



Создано Группой разработчиков учебных курсов Всемирной образовательной сети компании Cisco Systems, Inc.

Редактор серии "Основы организации сетей Cisco" – Вито Амати

Авторизованное учебное пособие по программе
"Основы организации сетей Cisco"

ОСНОВЫ ОРГАНИЗАЦИИ СЕТЕЙ CISCO

ТОМ 1



ББК 32.973.26-018.2.75

А61 УДК 681.3.07

Издательский дом "Вильяме" Зав. редакцией *С. Н. Тригуб*

Перевод с английского и редакция *А.А. Голубченко*

По общим вопросам обращайтесь в Издательский дом "Вильяме" адресу:

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

Амато, Вито.

А61 Основы организации сетей Cisco, том 1. : Пер. с англ. — М. : Издательский - дом "Вильяме", 2002. — 512 е. : ил. — Парал., тит. англ.

ISBN 5-8459-0258-4 (рус.)

Данная книга является учебным пособием по курсу "Основы организации сетей Cisco, часть 1" и соответствует учебному плану версии 2.1 Сетевой академии Cisco. В ней изложены основы построения IP-сетей на базе маршрутизаторов Cisco и описаны способы конфигурирования маршрутизаторов. В книге рассмотрены основополагающие вопросы теории сетей, в частности, эталонная модель OSI, физические основы передачи данных и сигналов, IP-адресация, технология Ethernet и много другое.

Большое внимание уделяется поиску неисправностей и устранению конфликтов в сети. Книга рекомендуется для подготовки к тесту CCNA и сертификационному экзамену CompTIA Net+.

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 © 2000

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

Russian language edition published by Williams Publishing House according to the Agreement with R&I Enterprises International, Copyright © 2002

ISBN 5-8459-0258-4 (рус.)

© Издательский дом "Вильяме", 2002

ISBN 1-58713-004-] (англ.)

© Cisco Press, 2000

Оглавление

Глава 1. Организация сети и эталонная модель OSI
Глава 2. Физический и канальный уровни
Глава 3. Сетевые устройства
Глава 4. Глобальные и локальные сети
Глава 5. IP-адресация
Глава 6. ARP и RARP
Глава 7. Топологии
Глава 8. Структурированная кабельная система и электропитание в сетях
Глава 9. Уровни приложений, представлений, сеансовый и транспортный
Глава 10. Протокол TCP/IP
Глава 11. Сетевой уровень и маршрутизация
Глава 12. Пользовательский интерфейс маршрутизатора и режимы
Глава 13. Вывод информации о конфигурации маршрутизатора
Глава 14. Запуск маршрутизатора и его начальное конфигурирование
Глава 15. Конфигурирование маршрутизатора
Глава 16. Источники загрузки ОС IOS
Глава 17. Конфигурирование IP-адресов интерфейсов маршрутизатора
Глава 18. Конфигурирование маршрутизатора и протоколы маршрутизации RIP и IGRP
Глава 19. Управление сетью
Приложение А. Список видеороликов
Приложение Б. Сводные данные о командах
Приложение В. Ответы на контрольные вопросы
Приложение Г. Основы компьютерной техники
Приложение Д. Основы электроники и сигналы
Приложение Е. Формирование сигналов и передача данных
Приложение Ж. Преобразование в двоичную и шестнадцатеричную систему счисления
Приложение З. Поиск и устранение неисправностей в сетях
Словарь терминов
Указатель англоязычных терминов
Предметный указатель

Содержание

Введение

Глава 1. Организация сети и эталонная модель OSI

Введение

Организация сети

С чего все начиналось

Локальные сети

Глобальные сети

Потребность в стандартах

Эталонная модель взаимодействия открытых систем (OSI)

Зачем нужна многоуровневая сетевая модель

Семь уровней эталонной модели OSI

Уровень 7 (уровень приложений)

Уровень 6 (уровень представлений)

Уровень 5 (сеансовый)

Уровень 4 (транспортный)

Уровень 3 (сетевой)

Уровень 2 (канальный)

Уровень 1 (физический)

Одноранговая модель взаимодействия

Инкапсулирование данных

Резюме

Контрольные вопросы

Глава 2. Физический и канальный уровни

Введение

Физический уровень

Среда передачи данных

Коаксиальный кабель

Неэкранированная витая пара

Экранированная витая пара

Оптоволоконный кабель

Выбор типа среды передачи данных

Канальный уровень

MAC-адреса

Сетевые адаптеры

Резюме

Контрольные вопросы

Глава 3. Сетевые устройства

Введение

Повторители

Использование повторителей для увеличения протяженности сети

Использование повторителей для увеличения числа узлов сети Концентраторы Мосты

Маршрутизаторы Резюме Контрольные вопросы

Глава 4. Глобальные и локальные сети

Введение

Локальные вычислительные сети

Сетевые стандарты Ethernet и IEEE 802.3

ЛВС и физический уровень

ЛВС и канальный уровень

Как работает сеть Ethernet/802.3

Широковещание в сети Ethernet/802.3

ЛВС и сетевой уровень

Множественный доступ с контролем несущей и обнаружением конфликтов Глобальные сети

Устройства глобальных сетей

Стандарты глобальных сетей

Глобальные сети и физический уровень

Глобальные сети и канальный уровень

HDLC

Frame Relay

PPP

ISDN Резюме Контрольные вопросы

Глава 5. IP-адресация

Введение

Обзор адресации

Двоичная система счисления

Двоичная IP-адресация Классы IP-адресов

Зарезервированные классы сетей Адресация подсетей

Адреса в подсети, зарезервированные для широковещания

Адреса в подсети, зарезервированные для номеров подсетей Маскирование подсетей

Операция AND Планирование подсетей

Пример планирования подсетей в сетях класса B

Пример планирования подсетей в сетях класса C Резюме Контрольные вопросы

Глава 6. ARP и RARP

Введение

ARP

ARP-запросы

ARP-ответы

ARP-таблицы

RARP

RARP-запросы

RARP-ответы

Маршрутизаторы и ARP-таблицы

Шлюз по умолчанию

Резюме

Контрольные вопросы

Глава 7. Топологии

Введение

Топология

Шинная топология

Передача сигнала в сети с шинной топологией

Преимущества и недостатки шинной топологии

Топология "звезда"

Преимущества и недостатки топологии "звезда"

Область покрытия сети с топологией "звезда"

Топология "расширенная звезда"

Резюме

Контрольные вопросы

Глава 8. Структурированная кабельная система и электропитание в сетях

Введение

Стандарты сетевых сред передачи данных

Стандарты EIA/TIA-568B

Горизонтальная кабельная система

Спецификации на кабельную систему

Гнездовые разъемы телекоммуникационного выхода

Разводка

Запрессовочные приспособления

Прокладка кабелей

Документирование и маркировка

Помещение для коммутационного оборудования

Магистральная кабельная система

Коммутационные панели

Порты коммутационной панели

Структура разводки коммутационной панели

Тестирование кабельной системы

Кабельные тестеры

Карты соединений

Электропитание

Заземление

Опорная земля сигналов

Влияние электрического шума на цифровые сигналы

Подавители перенапряжения

Перебои электропитания

Источники бесперебойного питания Резюме Контрольные вопросы

Глава 9. Уровни приложений, представлений, сеансовый и транспортный

Введение

Уровень приложений Уровень представлений Сеансовый уровень Транспортный уровень

Управление потоком

Установление соединения с одноранговой системой

Работа с окнами

Подтверждение Резюме Контрольные вопросы

Глава 10. Протокол TCP/IP

Введение

Краткое описание протокола TCP/IP

Группа протоколов TCP/IP TCP/IP и уровень приложений TCP/IP и транспортный уровень

Формат сегмента протокола TCP

Номера портов

Открытое TCP-соединение с трехсторонним квитированием

Простое подтверждение и работа с окнами в протоколе TCP

Скользящие окна в протоколе TCP

Порядковые номера и номера подтверждений в протоколе TCP

Формат сегмента в протоколе UDP TCP/IP и межсетевой уровень

IP-дейтаграмма

Протокол ICMP

Проверка пункта назначения с помощью протокола ICMP

Протокол ARP

Протокол RARP Резюме Контрольные вопросы

Глава 11. Сетевой уровень и маршрутизация

Введение

Маршрутизаторы Cisco Основные характеристики сетевого уровня Определение пути сетевым уровнем

Путь коммуникации

Адресация: сеть и хост-машина

Маршрутизация с использованием сетевых адресов

Протоколы маршрутизации и маршрутизируемые протоколы

Операции, выполняемые протоколом сетевого уровня

Многопротокольная маршрутизация

Статические и динамические маршруты

Пример статического маршрута

Пример маршрута по умолчанию

Адаптация к изменениям топологии

Операции динамической маршрутизации

Представление расстояния с помощью метрики

Протоколы маршрутизации

Алгоритмы маршрутизации по вектору расстояния

Алгоритм маршрутизации по вектору расстояния и исследование сети

Алгоритм маршрутизации по вектору расстояния и изменения топологии

Проблема- маршрутизация по замкнутому кругу

Проблема: счет до бесконечности

Решение: задание максимального значения

Решение: расщепление горизонта

Решение: таймеры удержания

Алгоритмы маршрутизации с учетом состояния канала связи

Режим исследования сети в алгоритмах с учетом состояния канала

Обработка изменений топологии в протоколах маршрутизации с учетом состояния канала связи

Моменты, которые требуют внимания

Проблема: обновление информации о состоянии каналов связи

Решение: механизмы учета состояния канала связи

Сравнение маршрутизации по вектору расстояния и маршрутизации с учетом состояния канала связи

Сбалансированная гибридная маршрутизация

Базовые процессы маршрутизации

Маршрутизация из одной локальной сети в другую

Маршрутизация из локальной сети в глобальную

Резюме

Контрольные вопросы

Глава 12. Пользовательский интерфейс маршрутизатора и режимы

Введение

Краткое описание интерфейса пользователя

Вход в систему маршрутизатора: межсетевая операционная система компании Cisco (IOS)

Команды пользовательского режима

Команды привилегированного режима

Функции команды help

Применение команд редактирования

Просмотр истории команд

Резюме

Контрольные вопросы

Глава 13. Вывод информации о конфигурации маршрутизатора

Введение

Компоненты маршрутизатора, участвующие в конфигурировании, и режимы работы маршрутизатора

Внешние источники конфигурации

Внутренние компоненты маршрутизатора, участвующие в конфигурировании

Рабочее хранение информации в ОЗУ

Режимы маршрутизатора Проверка состояния маршрутизатора с помощью команд просмотра статуса

Команды show running-config и show startup-config

Команда show interfaces

Команда show version

Команда show protocols

Получение доступа к другим маршрутизаторам с помощью протокола Cisco Discovery Protocol

Вывод записей протокола CDP о соседних устройствах

Пример конфигурирования протокола CDP

Вывод CDP-записи для конкретного устройства

Вывод данных о CDP-соседах Базовое тестирование взаимодействия в сети

Тестирование уровня приложений с помощью команды telnet

Проверка сетевого уровня с помощью команды ping

Проверка сетевого уровня с помощью команды trace

Применение команды show ip route для проверки сетевого уровня

Проверка физического и канального уровней с помощью команды

show interfaces serial Резюме Контрольные вопросы

Глава 14. Запуск маршрутизатора и его начальное конфигурирование

Введение

Процедуры запуска межсетевой операционной системы Cisco (OS IOS)

Последовательность запуска

Команды режима запуска Начальная установка: диалог конфигурирования системы

Установка глобальных параметров

Начальная установка параметров интерфейсов

Сценарий начальной установки и его использование Резюме Контрольные вопросы

Глава 15. Конфигурирование маршрутизатора

Введение

Конфигурирование маршрутизатора

Использование TFTP-сервера

Использование энергонезависимой памяти в маршрутизаторах, работающих под управлением ОС IOS версии 10.3

Использование энергонезависимой памяти в маршрутизаторах, работающих под управлением ОС IOS версии 11.0

Краткие сведения о режимах маршрутизатора

Режимы конфигурирования

Режим протокола IP-маршрутизации
Режим конфигурирования интерфейса
Примеры конфигурирования интерфейса
Методы конфигурирования
Конфигурирование версии, предшествующей версии 11.0
Конфигурирование паролей
Резюме
Контрольные вопросы

Глава 16. Источники загрузки ОС IOS

Введение
Обнаружение местоположения ОС IOS
Значения в регистре конфигурирования
Команда show version
Варианты начальной загрузки программного обеспечения
Подготовка к работе с TFTP-сервером
Команда show flash
Правила именования ОС IOS
Создание резервных копий образов программного обеспечения
Обновление версии образа по сети
Резюме
Контрольные вопросы

Глава 17. Конфигурирование IP-адресов интерфейсов маршрутизатора

Введение
Краткие сведения о TCP/IP-адресах
Концепции конфигурирования IP-адресов
Адреса хост-машин
Пример разбиения на подсети
Адрес широковещания
Конфигурирование IP-адресов
IP-имена хост-машин
Конфигурирование сервера имен
Схемы отображения "имя—адрес"
Вывод информации об именах хост-машин
Верификация конфигурации адресов
Команда telnet
Команда ping
Расширенная команда ping
Команда trace
Резюме
Контрольные вопросы

