентировочный план подготовки к экзамену, способный помочь организовать и оптимизировать процесс обучения.

Хорошо выверенный по уровню детализации, оснащенный планом подготовки, средствами оценки, вопросами и практическими упражнениями, этот официальный учебник поможет овладеть концепциями и методиками, позволяющими преуспеть на экзамене.

Уэнделл Одом, CCIE® №1624, является самым авторитетным в мире автором книг о сетях Cisco. Он написал книги по сертификации Cisco начального уровня (CCENT и CCNA), сертификации более высокого (CCNP) и отраслевого (CCIE) уровня. Его книги отличаются технической глубиной и точностью. Уэнделл работал сетевым инженером, консультантом, системным инженером, 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 978-5-8459-1907-6

Категория: Cisco Press — сертификация компании Cisco

Содержание: экзамены 200-101 ICND2 и 200-120 CCNA

ВИЛЬЯМС

www.williamspublishing.com
www.ciscopress.com

CCNA