Глава 18. Конфигурирование маршрутизатора и протоколы маршрутизации RIP и IGRP

Введение
Начальное конфигурирование маршрутизатора
Начальная таблица IP-маршрутизации
Конфигурирование статических маршрутов
Пример статического маршрута
Конфигурирование маршрута по умолчанию
Пример маршрута по умолчанию
Протоколы внутренней или внешней маршрутизации
 Задачи, связанные с конфигурированием IP-маршрутизации
 Конфигурирование динамической маршрутизации
Протокол RIP
 Пример конфигурирования протокола RIP
 Мониторинг IP-маршрутизации
 Вывод содержимого таблицы IP-маршрутизации
Протокол IGRP

Пример конфигурирования протокола IGRP Резюме Контрольные вопросы

Глава 19. Управление сетью

Введение

Первые шаги в управлении сетью

Инвентаризационная ревизия

Ревизия установленного оборудования

Карта сети

Ревизия эксплуатации

Программные средства для управления сетью

Протокол SNMP

Протокол CMIP

Мониторинг сети

Ревизия эффективности

Ревизия средств защиты

Сетевые анализаторы

Решение проблем в сети

Документирование проблем в сети

Анализ и решение проблем в сети

Процедуры устранения неполадок

Оценки производительности сети

Процедуры выполнения изменений в сети

Резюме Контрольные вопросы

Приложение А. Список видеороликов

Приложение Б. Сводные данные о командах

Приложение В. Ответы на контрольные вопросы

Приложение Г. Основы компьютерной техники

Составляющие компьютера

Мелкие дискретные компоненты

Подсистемы персонального компьютера

Элементы задней стенки

Платы сетевого интерфейса

Компоненты портативных компьютеров

Программное обеспечение

Броузеры

Интегрируемые программные модули

Офисные прикладные программы

Сети

Полоса пропускания

Резюме

Приложение Д. Основы электроники и сигналы

Основы электричества

Типы электрических материалов

Изоляторы

Проводники

Полупроводники

Измерение электричества

Напряжение

Ток

Сопротивление

Импеданс

Электрическая земля

Простая цепь

Резюме

Приложение Е. Формирование сигналов и передача данных

Сигналы и шумы в коммуникационных системах

Сравнение аналоговых и цифровых сигналов
Использование цифровых сигналов для построения аналоговых сигналов
Представление одного бита в физической среде
Распространение
Аттенюация
Отражение
Шум
Дисперсия, неустойчивая синхронизация и запаздывание
(проблемы синхронизации)
Конфликты
Сообщения в терминах битов
Кодирование сетевых сигналов
Кодирование и модуляция
Резюме

Приложение Ж. Преобразование в двоичную и шестнадцатеричную систему счисления

Предварительные сведения
Как узнать, какое основание имеется в виду?
Некоторые факты
Принятые способы указания на величину основания
Работа с показателями степени
Двоичные числа
Преобразование десятичного числа в двоичное
Счет в двоичной системе
Четные и нечетные числа
Шестнадцатеричные числа
Преобразование десятичного числа в шестнадцатеричное
Преобразование шестнадцатеричного числа в двоичное
Практические упражнения

Приложение 3. Поиск и устранение неисправностей в сетях

Лабораторные работы по устранению неисправностей,
которые выполняются во втором семестре обучения
Общая модель поиска и устранения неисправностей
Практическое применение модели поиска и устранения неисправностей

Словарь терминов

Указатель англоязычных терминов

Предметный указатель

О редакторе серии

Вито Амато (Vito Amato) — старший технический автор во Всемирной образовательной системе компании Cisco. В свое время он работал директором по информационным технологиям отдела образования штата Аризона. Степень доктора философии Вито получил в Аризонском государственном университете, где специализировался на разработке учебных курсов и методичек, ориентированных на среду учебного процесса и применение в нем компьютеров. В настоящее время Вито преподает в Аризонском государственном университете теорию и практику заочного обучения. В течение трех последних лет Вито был вовлечен в планирование, написание и внедрение программы Сетевой академии Cisco. Основное внимание в ходе своей исследовательской, писательской и преподавательской деятельности Вито уделяет внедрению информационных технологий в среду преподавания и обучения.

Благодарности редактора серии

Данная книга была бы невозможна без четкого видения стоявших целей и самоотверженности Джорджа Варда (George Ward), Кевина Уорнера (Kevin Warner), Алекса Белу (Alex Belous), Дэвида Александера (Devid Alexander) и всей группы, которая занимается разработкой учебных курсов. Мне хотелось бы высказать слова признательности за их поддержку, которая не только сделала эту книгу реальностью, но и вдохнула жизнь в программу Сетевой академии Cisco, в рамках которой, собственно, и была создана данная книга. Мне также хотелось бы поблагодарить Джая Госина (Jai Gosine) и Денниса Фреззо (Dennis Frezzo), глубокое знание предмета которых позволило мне организовать материал книги. Кроме того, хотелось бы поблагодарить Уэйна Левиса (Wayne Lewis), обновившего устаревшие данные. Уэйн является координатором учебного центра Академии Cisco при городском общеобразовательном колледже Гонолулу. Он также занимается обучением инструкторов для Академии Cisco в Японии, Индонезии, Гонконге, США и на Тайване. В 1992 году Уэйн получил звание доктора философии в области математики Гавайского университета. Он является сертифицированным специалистом Cisco по сетям и проектированию, а также сертифицированным инструктором Академии Cisco и специалистом Microsoft. В свободное время Уэйн занимается серфингом на северном побережье Оаху. И, конечно же, я хотел бы поблагодарить свою жену Бонни и моих детей Тори, Майкла, Мет-тью и Лауру за их терпение и поддержку.

Данная книга является результатом синтеза и интеграции многих публикаций Cisco образовательного характера. И мне хотелось бы поблагодарить всю команду по разработке маркетинга системы образования за их вклад в это издание И, наконец, я хотел бы поблагодарить сотрудников издательства Cisco Press в лице Дейва Дастимера (Dave Dusthimer), Ами Левис (Amy Lewis) и Китти Джаррет (Kitty Jarrett), которые провели меня через весь процесс издания этой книги.

О технических рецензентах

Рецензенты внесли свой огромный практический опыт в процесс разработки первого тома книги *Основы организации сетей Cisco*. По мере написания книги они просматривали все материалы с точки зрения технического содержания, организации и подачи. Сделанные ими замечания оказали критически важное влияние на то, чтобы эта книга удовлетворяла потребность наших читателей в высококачественной технической информации.

Дениз Хойт (Denise Hoyt) 16 лет была преподавателем. Степень бакалавра получила в Калифорнийском государственном университете, Чико, а степень магистра по администрированию — в университете Редлендса. Летом 1998 года она прошла сертификацию на звание инструктора по программе Сетевой академии Cisco и в конце этого же года заняла

пост регионального координатора академии Cisco Systems в округе Сан-Бернардино. Дениз также работает координатором округа в области технологий и преподает курс по программе Сетевой Академии Cisco в средней школе в Юкаипо, штат Калифорния.

Марк Мак-Грегор (Mark McGregor) — сертифицированный специалист Cisco по сетевому администрированию и инструктор по программе Сетевой академии Cisco в колледже в Лос-Меданос и в школе для взрослых в Антиоке, Северная Калифорния. Имеет степень бакалавра по английскому языку университета штата Калифорния. В течение пяти лет преподавал в государственных школах, занимаясь главным образом обучением трудных подростков и альтернативным образованием.

Уэйн Ярвимаки (Wayne Jarvimaki) — сертифицированный специалист Cisco по сетевому администрированию и инструктор по программе Сетевой академии Cisco, а также инструктор и директор программы регионального учебного центра компании Cisco в Северном Сिएтле. Занимается обучением региональных инструкторов и инструкторов для регионального учебного центра Cisco с 1989 года. Как инструктор в области создания сетей он занимался разработкой программы обучения сертифицированных и дипломированных специалистов Cisco в общественном колледже Северного Сिएтла. Уэйн также состоит в группе рецензентов учебных курсов Сетевой академии Cisco.

Предисловие

Компания Cisco создала систему интерактивного обучения, которая интегрирует мультимедийную доставку курса по теории и практике создания сетей с тестированием, оценкой профессиональных навыков на основе выполнения практических заданий и сообщением результатов через Web-интерфейс. Программа *Основы организации сетей Cisco* выходит за рамки традиционных компьютерных учебных программ, помогающих обучающимся получить практические знания и навыки в области создания сетей с использованием среды, близко соответствующей реальной обстановке, в которой приходится работать при организации сети. В процессе изучения принципов и практических реализаций сетевых технологий вы будете работать с архитектурой и инфраструктурными элементами технологии создания сетей.

Главное в программе *Основы организации сетей Cisco* — это интеграция в учебный процесс ориентированного на Web сетевого курса. Как результат, программа *Основы организации сетей Cisco* дает средства для динамического обмена информацией за счет предоставления набора услуг, которые заново определяют способы распространения средств обучения, что, в свою очередь, приводит к возникновению сети интерактивно взаимодействующих друг с другом участников процесса обучения, разбросанных по всему миру.

От издательства

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

Мы ждем ваших комментариев и надеемся на них. Вы можете прислать электронное письмо или просто посетить наш Web-сервер, оставив свои замечания, — одним словом, любым удобным для вас способом дайте нам знать, нравится или нет вам эта книга, а также выскажите свое мнение о том, как сделать наши книги более 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 последующих книг. Наши координаты:

E-mail: info@ciscopress.ru

<http://www.ciscopress.ru>

Введение

Первый том книги *Основы организации сетей Cisco* задуман как дополнение к классным и лабораторным занятиям студентов, изучающих интерактивный курс Сетевой академии Cisco версии 2.1. В отсутствие курса эта книга помогает получить углубленные знания основ теории и практики создания сетей и основ конфигурирования маршрутизаторов. Настоящее издание включает дополнительный материал, который был недавно добавлен в интерактивный курс. В состав данного введения также включена подробная таблица соответствия, которая поможет студентам и преподавателям найти нужный материал для дополнительного чтения по темам соответствующих глав учебного курса версии 2.1. Если читатель не является студентом Сетевой Академии, он может пропустить эту таблицу.

Первый семестр курса версии 2.1 полностью посвящен модели OSI и только в середине рассматривается понятие структурированной кабельной системы. С учетом этих изменений в книгу включены приложение Г, "Основы компьютерной техники", содержащее основополагающие сведения, существенные для освоения курса, приложения Д, "Основы электроники и сигналы", и Е, "Формирование сигналов и передача данных", которые разъясняют материал разделов курса, посвященных средам передачи данных и основам электроники. Приложение Ж, "Преобразование в двоичную и шестнадцатеричную систему счисления", отражает присутствующие в курсе элементы двоичной и шестнадцатеричной математики, преподаваемые отдельно от IP-адресации, чтобы дать студентам время освоить эту математику до ее практического применения. Для поддержки курса в книгу также введено приложение З, "Поиск и устранение неисправностей в сетях".

И наконец, цель — этой книги подготовить читателя не только к тестированию и сдаче квалификационного экзамена на звание сертифицированного Cisco сетевого администратора, но и к сдаче квалификационного экзамена на звание специалиста по сетям в рамках программы сертифицирования CompTIA Net+. Знание и понимание модели OSI являются абсолютно необходимыми для всех студентов, специализирующихся в области создания сетей, которые готовятся к сдаче экзамена на звание сертифицированного Cisco сетевого администратора. Наряду с разделом об Ethernet, который важен для понимания доминирующей в мире технологии локальных сетей, также важными для сдачи этого экзамена являются разделы, посвященные конфликтам и сегментированию. Главы, посвященные теме IP-адресации, являются, вероятно, наиболее трудными с концептуальной точки зрения, но, тем не менее, это очень важные главы, и особенно для сдачи экзамена на звание сертифицированного сетевого администратора. Наконец, если вы ищете работу, связанную с созданием сетевых кабельных систем, то критически важно хорошо усвоить материал глав, посвященных структурированным кабельным системам и системам электропитания в сети.

Таблица соответствия для учебного курса

Если вы студент Сетевой академии, то интерактивный курс представляет собой наиболее динамичную часть программы Сетевой академии. Предполагается, что изучение каждой главы читатель начинает с интерактивного материала, а затем переходит к печатным материалам. Чтобы получить наибольшую отдачу от различных компонентов программы, используйте настоящую таблицу соответствия.

Интерактивный курс		Основы организации сетей Cisco, том 1		Сборник заданий и методичка по курсу "Основы организации сетей Cisco", том 1	
Глава	Название	Глава	Название	Глава	Название
1	Основы вычислительной техники	Приложение Г	Основы компьютерной техники	1	Основы вычислительной техники

2	Модель OSI	1	Организация сети и эталонная модель OSI	2	Модель OSI
3	Локальные сети	1	Организация сети и эталонная модель OSI	3	ЛС
		3	Сетевые устройства	17	ЛС: уровни 1-3
		4	Глобальные и локальные сети		
4	Основы электроники и сигналы	Приложение Д	Основы электроники и сигналы	4	Основы электроники и сигналы
5	Соединения в средах передачи данных и конфликты	2	Физический и канальный уровни	5	Уровень 1: сетевые среды передачи данных
6	Уровень 2: концепции	2	Физический и канальный уровни	6	Уровень 2: канальный
7	Уровень 2: технологии	4	Глобальные и локальные сети	7	Уровень 2: технологии
8	Проектирование и документирование	8	Структурированная кабельная система и электропитание в сетях	8	Проектирование и документирование
9	Проект структурированной кабельной системы	8	Структурированная кабельная система и электропитание в сетях	9	Структурированная кабельная система
10	Уровень 3: маршрутизация и адресация	5	IP-адресация	10	Уровень 3: маршрутизация и адресация
		7	Топологии		
		11	Сетевой уровень и маршрутизация		
		Приложение Ж	Преобразование в двоичную и шестнадцатеричную систему счисления		
11	Уровень 3 протоколы маршрутизации	11	Сетевой уровень и маршрутизация	11	Уровень 3. протоколы маршрутизации
12	Уровень 4. транспортный	9	Уровни приложений, представлений, сеансовый и транспортный	12	Уровень транспортный 4'
				18	Уровни 4-7
		10	Протокол TCP/IP		

13	Уровень 5. сеансовый	9	Уровни приложений, представлений, сеансовый и транспортный	13	Уровень 5: сеансовый
				18	Уровни 4-7
14	Уровень 6. уровень представлений	9	Уровни приложений, представлений, сеансовый и транспортный	14	Уровень 6 уровень представлений
				18	Уровни 4-7
15	Уровень 7: уровень приложений	9	Уровни приложений, представлений, сеансовый и транспортный	15	Уровень 7: уровень приложений
				18	Уровни 4-7
Второй семестр					
1	Краткий обзор	1	Организация сети и эталонная модель OSI	16	Краткий обзор модели OSI
2	Маршрутизаторы	4	Глобальные и локальные сети	19	Глобальные сети
		13	Вывод информации о конфигурации маршрутизатора	20	Маршрутизация
3	Использование маршрутизатора	12	Ползовательски и интерфейс маршрутизатора и режимы	21	Использование маршрутизатора
4	Составляющие маршрутизатора	13	Вывод информации о конфигурации маршрутизатора	22	Составляющие маршрутизатора
5	Запуск и начальная настройка маршрутизатора	14	Запуск маршрутизатора и его начальное конфигурирование	23	Запуск и начальная настройка маршрутизатора
6	Конфигурирование маршрутизатора	15	Конфигурирование маршрутизатора	24	Конфигурирование маршрутизатора
7	ОС IOS	16	Источники загрузки ОС IOS		ОС IOS
8	Индивидуальная работа по конфигу-				
9	Протокол TCP/IP	10	Протокол TCP/IP	26	Протокол TCP/IP
10	IP-адресация	17	Конфигурирование IP-адресов интерфейсов маршрутизатора	27	IP-адресация

11	Маршрутизация	11	Сетевой уровень и маршрутизация	20	Маршрутизация
12	Протоколы маршрутизации	18	Конфигурирование маршрутизатора и протоколы маршрутизации RIP и IGRP	28	Протоколы маршрутизации

Особенности книги

Многие элементы этой книги облегчают понимание излагаемых в ней вопросов по теории и практике создания сетей и маршрутизации.

- *Цели главы.* В начале каждой главы приводится перечень целей, которые должны быть достигнуты к концу изучения конкретной главы. Кроме того, в перечне упоминаются объясняемые в этой главе понятия, что позволяет использовать его в качестве средства систематизации.
- *Рисунки, листинги и таблицы.* В книге содержатся рисунки, листинги и таблицы, которые помогают в объяснении теоретических вопросов, понятий и команд, а также смысла последовательностей начального конфигурирования; они подкрепляют разъяснения концепций и помогают визуализировать содержание излагаемого в главе материала. Кроме того, листинги и таблицы содержат сводные данные о командах и их описания, примеры выводимой на экран информации, а также включают информацию практического и теоретического характера.
- *Резюме глав.* В конце каждой главы кратко изложены описываемые в ней концепции и понятия; по сути — это конспективное изложение содержания главы, которое помогает в освоении материала.
- *Контрольные вопросы.* После резюме в каждой главе даются 10 контрольных вопросов, которые позволяют оценить качество усвоения материала. Кроме того, вопросы подкрепляют объяснение концепций, введенных в главе, и помогают проверить уровень понимания перед переходом к изучению новой темы.

Условные обозначения

В этой книге используются следующие условные обозначения.

- Важные или новые термины выделяются *курсивом*.
- Все примеры кода даются шрифтом `courier`, при этом различные элементы кода приводятся с использованием следующих условных обозначений.
 - Команды и ключевые слова набраны **полужирным** шрифтом.
 - Названия аргументов, которые замещают собой значения, вводимые пользователем, показаны курсивом.
 - Квадратные скобки ([]) указывают на опционный характер ключевых слов или аргументов.
 - Фигурные скобки ({ }) указывают на обязательность выбора какого-либо из приведенных значений.
 - Вертикальные черточки () используются для разделения значений для выбора.

Структура книги

Книга содержит 19 глав, 8 приложений и словарь терминов.

Глава 1, "Организация сети и эталонная модель OSI", посвящена обсуждению сетевых терминов и концепций, а также определению понятий локальной и глобальной сетей. Кроме того, в ней рассматриваются семиуровневая эталонная модель взаимодействия открытых систем

(модель OSI) и процесс обмена информацией между нижними уровнями модели.

В главе 2, "Физический и канальный уровни", представлены функции сети, реализуемые на физическом и канальном уровнях эталонной модели OSI, а также различные типы сетевых сред передачи данных, которые используются на физическом уровне. Кроме того, в ней обсуждается тот факт, что доступ к сетевой среде передачи данных происходит на канальном уровне модели OSI, и то, каким образом данные находят в сети свой пункт назначения.

В главе 3, "Сетевые устройства", описаны сетевые устройства, которые могут использоваться для фильтрации трафика сети и уменьшения размеров больших доменов конфликтов, представляющих собой области, в которых есть вероятность того, что пакеты будут мешать друг другу.

В главе 4, "Глобальные и локальные сети", представлены технологии локальных и глобальных сетей, а также сетевые устройства, которые работают на физическом, канальном и сетевом уровнях модели OSI.

Глава 5, "IP-адресация", посвящена описанию структуры IP-адресов и трех классов сетей, определяемых в соответствии со схемами IP-адресации, а также описаны IP-адреса, которые выделены ARIN в отдельную группу и не могут быть присвоены какой-либо сети. Наконец, в ней рассматриваются подсети и маски подсетей, описываются схемы их IP-адресации.

В главе 6, "ARP и RARP", рассматриваются устройства локальной сети, которые перед переадресацией пакетов в пункт назначения используют протокол преобразования адресов (ARP). Кроме того, рассматривается ситуация, когда устройство, находящееся в одной сети, не знает MAC-адреса устройства, находящегося в другой сети.

В главе 7, "Топологии", описываются топологии, которые используются при создании сетей.

Глава 8, "Структурированная кабельная система и электропитание в сетях", посвящена структурированным кабельным системам и электрическим спецификациям для локальных сетей, а также способам прокладки кабелей и подачи электропитания в сетях, находящихся в зданиях.

В главе 9, "Уровни приложений, представлений, сеансовый и транспортный", рассматриваются четыре верхних уровня эталонной модели OSI. Подробно описываются процессы, используемые на транспортном уровне для обеспечения надежной доставки данных и эффективного управления их потоком.

В главе 10, "Протокол TCP/IP", описываются протокол управления передачей/межсетевой протокол (TCP/IP) и его работа по обеспечению обмена данными в произвольном множестве соединенных между собой сетей.

Глава 11, "Сетевой уровень и маршрутизация", посвящена вопросам применения и работы маршрутизаторов при реализации ключевых функций межсетевого взаимодействия сетевого уровня эталонной модели OSI.

В главе 12, "Пользовательский интерфейс маршрутизатора и режимы", рассматривается роль сетевого администратора в эксплуатации маршрутизатора таким образом, чтобы обеспечить рациональную и эффективную доставку данных в сети.

В главе 13, "Вывод информации о конфигурации маршрутизатора", описаны корректные процедуры и команды доступа к маршрутизатору, команды для проверки и обслуживания его составных частей, а также для проверки его способности обеспечить соединения в сети.

В главе 14, "Запуск маршрутизатора и его начальное конфигурирование", объясняется порядок запуска маршрутизатора при его первом включении путем применения корректных команд и запускающей последовательности начального конфигурирования маршрутизатора.

В главе 15, "Конфигурирование маршрутизатора", объясняется использование режимов маршрутизатора и методов конфигурирования для обновления конфигурационного файла при работе с текущей и предыдущей версиями ОС IOS.

Глава 16, "Источники загрузки ОС IOS", посвящена использованию разнообразных источников получения кода ОС IOS, исполнению команд загрузки ОС IOS в маршрутизатор, ведению резервных копий файлов и выполнению обновления версии ОС IOS.

В главе 17, "Конфигурирование IP-адресов интерфейсов маршрутизатора", описывается конфигурирование IP-адресов.

В главе 18, "Конфигурирование маршрутизатора и протоколы маршрутизации RIP и IGRP", описывается начальное конфигурирование маршрутизатора с активизацией исполнения протоколов IP-маршрутизации RIP и IGRP.

Глава 19, "Управление сетью", посвящена базовым основам управления сетью путем

применения таких методик, как документирование, аудит, мониторинг и оценка эффективности работы.

Приложение А, "Список видеороликов", содержит справочную информацию по каждому видеоролику в формате QuickTime, который содержится на прилагаемом к книге компакт-диске.

В приложении Б, "Сводные данные о командах", даны определения встречающихся в данной книге команд, связанных с конфигурированием и использованием маршрутизаторов Cisco. Команды располагаются в алфавитном порядке, что позволяет быстро и легко найти информацию о заданной команде.

Приложение В, "Ответы на контрольные вопросы", содержит ответы на контрольные вопросы, приведенные в конце каждой главы.

Приложение Г, "Основы компьютерной техники", содержит дополнительный материал для чтения по теме новой главы 1 интерактивного курса.

Приложение Д, "Основы электроники и сигналы", дает дополнительную информацию по физике электричества и электронике: темам, которые были добавлены в версию интерактивного курса 2.1.

В приложении Е, "Формирование сигналов и передача данных", содержится новая информация о формировании сигналов, которая была добавлена в версии интерактивного курса 2.1.

Приложение Ж, "Преобразование в двоичную и шестнадцатеричную систему счисления", содержит дополнительный материал и практические задания, призванные помочь в освоении этой важной темы.

В приложении З, "Поиск и устранение неисправностей в сетях", содержится новая добавленная в интерактивный курс информация о методах поиска и устранения неисправностей.

Словарь терминов включает определения использованных в данной книге терминов и аббревиатур, относящихся к теории и практике создания сетей передачи данных.

Глава 1

Организация сети и эталонная модель OSI

В этой главе

Организация сети

- Протоколы и их важность в организации
- Локальная сеть (LAN)
- Глобальная сеть (WAN)
- Программные и аппаратные особенности различных способов организации сети
- Определение и описание основных сетевых стандартов
- Функции каждого из уровней эталонной модели OSI
- Процесс инкапсуляции и взаимодействие между уровнями

Введение

В этой главе объясняются основные термины и концепции, применяемые в теории сетей и рассматриваются два различных типа сетей

Локальные сети (Local Area Networks, LAN), позволяющие предприятиям, применяющим в своей производственной деятельности компьютерные технологии, повысить эффективность коллективного использования одних и тех же ресурсов, например, файлов и принтеров

Глобальные сети (Wide Area Networks, WAN), делающие возможным обмен данными V между предприятиями, которые удалены на значительные расстояния друг от друга.

Наконец, будут рассмотрены эталонная модель взаимодействия открытых систем (Open System Interconnection, OSI) и процессы обмена данными между нижними уровнями этой модели.

Организация сети

Организацией сети называется обеспечение взаимосвязи между рабочими станциями, периферийным оборудованием (принтерами, накопителями на жестких дисках, сканерами, приводами CD-ROM) и другими устройствами. При организации сети одной из задач является согласование различных типов компьютеров. Независимо от того, какие устройства используются в сети — Macintosh, IBM-совместимые компьютеры или мэйнфреймы, — все они должны использовать для общения один и тот же язык. Таким языком служит *протокол*, который является формальным описанием набора правил и соглашений, регламентирующих обмен информацией между устройствами в сети. Например, если группе людей поручают работу над общим проектом, то не имеет значения, кто эти люди по национальности — немцы, французы, итальянцы или американцы, — главное, чтобы они могли понять друг друга, т.е. разговаривали на одном языке. В современном мире такая группа людей, скорее всего, использовала бы английский язык. В сфере компьютерных технологий роль такого языка выполняют протоколы, которые понятны всем устройствам сети.

С чего все начиналось

Первые компьютеры были *автономными устройствами*. Другими словами, каждый компьютер работал отдельно, независимо от других. Очень скоро стала очевидной низкая эффективность такого подхода. Необходимо было найти решение, которое бы удовлетворяло трем перечисленным ниже требованиям, а именно:

- устраняло дублирование оборудования и ресурсов;
- обеспечивало эффективный обмен данными между устройствами;
- снимало проблему управления сетью.

Было найдено два решения, выполняющих поставленные условия. И это были локальные и глобальные сети.

Локальные сети

Локальные сети служат для объединения рабочих станций, периферии, терминалов и других устройств. Локальная сеть позволяет повысить эффективность работы компьютеров за счет совместного использования ими ресурсов, например файлов и принтеров. Как результат, это дает возможность предприятию использовать локальную сеть для связи воедино данных, функций обмена и вычислений, а также хранения информации на файл-серверах.

Характерными особенностями локальной сети являются:

- ограниченные географические пределы;

- обеспечение многим пользователям доступа к среде с высокой пропускной способностью;
- постоянное подключение к локальным сервисам;
- физическое соединение рядом стоящих устройств.

Глобальные сети

Быстрое распространение компьютеров привело к увеличению числа локальных сетей. Они появились в каждом отделе и учреждении. В то же время каждая локальная сеть — это отдельный электронный остров, не имеющий связи с другими себе подобными. Стало очевидным, что использования технологии локальных сетей уже недостаточно.

Требовалось найти способ передачи информации от одной локальной сети к другой. Решить эту задачу помогло создание *глобальных сетей*. Глобальные сети служат для объединения локальных сетей и обеспечивают связь между компьютерами, находящимися в локальных сетях. Глобальные сети охватывают значительные географические пространства и дают возможность связать устройства, расположенные на большом удалении друг от друга.

При подключении компьютеров, принтеров и других устройств к глобальной сети возникает возможность совместного использования информации и ресурсов, а также доступа к Internet. Один из вариантов организации сети показан на рис. 1.1.

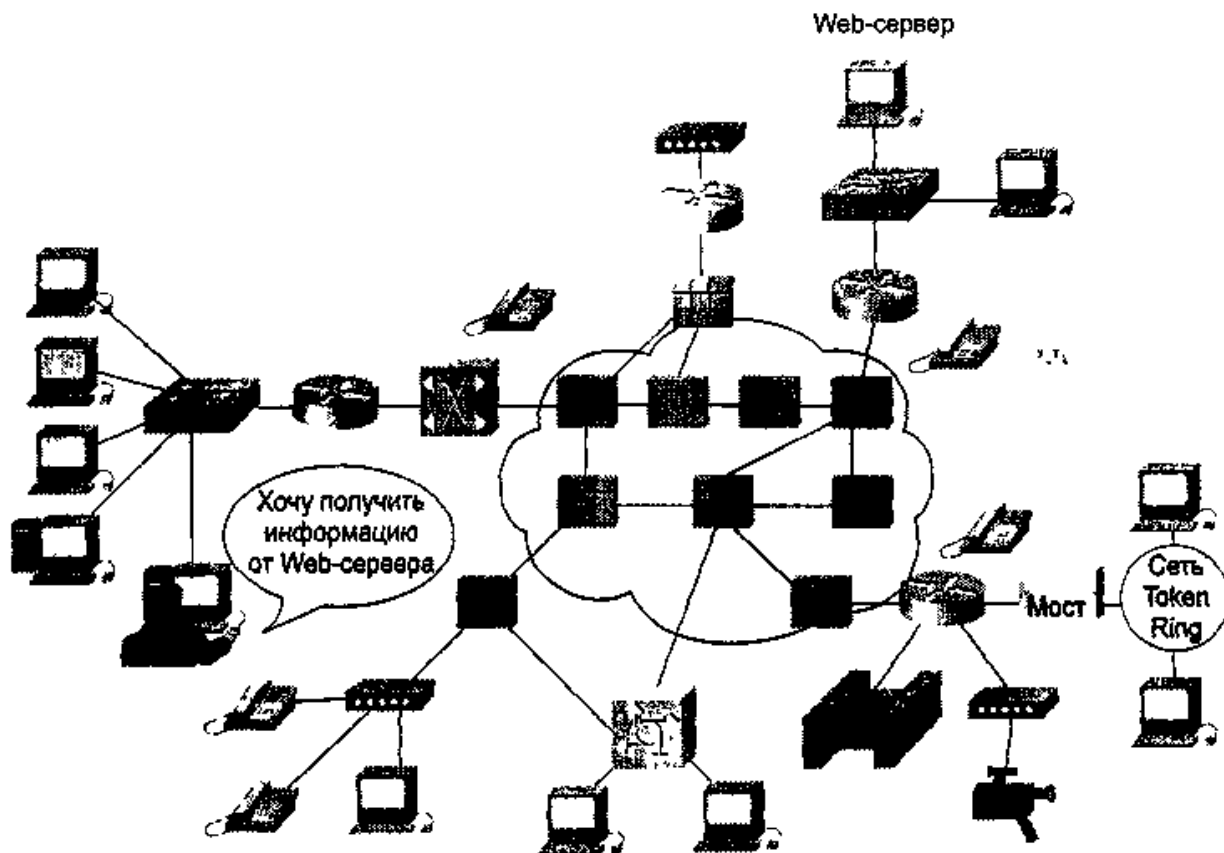


Рис. 1.1 При подключении компьютеров и принтеров к WAN становится возможным совместно использование информации

Потребность в стандартах

В течение двух последних десятилетий наблюдался значительный рост глобальных сетей. Убедившись, что использование сетевых технологий сулит существенную экономию денежных средств и повышение производительности труда, крупные организации стали уделять особое внимание этому направлению. Новые технологии и продукты внедрялись

сразу после их появления, и поэтому многие сети были сформированы с использованием различных аппаратных и программных средств. Вследствие этого многие сети оказались несовместимыми и стало сложным организовывать обмен информацией между компьютерами, использующими различные сетевые спецификации.

Для решения проблемы совместимости *Международная организация по стандартизации (International Organization for Standardization, ISO)* исследовала существующие схемы сетей. В результате исследования была признана необходимость в создании эталонной модели сети, которая смогла бы помочь поставщикам создавать совместимые сети. И в 1984 году ISO выпустила в свет эталонную модель взаимодействия открытых систем (OSI).

Эталонная модель OSI быстро стала основной архитектурной моделью взаимодействия между компьютерами. Несмотря на то, что были разработаны и другие архитектурные модели, большинство поставщиков сетей, желая сказать пользователям, что их продукты совместимы и способны работать с разными производимыми в мире сетевыми технологиями, ссылаются на их соответствие эталонной модели OSI. И действительно, эта модель является самым лучшим средством, имеющимся в распоряжении тех, кто надеется изучить технологию сетей.

Эталонная модель взаимодействия открытых систем (OSI)

Эталонная модель OSI — это описательная схема сети; ее стандарты гарантируют высокую совместимость и способность к взаимодействию различных типов сетевых технологий. Кроме того, она иллюстрирует процесс перемещения информации по сетям. Это концептуальная структура, определяющая сетевые функции, реализуемые на каждом ее уровне. Модель OSI описывает, каким образом информация проделывает путь через сетевую среду (например, провода) от одной прикладной программы (например, программы обработки таблиц) к другой прикладной программе, находящейся в другом подключенном к сети компьютере. По мере того, как подлежащая отсылке информация проходит вниз через уровни системы, она становится все меньше похожей на человеческий язык и все больше похожей на ту информацию, которую понимают компьютеры, а именно на "единицы" и "нули".

Эталонная модель OSI делит задачу перемещения информации между компьютерами через сетевую среду на семь менее крупных и, следовательно, более легко разрешимых подзадач. Каждая из этих семи подзадач выбрана потому, что она относительно автономна и, следовательно, ее легче решить без чрезмерной опоры на внешнюю информацию. Такое разделение на уровни называется *иерархическим представлением*. Каждый уровень соответствует одной из семи подзадач (рис. 1.2).



Рис. 1.2. Семь уровней эталонной модели OSI

Поскольку нижние уровни (с 1 по 3) модели OSI управляют физической доставкой сообщений по сети, их часто называют *уровнями среды передачи данных (media layers)*. Верхние уровни (с 4 по 7) модели OSI обеспечивают точную доставку данных между компьютерами в сети, поэтому их часто называют *уровнями хост-машины (host layers)* (рис. 1.3).

В большинстве сетевых устройств реализованы все семь уровней. Однако для ускорения

выполнения операций в некоторых сетях сама сеть реализует функции сразу нескольких уровней.

Модель OSI не является схемой реализации сети, она только определяет функции каждого уровня и в этом смысле подобна чертежу автомобиля (рис. 1.4).

После создания чертежа автомобиля сам автомобиль еще надо изготовить. Для выполнения фактической работы по изготовлению автомобиля могут быть заключены контракты с любым количеством автомобилестроительных компаний. Если чертеж полон, то все автомобили должны быть в механическом смысле одинаковы. Они могут отличаться по внешнему виду цветом или количеством используемых в отделке хромированных деталей, однако, все они будут одинаковы функционально.

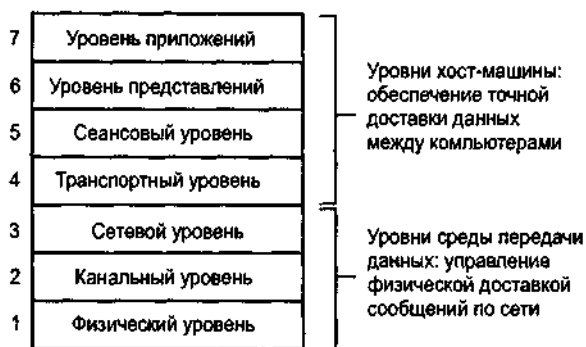


Рис. 1.3 Уровни среды передачи данных управляют физической доставкой сообщений, а уровни хост-машины обеспечивают точную доставку данных

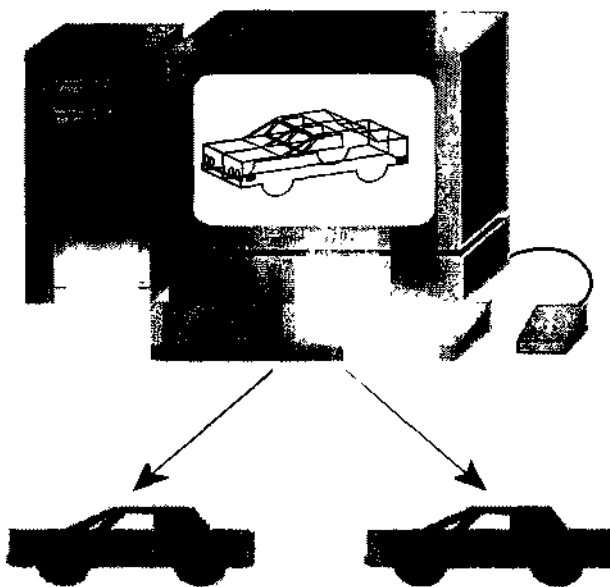


Рис. 1.4. Эталонная модель OSI похожа на чертеж автомобиля она задает функции каждого уровня

Чем объясняется разница в реализациях одного и того же чертежа автомобиля (или спецификации протокола)? Частично эта разница вызвана невозможностью учесть в любой спецификации все возможные детали реализации. Кроме того, разные люди, реализующие один и тот же проект, всегда интерпретируют его немного по-разному. Как следствие, неизбежные ошибки в реализации приводят к тому, что результаты разных реализаций отличаются исполнением. Этим объясняется то, что реализация протокола X одной компании не всегда взаимодействует с реализацией этого же протокола, осуществленной другой компанией.

Поэтому каждый уровень эталонной модели выполняет соответствующие ему функции, определенные стандартом OSI, к которому может обратиться любой производитель сетевых продуктов.

Зачем нужна многоуровневая сетевая модель

В эталонной модели OSI семь нумерованных уровней указывают на наличие различных сетевых функций. Деление сети на семь уровней обеспечивает следующие преимущества.

- Делит взаимосвязанные аспекты работы сети на менее сложные элементы.
- Определяет стандартные интерфейсы для автоматического интегрирования в систему новых устройств (*plug-and-play*) и обеспечения совместимости сетевых продуктов разных поставщиков.
- Дает возможность инженерам закладывать в различные модульные функции межсетевое взаимодействие симметрию, что позволяет легко наладить их взаимодействие.
- Изменения в одной области не требуют изменений в других областях, что позволяет отдельным областям развиваться быстрее.
- Делит сложную межсетевую структуру на дискретные, более простые для изучения подмножества операций.

Семь уровней эталонной модели OSI

После описания основных особенностей принципа деления модели OSI на уровни можно перейти к обсуждению каждого отдельного уровня и его функций. Каждый уровень имеет заранее заданный набор функций, которые он должен выполнять, чтобы связь могла состояться.

Уровень 7 (уровень приложений)

Уровень приложений — это самый близкий к пользователю уровень модели OSI. Он отличается от других уровней тем, что не предоставляет услуги ни одному другому уровню модели OSI и только обслуживает прикладные процессы, находящиеся вне пределов модели OSI. Примерами таких прикладных процессов могут служить программы работы с электронными таблицами, текстовые процессоры и программы работы банковских терминалов.

Уровень приложений идентифицирует и устанавливает доступность предполагаемых партнеров для связи, синхронизирует совместно работающие прикладные программы, а также устанавливает договоренность о процедурах восстановления после ошибок и контроля целостности данных. Уровень приложений также определяет степень достаточности ресурсов для осуществления предполагаемой связи.

Уровень 6 (уровень представлений)

Уровень представлений отвечает за то, чтобы информация, посылаемая из уровня приложений одной системы, была читаемой для уровня приложений другой системы. При необходимости уровень представлений преобразовывает форматы данных путем использования общего формата представления информации.

Уровень 5 (сеансовый)

Как указывает его название, сеансовый уровень устанавливает, управляет и завершает сеансы взаимодействия приложений. Сеансы состоят из диалога между двумя или более объектами представления (как вы помните, сеансовый уровень обеспечивает своими услугами уровень представлений). Сеансовый уровень синхронизирует диалог между объектами уровня представлений и управляет обменом информацией между ними. В дополнение к основным

функциям сеансовый уровень предоставляет средства для синхронизации участвующих в диалоге сторон, обеспечивает класс услуг и средства формирования отчетов об особых ситуациях, возникающих на сеансовом уровне, а также на уровнях приложений и представлений.

Уровень 4 (транспортный)

Транспортный уровень сегментирует и повторно собирает данные в один поток. Если уровень приложений, сеансовый уровень и уровень представлений заняты прикладными вопросами, четыре нижних уровня решают задачу транспортировки данных.

Транспортный уровень пытается обеспечить услуги по транспортировке данных, которые изолируют верхние уровни от деталей ее реализации. В частности, заботой транспортного уровня является решение таких вопросов, как выполнение надежной транспортировки данных через многосетевой комплекс. Предоставляя надежные услуги, транспортный уровень обеспечивает механизмы для установки, поддержания и упорядоченного завершения действия виртуальных каналов, обнаружения и устранения неисправностей транспортировки, а также управления информационным потоком (с целью предотвращения переполнения одной системы данными от другой системы).

Уровень 3 (сетевой)

Сетевой уровень — это комплексный уровень, который обеспечивает соединение и выбор маршрута между двумя конечными системами, которые могут находиться в географически разных сетях. Более подробно уровень 3 будет рассмотрен в главе 3, "Сетевые устройства".

Уровень 2 (канальный)

Канальный уровень обеспечивает надежный транзит данных через физический канал. Выполняя эту задачу, канальный уровень решает вопросы физической адресации (в противоположность сетевой или логической адресации), топологии сети, дисциплины в канале связи (т.е. каким образом конечная система использует сетевой канал), уведомления об ошибках, упорядоченной доставки кадров, а также вопросы управления потоком данных.

Уровень 1 (физический)

Физический уровень определяет электротехнические, механические, процедурные и функциональные характеристики активизации, поддержания и деактивизации физического канала между конечными системами. Спецификации физического уровня определяют такие характеристики, как уровни напряжений, временные параметры изменения напряжений, скорости физической передачи данных, максимальные расстояния передачи информации, физические разъемы, и другие подобные характеристики.

Одноранговая модель взаимодействия

Многоуровневая модель OSI исключает прямую связь между равными по положению уровнями, находящимися в разных системах, как показано на рис. 1.5.

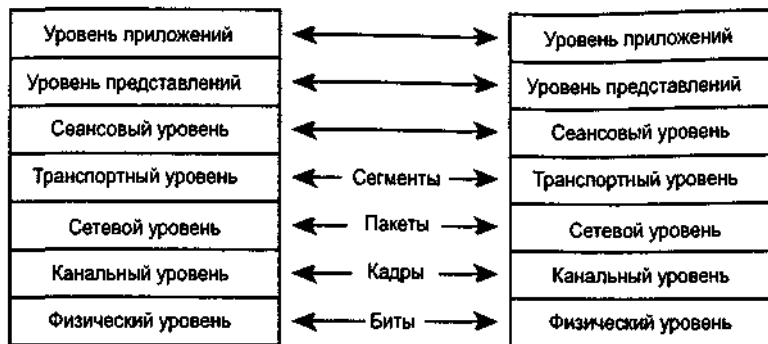


Рис. 1.5. Равные по положению уровни разных систем для связи между собой используют собственные протоколы

Каждый уровень системы имеет свои определенные задачи, которые он должен выполнять. Для выполнения этих задачи, он должен общаться с соответствующим уровнем в другой системе. Обмен сообщениями между одноранговыми уровнями или, как их еще называют, *блоками данных протокола (protocol data units, PDUs)*, осуществляется с помощью протокола соответствующего уровня. Каждый уровень может использовать свое специфическое название для PDU.

Подобный обмен данными по протоколу между одноранговыми уровнями достигается за счет использования услуг уровней, лежащих в модели ниже общающихся. Уровень, находящийся ниже любого текущего, оказывает услуги текущему уровню. Каждая из служб низлежащего уровня использует информацию от верхних уровней в качестве части PDU протокола более низкого уровня, которыми она обменивается с соответствующим уровнем другой системы.

Например, в семействе протоколов TCP/IP транспортные уровни для обмена пользуются сегментами (см. рис. 1.5). Таким образом, TCP-сегменты становятся частью пакетов сетевого уровня (также называемых *дейтаграммами*) и будут участвовать в обмене между соответствующими IP-уровнями. В свою очередь, на канальном уровне IP-пакеты должны стать частью кадров, которыми обмениваются непосредственно соединенные устройствами. В конечном итоге при передаче данных по протоколу физического уровня с использованием аппаратных средств кадры преобразовываются в биты.

Инкапсулирование данных

Чтобы понять структуру и принципы функционирования сети, необходимо уяснить, что любой обмен данными в сети осуществляется от источника к получателю (рис. 1.6). Информацию, посланную в сеть, называют *данными, или пакетами данных*. Если один компьютер (источник) хочет послать данные другому компьютеру (получателю), то данные сначала должны быть собраны в пакеты в процессе *инкапсуляции*; который перед отправкой в сеть погружает их в заголовок конкретного протокола. Этот процесс можно сравнить с подготовкой бандероли к отправке — обернуть содержимое бумагой, вложить в транспортный конверт, указать адрес отправителя и получателя, наклеить марки и бросить в почтовый ящик.

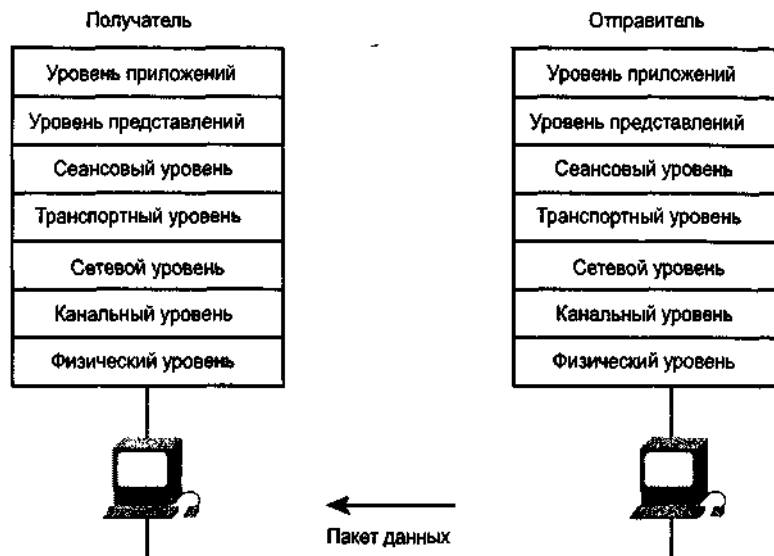


Рис. 1.6. Пакеты данных в сети движутся от источника к получателю

Каждый уровень эталонной модели зависит от услуг нижележащего уровня. Чтобы обеспечить эти услуги, нижний уровень при помощи процесса инкапсуляции помещает PDU, полученный от верхнего уровня, в свое поле данных; затем могут добавляться заголовки и трейлеры, необходимые уровню для реализации своей функции. Впоследствии, по мере перемещения данных вниз по уровням модели OSI, к ним будут прикрепляться дополнительные заголовки и трейлеры.

Например, сетевой уровень обеспечивает поддержку уровня представлений, а уровень представлений передает данные в межсетевую подсистему (рис. 1.7).

Задачей сетевого уровня является перемещение данных через сетевой комплекс. Для выполнения этой задачи данные инкапсулируются в заголовок который содержит информацию, необходимую для выполнения передачи, например логические адреса отправителя и получателя.

В свою очередь, канальный уровень служит для поддержки сетевого уровня (рис. 1.8) и инкапсулирует информацию от сетевого уровня в кадр. Заголовок кадра содержит данные (к примеру, физические адреса), необходимые канальному уровню Для выполнения его функций.

Физический уровень служит для поддержки канального уровня. Кадры канального Уровня преобразуются в последовательность нулей и единиц для передачи по физическим каналам (как правило, по проводам) (рис. 1.9).

При выполнении сетями услуг пользователям, поток и вид упаковки информации изменяются. В показанном на рис. 1-10 примере инкапсуляции имеют место пять этапов преобразования:

1. *Формирование данных.* Когда пользователь посылает сообщение электронной почтой, алфавитно-цифровые символы сообщения преобразовываются в данные, которые могут перемещаться в сетевом комплексе.

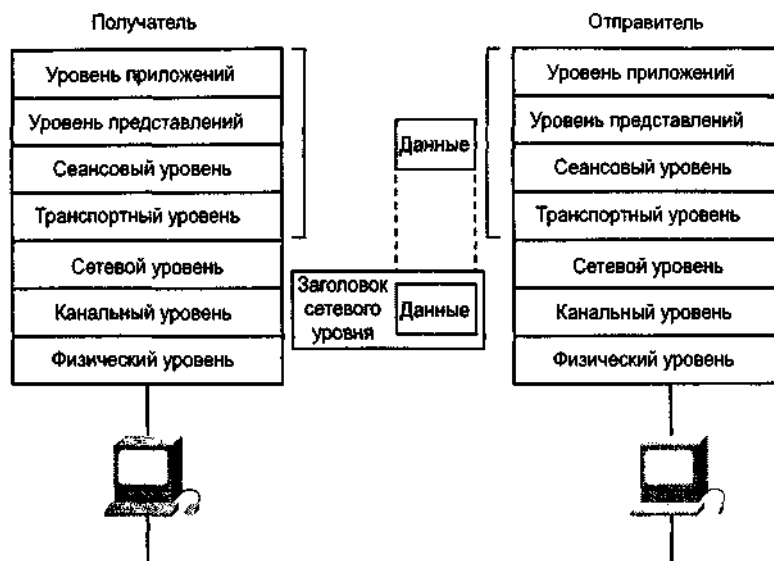


Рис. 1.7. Сетевой уровень оказывает услуги уровню представлений, инкапсулируя данные в сетевой заголовок

2. *Упаковка данных для сквозной транспортировки.* Для передачи через сетевой комплекс данные соответствующим образом упаковываются. Благодаря использованию сегментов, транспортная функция гарантирует надежное соединение участвующих в обмене сообщениями хост-машин на обоих концах почтовой системы.
3. *Добавление сетевого адреса в заголовок.* Данные помещаются в пакет или дейтаграмму, которая содержит сетевой заголовок с логическими адресами отправителя и получателя. Эти адреса помогают сетевым устройствам посылать пакеты через сеть по выбранному пути.
4. *Добавление локального адреса в канальный заголовок.* Каждое сетевое устройство должно поместить пакеты в кадр. Кадры позволяют взаимодействовать с ближайшим непосредственно подключенным сетевым устройством в канале. Каждое устройство, находящееся на пути движения данных по сети, требует формирования кадров для соединения со следующим устройством.
5. *Преобразование в последовательность битов для передачи.* Для передачи по физическим каналам (обычно по проводам) кадр должен быть преобразован в последовательность единиц и нулей. Функция тактирования дает возможность устройствам различать эти биты в процессе их перемещения в среде передачи данных. Среда на разных участках пути следования может меняться. Например, сообщение электронной почты может выходит из локальной сети, затем пересекать магистральную сеть комплекса зданий и дальше выходить в глобальную сеть, пока не достигнет получателя, находящегося в удаленной локальной сети.

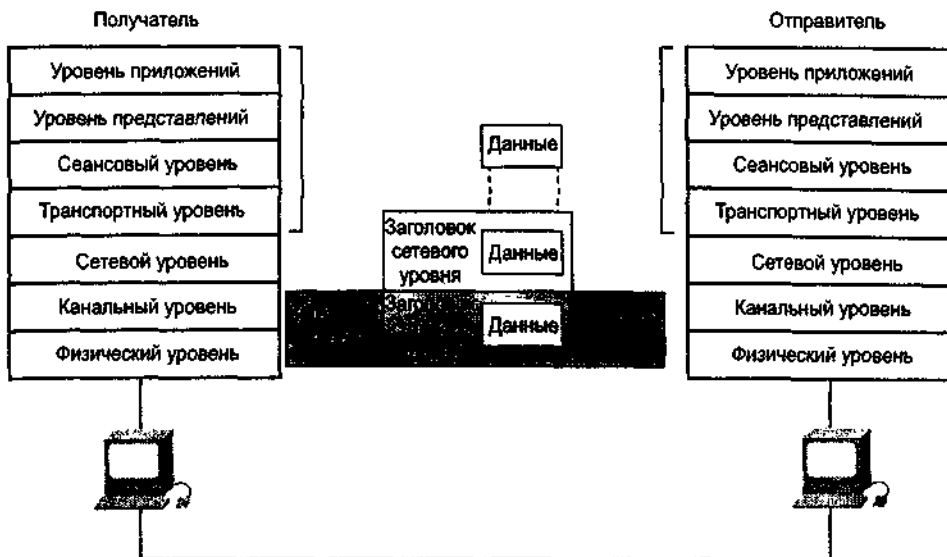


Рис. 1.8. Канальный уровень оказывает услуги сетевому, помещая информацию, полученную от сетевого уровня, в кадр

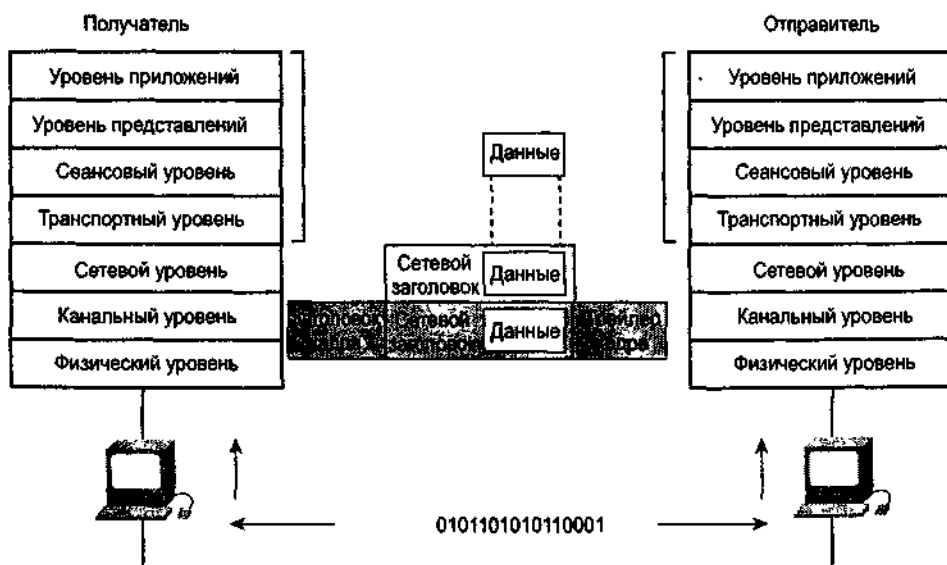


Рис. 1.9. Кадр, полученный от канального уровня, преобразуется физическим уровнем в последовательность нулей и единиц для дальнейшей передачи

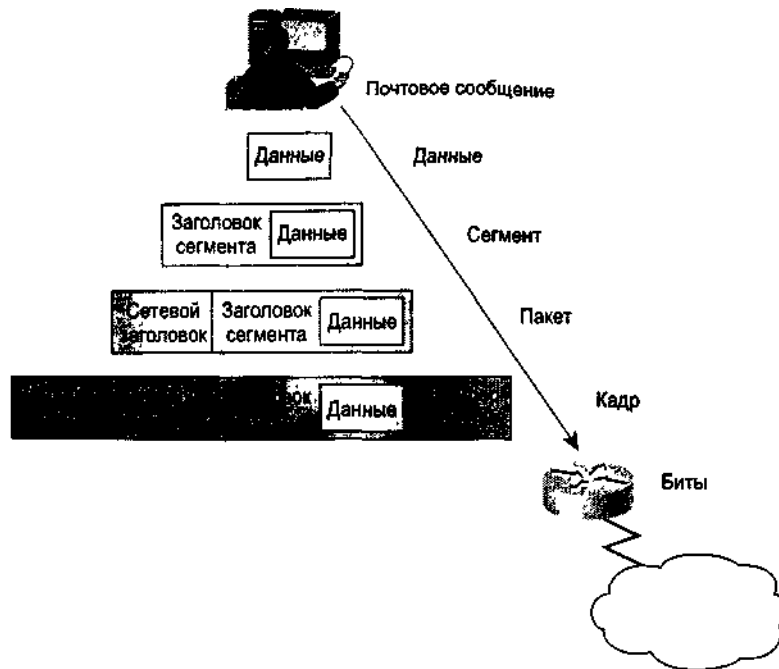


Рис. 1 10. По мере движения данных вниз по уровням эталонной модели OSI к ним добавляются новые заголовки и трейлеры

Резюме

- *Организацией сети* называется обеспечение взаимосвязи между рабочими станциями, периферийным оборудованием (принтерами, накопителями на жестких дисках, сканерами, приводами CD-ROM) и другими устройствами.
- *Протокол* — это формальное описание набора правил и соглашений, регламентирующих процессы обмена информацией между устройствами в сети.
- *Эталонная модель OSI* — это описательная схема сети; ее стандарты гарантируют высокую совместимость и взаимодействие сетевых технологий различных типов.
- В эталонной модели OSI отдельные сетевые функции организованы в семь нумерованных уровней:
 - уровень 7 (уровень приложений);
 - уровень 6 (уровень представлений);
 - уровень 5 (сеансовый);
 - уровень 4 (транспортный);
 - уровень 3 (сетевой);
 - уровень 2 (канальный);
 - уровень 1 (физический);

Многоуровневая модель OSI исключает прямую связь между равными по положению уровнями, находящимися в разных системах.

Инкапсуляция — это процесс погружения данных в заголовок конкретного протокола перед отправкой их в сеть.

Контрольные вопросы

1. Эталонная модель OSI является многоуровневой. Какое из положений неправильно характеризует причину многоуровневости модели?
 - A. Многоуровневая модель увеличивает сложность.
 - B. Многоуровневая модель стандартизирует интерфейсы.
 - C. Многоуровневая модель дает возможность разработчикам сконцентрировать усилия на более

- специализированных направлениях.
- D. Многоуровневая модель предотвращает влияние изменений в одной области на другие области.
2. Какой уровень эталонной модели OSI решает вопросы уведомления о неисправностях, учитывает топологию сети и управляет потоком данных?
- A. Физический.
 - B. Канальный.
 - C. Транспортный.
 - D. Сетевой.
3. Какой уровень эталонной модели OSI устанавливает, обслуживает и управляет сеансами взаимодействия прикладных программ?
- A. Транспортный.
 - B. Сеансовый.
 - C. Уровень представлений.
 - D. Уровень приложений.
4. Что из приведенного ниже наилучшим образом описывает функцию уровня представлений?
- A. Он обеспечивает форматирование кода и представление данных.
 - B. Он обрабатывает уведомления об ошибках, учитывает топологию сети и управляет потоком данных.
 - C. Он предоставляет сетевые услуги пользовательским прикладным программам.
 - D. Он обеспечивает электрические, механические, процедурные и функциональные средства для активизации и поддержания канала связи между системами.
5. Какой уровень эталонной модели OSI обеспечивает сетевые услуги пользовательским прикладным программам?
- A. Транспортный.
 - B. Сеансовый.
 - C. Уровень представлений.
 - D. Уровень приложений.
6. Какое описание пяти этапов преобразования данных в процессе инкапсуляции при отправке почтового сообщения одним компьютером другому является правильным?
- A. Данные, сегменты, пакеты, кадры, биты.
 - B. Биты, кадры, пакеты, сегменты, данные.
 - C. Пакеты, сегменты, данные, биты, кадры.
 - D. Сегменты, пакеты, кадры, биты, данные.
7. При отправке почтового сообщения с компьютера А на компьютер В данные необходимо инкапсулировать. Какое из описаний первого этапа инкапсуляции является правильным?
- A. Алфавитно-цифровые символы конвертируются в данные.
 - B. Сообщение сегментируется в легко транспортируемые блоки.
 - C. К сообщению добавляется сетевой заголовок (адреса источника и получателя).
 - D. Сообщение преобразовывается в двоичный формат.
8. При отправке почтового сообщения с компьютера А на компьютер В по локальной сети данные необходимо инкапсулировать. Что происходит после создания пакета?
- A. Пакет передается по среде.
 - B. Пакет помещается в кадр.
 - C. Пакет сегментируется на кадры.
 - D. Пакет преобразовывается в двоичный формат.
9. При отправке почтового сообщения с компьютера А на компьютер В данные необходимо инкапсулировать. Что происходит после преобразования алфавитно-цифровых символов в данные?
- A. Данные преобразовываются в двоичный формат.
 - B. К данным добавляется сетевой заголовок.
 - C. Данные сегментируются на меньшие блоки.
 - D. Данные помещаются в кадр.
10. Что из приведенного ниже наилучшим образом описывает дейтаграмму?
- A. Посылаемое источнику сообщение с подтверждением получения неповрежденных данных.

- B. Двоичное представление информации о маршрутизации.
- C. Пакет данных размером менее 100 байт.
- D. Пакет сетевого уровня.

Глава 2

Физический и канальный уровни

В этой главе

- Описание уровня 1 (физического) эталонной модели OSI
- Кодирование
- Название и определение четырех сред передачи данных
- Критерии для оценки качественных характеристик среды передачи данных
- Описание уровня 2 (канального) эталонной модели OSI
- Описание и назначение MAC-адреса
- Описание и назначение сетевого адаптера.

Введение

В главе 1, "Организация сети и эталонная модель OSI", были рассмотрены два различных типа сетей — локальные и глобальные, которые используются предприятиями для реализации коллективного пользования компьютерами, файлами и устройствами. Было также указано, что эталонная модель OSI стала основной архитектурной моделью процесса обмена информацией в сети. Несмотря на то, что были разработаны и другие архитектурные модели, на сегодня большинство поставщиков сетевых решений, рассказывая пользователям о возможностях своих сетевых продуктов, связывают их с эталонной моделью OSI. Кроме того, в этой главе говорилось, что данные всегда движутся по направлению от отправителя к получателю.

В данной главе будут рассмотрены основные функции физического и канального уровней эталонной модели OSI. Будет рассказано о различных средах передачи данных, используемых физическим уровнем, включая экранированную и неэкранированную витую пару, коаксиальный и оптоволоконный кабели. Также будет рассмотрена зависимость величины и скорости информационного потока от типа используемой среды передачи данных. Наконец, будет показано, что доступ к среде передачи данных осуществляется на канальном уровне эталонной модели OSI. В частности, будет рассказано, за счет чего данные имеют возможность определять местонахождение своего пункта назначения в сети.

Физический уровень

Термин "физический уровень" используется для того, чтобы показать, как сетевые функции привязаны к эталонной модели OSI. Как здание нуждается в фундаменте, так и сеть должна иметь основание, на котором она будет строиться. В эталонной модели OSI таким фундаментом служит *физический уровень* (рис. 2.1).

Физический уровень определяет электрические, механические, процедурные и функциональные спецификации для активизации, поддержания и деактивизации физической связи между конечными системами.

Назначением физического уровня является передача данных. Данные, которыми является любой тип информации (рисунки, тексты и звуки), представлены в виде импульсов: либо электрических, называемых *напряжением* — при передаче по медному кабелю, либо световых — при передаче по оптоволоконному кабелю. Процесс передачи, называемый *кодированием*, выполняется с помощью среды передачи данных — кабелей и разъемов.

Среда передачи данных

Средой передачи данных называется физическая среда, пригодная для прохождения сигнала. Чтобы компьютеры могли обмениваться кодированной информацией, среда должна обеспечить их физическое соединение друг с другом. Существует несколько видов сред, применяемых для соединения компьютеров (рис. 2.2):

- коаксиальный кабель;
- неэкранированная витая пара;
- экранированная витая пара;
- оптоволоконный кабель.

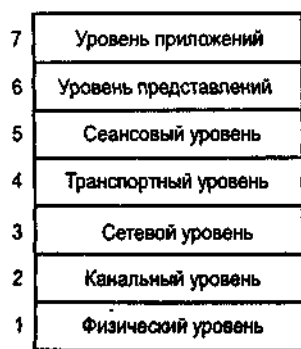


Рис. 2.1. В эталонной модели OSI фундаментом является физический уровень



Коаксиальный кабель



Неэкранированная витая пара



Оптоволоконный кабель

Рис. 2.2. Обычно в качестве среды передачи данных используются коаксиальный кабель, витая пара и оптоволоконный кабель

Коаксиальный кабель

Коаксиальный кабель состоит из внешнего цилиндрического пустотелого проводника, окружающего один внутренний провод (рис. 2.3).

Коаксиальный кабель состоит из двух проводящих элементов. Один из них — медный провод, находящийся в центре кабеля и окруженный слоем гибкой изоляции. Поверх изоляционного материала расположен экран из тонких переплетающихся медных проводов или из металлической фольги, который в электрической цепи играет роль второго провода. Как следует из названия, внешняя оплетка служит для экранирования центрального провода от влияния помех. Снаружи экран покрыт оболочкой

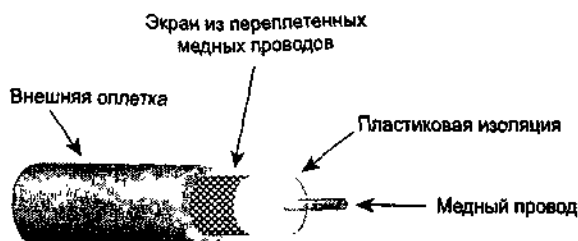


Рис 2.3. Коаксиальный кабель состоит из внутреннего провода, окруженного пустотелым цилиндрическим проводником.

Для локальных сетей применение коаксиального кабеля дает несколько преимуществ. Коаксиальный кабель может использоваться без усиления сигнала на больших расстояниях, чем экранированная или неэкранированная витая пара. Это означает, что сигнал может проходить более длинные расстояния между сетевыми узлами, не нуждаясь в повторителе для усиления сигнала, как в витой паре. Коаксиальный кабель дешевле, чем оптоволоконный. Наконец, в течение долгого времени коаксиальный кабель использовался во всех типах обмена данными, что позволило хорошо изучить эту технологию.

Коаксиальный кабель бывает разной толщины. Как правило, с более толстым кабелем работать менее удобно. Об этом следует помнить, особенно если кабель надо будет протягивать по уже существующим коробам и желобам с ограниченным размером. Такой кабель так и называют — *толстым* (*thicknet*). Он достаточно жесткий из-за экрана и имеет оболочку желтого цвета. В некоторых ситуациях прокладка толстого кабеля весьма затруднительна, поэтому необходимо помнить, что чем сложнее среда передачи данных в установке, тем дороже сама

установка.

Неэкранированная витая пара

Кабель на основе неэкранированной витой пары (unshielded twisted-pair, UTP) используется во многих сетях и представляет собой четыре пары скрученных между собой проводов, при этом каждая пара изолирована от других (рис. 2.4).

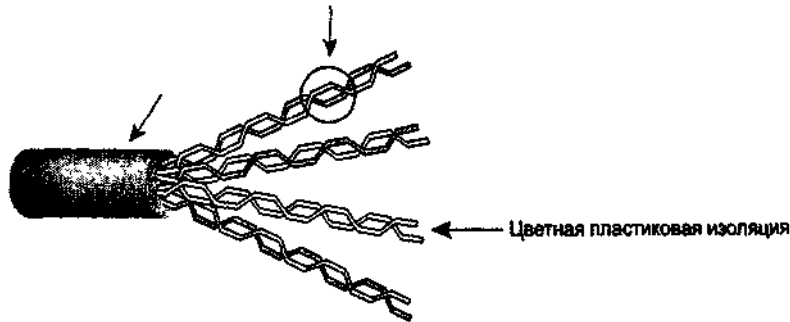


Рис. 2.4. Многие сети используют кабель UTP, который состоит из четырех пар проводов

Кабель UTP, применяемый в сетях передачи данных, имеет четыре пары медных проводов сортамента 22 или 24 и наружный диаметр около 0,17 дюйма (4,35 мм). Небольшой диаметр кабеля UTP дает определенные преимущества при прокладке. Поскольку неэкранированная витая пара может использоваться в большинстве сетевых архитектур, популярность ее продолжает расти.

Кабель UTP проще в установке и дешевле других типов сред передачи данных. Фактически удельная стоимость UTP на единицу длины меньше, чем у любого другого типа кабелей, использующихся в локальных сетях. Однако реальным преимуществом витой пары остается ее размер. Так как этот кабель имеет небольшой внешний диаметр, то он будет не так быстро заполнять сечение коробов, как другие виды кабелей. Этот фактор становится особенно важным, когда речь идет о прокладке сети в старых зданиях. Кроме того, на концах кабеля UTP, как правило, используется специальный разъем — RJ-коннектор (registered jack connector) (рис. 2.5).

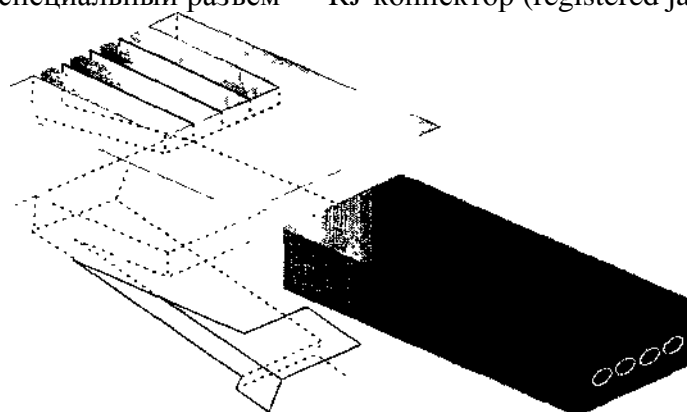


Рис. 2.5. UTP использует RJ-коннекторы

Первоначально RJ-коннектор применялся для подключения к телефонной линии, а сейчас используется в сетевых соединениях и гарантирует хорошее и надежное подключение. Следовательно, может быть существенно снижено количество потенциальных источников шума в сети.

Вообще говоря, кабель UTP более подвержен электрическим шумам и помехам, чем другие типы носителей. Одно время можно было сказать, что кабель UTP уступает в скорости передачи данных другим видам кабелей. Но сейчас это уже не так. Фактически, сегодня UTP является самой быстрой средой передачи данных на основе медных проводников. Однако, в случае использования кабеля UTP, расстояние между усилителями сигнала меньше, чем при использовании коаксиального кабеля.

Экранированная витая пара

Кабель на основе экранированной витой пары (shielded twisted-pair, STP) объединяет в себе методы экранирования и скручивания проводов. Предназначенный для использования в сетях передачи данных и правильно установленный STP-кабель по сравнению с UTP-кабелем имеет большую устойчивость к электромагнитным и радиочастотным помехам без существенного увеличения веса или размера кабеля.

Кабель STP имеет все преимущества и недостатки кабеля UTP, но он лучше защищает от всех типов внешних помех. Но кабель на основе экранированной витой пары дороже, чем на основе неэкранированной.

В отличие от коаксиального кабеля, в кабеле STP экран не является частью цепи передачи данных. Поэтому у кабеля должен быть заземлен только один конец. Обычно установщики заземляют кабель в концентраторе или в коммутационном шкафу, однако это не всегда легко сделать, особенно, если приходится использовать старые модели концентраторов, не приспособленные для кабеля STP. Неправильное заземление кабеля может стать основной причиной проблем в сети, поскольку в этом случае экран начинает работать как антенна, принимающая электрические сигналы от других проводов в кабеле и от внешних источников электрических шумов. И наконец, длина отрезков кабеля на основе экранированной витой пары без установки усилителей сигналов не может быть такой же большой, как при использовании других сред передачи данных.

Оптоволоконный кабель

Оптоволоконный кабель является средой передачи данных, которая способна проводить модулированный световой сигнал (рис. 2.6).

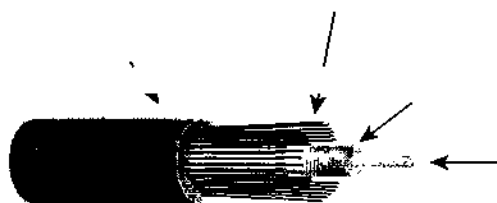


Рис. 2.6. Оптоволоконный кабель способен передавать модулированный световой сигнал

Оптоволоконный кабель невосприимчив к электромагнитным помехам и способен обеспечивать более высокую скорость передачи данных, чем кабели UTP, STP и коаксиальный кабель. В отличие от других сред передачи данных, имеющих в основе медные проводящие элементы, оптоволоконный кабель не проводит электрические сигналы. Вместо этого в оптоволоконном кабеле соответствующие битам сигналы заменяются световыми импульсами. Своими корнями оптоволоконная связь уходит в изобретениях, сделанных еще в XIX веке. Но только в 1960-х годах с появлением твердотельных лазерных источников света и высококачественного беспримесного стекла она начала активно применяться на практике. Широкое распространение оптоволоконный кабель получил благодаря телефонным компаниям, которые увидели его преимущества в междугородней связи.

Оптоволоконный кабель, используемый в сетях передачи данных, состоит из двух стекловолокон, заключенных в отдельные оболочки. Если посмотреть на кабель в поперечном сечении, то можно увидеть, что каждое стекловолокно окружено слоем отражающего покрытия, затем следует слой из пластмассы, имеющей название *кевлар (Kevlar)* (защитный материал, обычно использующийся в пуленепробиваемых жилетах), и дальше идет внешняя оболочка. Внешняя оболочка обычно делается из пластика и служит для защиты всего кабеля. Она отвечает требованиям соответствующих противопожарных и строительных норм.

Назначение кевлара состоит в том, чтобы придать кабелю дополнительные упругие свойства и предохранить от механического повреждения хрупкие толщиной в человеческий волос стекловолоконка. Если требуется прокладка кабеля под землей, то иногда для придания дополнительной жесткости в его конструкцию вводят провод из нержавеющей стали.

Светопроводящими элементами оптоволоконного кабеля являются *центральная жила* и *светоотражающее покрытие*. Центральная жила — это обычно очень чистое стекло с высоким коэффициентом преломления. Если центральную жилу окружить покрытием из стекла или пластмассы с низким коэффициентом преломления, то свет может как бы захватываться центральной жилой кабеля. Этот процесс называется *полным внутренним отражением* и позволяет оптопроводящему волокну играть роль световода и проводить свет на огромные расстояния, даже при наличии изгибов.

Кроме того, что оптоволоконный кабель устойчив к электромагнитным помехам, он также не подвержен влиянию и радиочастотных помех. Благодаря отсутствию внутренних и внешних шумов сигнал может проходить по оптоволоконному кабелю большее расстояние, чем в любых других средах передачи данных. Поскольку электрические сигналы не используются, оптоволоконный кабель является идеальным решением для соединения зданий, имеющих разное электрическое заземление. Принимая во внимание, что длинные пролеты медного кабеля между зданиями могут быть местом попадания ударов молнии, использование оптоволоконка в этой ситуации также более удобно.

Кроме того, подобно кабелю УТР, оптоволоконный кабель имеет небольшой диаметр, и он относительно плоский и похож на шнур от лампы. Поэтому в один желоб легко помещается несколько оптоволоконных кабелей. Таким образом, этот носитель является идеальным решением для старых зданий с ограниченным пространством.

Оптоволоконный кабель дороже и сложнее в установке, чем другие носители. Так как разъемы для этого кабеля представляют собой оптические интерфейсы, то они должны быть идеально плоско отполированными и не иметь царапин. Таким образом, установка может оказаться достаточно сложной. Обычно даже тренированному монтажнику для создания одного соединения требуется несколько минут. Все это может существенно повысить почасовую стоимость работы, и при создании крупных сетей стоимость работ может стать неприемлемо высокой.

Выбор типа среды передачи данных

Различные критерии, такие как скорость передачи данных и стоимость, помогают определить наиболее подходящую среду передачи данных. Тип материала, используемого в сети для обеспечения соединений, определяет такие параметры, как скорость передачи данных и их объем. Другим фактором, влияющим на выбор типа среды передачи данных, является ее стоимость.

Для достижения оптимальной производительности необходимо добиться, чтобы сигнал при движении от одного устройства к другому как можно меньше затухал. Причиной затухания сигнала может быть несколько факторов. Как будет показано далее, во многих носителях используется экранирование и применяются технические решения, предотвращающие ослабление сигнала. Однако использование экранирования становится причиной увеличения стоимости и диаметра кабеля, а также приводит к усложнению его прокладки.

Кроме того, в сетевых средах передачи данных могут использоваться различные типы оболочек. Оболочка, являясь внешним покрытием кабеля, обычно изготавливается из пластика, нелипкого покрытия или композитного материала. При проектировании локальной сети следует

помнить, что кабель, проложенный между стенами, в шахте лифта или проходящий по воздуховоду системы вентиляции, может стать факелом, способствующим распространению огня из одной части здания в другую. Кроме того, пластиковая оболочка в случае ее возгорания может стать причиной возникновения токсичного дыма. Для исключения подобных ситуаций существуют соответствующие строительные нормы, нормы пожарной безопасности и нормы техники безопасности, которые определяют типы оболочек кабелей, которые могут использоваться. Поэтому при определении типа среды передачи данных для использования при создании локальной сети следует (наряду с такими факторами, как диаметр кабеля, его стоимость и сложность прокладки) также учитывать и эти нормы.

Для лучшего понимания концепции выбора носителя можно представить два города, расположенных в нескольких милях друг от друга и соединенных двумя дорогами. Одна дорога имеет небольшую ширину и дешевое покрытие. Для примера можно взять однополосную дорогу с гравийным покрытием. Другая дорога — значительно шире и покрыта дорогостоящим материалом, например четырехполосная автострада с покрытием из армированного бетона.

Если планируется совершить утреннюю экскурсию из города А в город В, то скорее всего будет выбрана однополосная гравиевая дорога; с другой стороны, если необходимо доставить критического больного из города А в больницу города В, то использовать эту дорогу было бы безрассудством. Ведь более быстрая, гладкая и широкая автострада значительно лучше приспособлена для потребностей скорой помощи.

Эти города напоминают два соединенных компьютера, а дороги — сетевые носители, работающие на физическом уровне. Как в примере с городами и дорогами, тип соединительных материалов, используемых при создании сети, определяет объем и скорость передачи данных.

Канальный уровень

Как было сказано в главе 1, "Организация сети и эталонная модель OSI", все данные в сети отправляются источником и движутся в направлении получателя. К тому же, было определено, что функцией физического уровня является передача данных. После того как данные отправлены, канальный уровень эталонной модели OSI обеспечивает доступ к сетевой среде передачи данных и физическую передачу в среде, позволяющей данным определять местоположение адресата в сети. Также канальный уровень отвечает за выдачу сообщений об ошибках, учет топологии сети и управление потоком данных.

В эталонной модели OSI канальный и физический уровни являются смежными. Как было сказано в главе 1, "Организация сети и эталонная модель OSI", канальный уровень обеспечивает надежный транзит данных через физический уровень. Этот уровень использует адрес *управления доступом к среде передачи данных (Media Access Control, MAC)*. Как было сказано ранее, канальный уровень решает вопросы физической адресации (в противоположность сетевой или логической адресации), топологии сети, дисциплины линий связи (каким образом конечной системе использовать сетевой канал), уведомления об ошибках, упорядоченной доставки кадров и управления потоком информации. Кроме того, канальный уровень использует MAC-адрес в качестве средства задания аппаратного или канального адреса, позволяющего нескольким станциям коллективно использовать одну и ту же среду передачи данных и одновременно уникальным образом идентифицировать друг друга. Для того чтобы мог осуществляться обмен пакетами данных между физически соединенными устройствами, относящимися к одной локальной сети, каждое устройство-отправитель должно иметь MAC-адрес, который оно может использовать в качестве адреса пункта назначения.

MAC-адреса

Каждый компьютер, независимо от того, подключен он к сети или нет, имеет уникальный физический адрес. Не существует двух одинаковых физических адресов. Физический адрес (или MAC-адрес) зашит на плате *сетевой адаптера* (рис. 2.7).



Рис 2.7. Физический адрес компьютера зашит на плате сетевого адаптера

Таким образом, в сети именно плата сетевого адаптера подключает устройство к среде передачи данных. Каждая плата сетевого адаптера, который работает на канальном уровне эталонной модели OSI, имеет свой уникальный MAC-адрес.

В сети, когда одно устройство хочет переслать данные другому устройству, оно может установить канал связи с этим другим устройством, воспользовавшись его MAC-адресом. Отправляемые источником данные содержат MAC-адрес пункта назначения. По мере продвижения пакета в среде передачи данных сетевые адаптеры каждого из устройств в сети сравнивают MAC-адрес пункта назначения, имеющийся в пакете данных, со своим собственным физическим адресом. Если адреса не совпадают, сетевой адаптер игнорирует этот пакет, и данные продолжают движение к следующему устройству.

Если же адреса совпадают, то сетевой адаптер делает копию пакета данных и размещает ее на канальном уровне компьютера. После этого исходный пакет данных продолжает движение по сети, и каждый следующий сетевой адаптер проводит аналогичную процедуру сравнения.

Сетевые адаптеры

Сетевые адаптеры преобразуют пакеты данных в сигналы для передачи по сети. В ходе изготовления фирмой-производителем каждому сетевому адаптеру присваивается физический адрес, который заносится в специальную микросхему, устанавливаемую на плате адаптера. В большинстве сетевых адаптеров MAC-адрес зашивается в ПЗУ. Когда адаптер инициализируется, этот адрес копируется в оперативную память компьютера. Поскольку MAC-адрес определяется сетевым адаптером, то при замене адаптера изменится и физический адрес компьютера; он будет соответствовать MAC-адресу нового сетевого адаптера.

Для примера можно представить себе гостиницу. Предположим далее, что комната 207 имеет замок, открывающийся ключом А, а комната 410 — замок, открывающийся ключом F. Принято решение поменять замки в комнатах 207 и 410. После замены ключ А будет открывать комнату 410, а ключ F — комнату 207. В этом примере замки играют роль сетевых адаптеров, а ключи — роль MAC-адресов. Если адаптеры поменять местами, то изменятся и MAC-адреса.

Резюме

- Функцией физического уровня является передача данных.
- Для соединения компьютеров может использоваться несколько типов сред передачи данных.
 - Коаксиальный кабель, состоящий из внешнего цилиндрического пустотелого проводника, окружающего единственный внутренний провод.
 - Неэкранированная витая пара, используемая во многих сетях и представляющая собой четыре пары скрученных между собой проводов.
 - Экранированная витая пара, которая объединяет методы экранирования, подавления помех и скручивания проводов.
 - Оптоволоконный кабель, являющийся носителем, который способен проводить модулированный световой сигнал.
- Для определения наиболее подходящего типа среды передачи данных могут использоваться различные критерии, например скорость передачи данных и стоимость.
- Канальный уровень эталонной модели OSI обеспечивает доступ к среде передачи данных и саму физическую передачу данных, при которой данные имеют возможность определять

местоположение получателя в сети.

- Канальный уровень обеспечивает надежный транзит данных через физический канал связи. Этот уровень использует MAC-адрес — физический адрес, информация о котором находится на плате сетевого адаптера.
- Сетевые адаптеры преобразуют пакеты данных в сигналы, которые и посылают в сеть. Каждому адаптеру физический адрес присваивается фирмой-производителем.

Контрольные вопросы

1. Как называются все материалы, обеспечивающие физические соединения в сети?
 - A. Среда приложений.
 - B. Среда обучения.
 - C. Среда передачи данных.
 - D. Системная среда.
2. Какое преимущество имеет использование в сетях оптоволоконного кабеля?
 - A. Дешевизна.
 - B. Простота установки.
 - C. Это — промышленный стандарт, и он имеется в продаже в любом магазине, торгующем электронными устройствами.
 - D. Скорость передачи данных по оптоволоконному кабелю выше, чем по кабелю с витой парой и коаксиальному кабелю.
3. Какое из приведенных ниже определений наилучшим образом описывает понятия *среда передачи данных*?
 - A. Кабели и провода, по которым перемещаются данные.
 - B. Различные физические среды, пригодные для передачи сигналов.
 - C. Компьютерные системы и провода, образующие сеть.
 - D. Любые сетевые аппаратные и программные средства.
4. В каком виде информация хранится в компьютере?
 - A. В виде десятичных чисел.
 - B. В виде двоичных чисел.
 - C. В виде электронов.
 - D. В виде слов и рисунков.
5. Какой номер имеет канальный уровень в эталонной модели OSI?
 - A. 1.
 - B. 2.
 - C. 3.
 - D. 4.
6. Какое из приведенных ниже описаний канального уровня эталонной модели OSI является наилучшим?
 - A. Передает данные другим уровням.
 - B. Обеспечивает услуги прикладным процессам.
 - C. Принимает слабый сигнал, очищает его, усиливает и отправляет дальше в сеть.
 - D. Обеспечивает надежную передачу данных по физическому каналу.
7. К какому уровню эталонной модели OSI относится сетевой адаптер?
 - A. К канальному.
 - B. К физическому.
 - C. К транспортному.
 - D. К уровню представлений.
8. Как по-другому называется MAC-адрес?
 - A. Двоичный адрес.
 - B. Восьмеричный адрес.
 - C. Физический адрес.
 - D. Адрес TCP/IP.

9. Для чего служит сетевой адаптер?
- A. Устанавливает, управляет и прекращает сеансы между приложениями и осуществляет управление обменом данными между объектами уровня представлений.
 - B. Дает компьютерным системам возможность осуществлять двунаправленный обмен данными по сети.
 - C. Оказывает услуги прикладным процессам.
 - D. Предоставляет средства для установления, поддержания и закрытия виртуальных каналов, обнаружения ошибок передачи, восстановления и управления потоком информации.
10. Каким образом отправитель указывает местонахождение получателя в сети?
- A. Сетевой адаптер получателя идентифицирует свой MAC-адрес в пакете данных.
 - B. Пакет данных останавливается в пункте назначения.
 - C. Сетевой адаптер получателя посылает свой MAC-адрес источнику.
 - D. Источник посылает уникальный пакет данных по каждому MAC-адресу в сети.

Глава 3

Сетевые устройства

В этой главе

- Сетевые устройства
- Узлы
- Повторители
- Сигналы
- Концентраторы
- Фильтры
- Порты
- Домены
- Мосты
- Маршрутизаторы

Введение

В главе 2, "Физический и канальный уровни", были рассмотрены сетевые функции, которые выполняются на физическом и канальном уровнях эталонной модели OSI. Были также рассмотрены различные типы сред передачи данных, используемых на физическом уровне. В качестве таковых могут использоваться экранированная и неэкранированная витая пара, коаксиальный и оптоволоконный кабели. Также были изучены процессы, которые происходят в среде передачи данных на канальном уровне эталонной модели OSI. В частности, каким образом данные определяют местонахождение требуемого пункта назначения в сети.

Также говорилось, что если одно устройство хочет отправить данные другому устройству, то оно может установить связь этим устройством, используя его адрес доступа к среде передачи данных (MAC-адрес). Перед отправкой в сеть источник прикрепляет к отправляемым данным MAC-адрес требуемого получателя. По мере движения данных по носителю сетевые адаптеры (NIC) каждого устройства в сети сравнивают свой MAC-адрес с физическим адресом, содержащимся в пакете данных. Если эти адреса не совпадают, сетевой адаптер игнорирует пакет данных и пакет продолжает движение по сети к следующему узлу. Если же адреса совпадают, сетевой адаптер делает копию пакета данных и размещает ее на канальном уровне компьютера. После этого исходный пакет данных продолжает движение по сети, и каждый следующий сетевой адаптер проводит аналогичную процедуру сравнения.

Хотя подход, при котором данные отправляются каждому устройству в сети, оправдывает себя для сравнительно небольших сетей, легко заметить, что с увеличением сети возрастает трафик. Это может стать серьезной проблемой, поскольку в один момент времени в кабеле может находиться только один пакет данных. Если же все устройства в сети объединяются одним кабелем, такой подход приводит к замедлению движения потока данных по сети.

В этой главе будет рассмотрено, как с помощью сетевых устройств можно управлять величиной трафика в сети и повысить скорость потока данных.

Сетевыми устройствами называются аппаратные средства, используемые для объединения сетей. По мере увеличения размеров и сложности компьютерных сетей усложняются и сетевые устройства, которые их соединяют.

Однако все сетевые устройства служат для решения одной или нескольких общих задач:

- Увеличивают число узлов, подключаемых к сети. *Узлом* называется конечная точка сетевого соединения или общая переходная точка двух или более линий в сети. Узлами могут быть процессоры, контроллеры или рабочие станции. Они отличаются способом маршрутизации и другими возможностями; они могут соединяться линиями связи и служат точками управления сети. Термин "узел" иногда используется в более широком смысле для обозначения любого объекта, имеющего доступ к сети, и часто применяется в качестве синонима термина "устройство".
- Увеличивают расстояние, на которое может простирается сеть.
- Локализуют трафик в сети.
- Могут объединять существующие сети.
- Изолируют сетевые проблемы, делая их диагностику более простой.

На рис. 3.1 представлены символы следующих сетевых устройств: повторителя, концентратора, моста и маршрутизатора. Все эти устройства будут рассмотрены в данной главе.



Рис 3.1 К сетевым устройствам относятся повторители, концентраторы, мосты и маршрутизаторы

Повторители

Подобно средам передачи данных, *повторители* относятся к уровню 1 (физическому) эталонной модели OSI. Чтобы понять, как работает повторитель, необходимо учесть, что данные перед отправкой в сеть преобразуются в последовательность электрических или световых импульсов, которые и перемещающихся в среде передачи данных. Эти импульсы называются *сигналами*. Когда сигналы покидают передающую станцию, они четкие и легко распознаются. Однако чем длиннее кабель, тем сильнее затухает и ухудшается сигнал. В конце концов, это приводит к тому, что сигнал уже не может быть правильно распознан. Например, спецификации для витой пары категории 5 кабеля Ethernet устанавливают расстояние 100 метров как максимально допустимое для прохождения сигнала. Если сигнал проходит по сети больше указанного расстояния, то нет гарантии, что сетевой адаптер правильно распознает сигнал. Если такая проблема возникает, ее можно легко решить с помощью повторителя.

Использование повторителей для увеличения протяженности сети

Повторители позволяют увеличить протяженность сети, гарантируя при этом, что сигнал будет распознан принимающими устройствами. Повторители принимают ослабленный сигнал, очищают его от помех, усиливают и отправляют дальше в сеть, тем самым увеличивая расстояния, на которых сеть может функционировать.

Для примера представим болельщика, находящегося на стадионе во время футбольного матча. Он голоден. В соседнем секторе он видит продавца арахиса и пытается выяснить цену. Однако продавец находится слишком далеко и не может разобрать слов. Болельщик снова повторяет свой вопрос. В этот момент человек, сидящий на полпути между болельщиком и продавцом, слышит вопрос и передает его продавцу. Поскольку человек находится недалеко от продавца и повторяет сообщение достаточно громко, продавец без труда может расслышать вопрос. В этой аналогии человек, сидящий между болельщиком и продавцом арахиса, играет роль повторителя, а сообщение болельщика — роль сигнала, движущегося по носителю.

Использование повторителей для увеличения числа узлов сети

При организации сетей общей проблемой является слишком большое количество устройств, подключаемых к сети. Сигналы ухудшаются и становятся более слабыми, поскольку каждое устройство, подключенное к сети, становится причиной небольшого ослабления сигнала. Более того, так как сигнал проходит через слишком большое количество рабочих станций или узлов, он может оказаться настолько ослабленным, что принимающее устройство не сможет его распознать. Как было сказано в предыдущем разделе, решить эту проблему можно с помощью повторителя. Повторители принимают ослабленный сигнал, очищают его от помех, усиливают и отправляют дальше в сеть. Благодаря этому появляется возможность увеличить число узлов в сети.

В качестве примера представим мальчика Майкла, который хочет принести мороженое своему другу Тому. День выдался очень жаркий, а Майкл должен пронести мороженое больше мили от своего дома до школы, где его ожидает Том. К тому времени, когда Майкл добирается до школы, мороженое полностью растаивает. И когда он хочет отдать подарок Тому, от мороженого осталась уже только одна палочка, и в результате Том уже не может узнать, что ему хотели вручить.

Следующий день тоже выдался жарким. Майкл вышел из дома, чтобы отнести мороженое своему другу Тому. Пройдя квартал, он замечает, что мороженое начинает таять. Чтобы не дать мороженому растаять полностью, Майкл останавливается возле холодильника, расположенного

на углу, и помещает в него мороженое. После того как мороженое охладилось, Майкл снова может продолжить путь. Таким образом, останавливаясь возле каждого холодильника, Майклу удастся доставить мороженое адресату. Естественно, теперь Том легко узнает, что ему принесли, и может с удовольствием насладиться угощением.

Концентраторы

В локальных сетях каждая станция подключается с помощью некоей передающей среды. Как правило, у каждого файл-сервера имеется только один сетевой адаптер. Как результат, непосредственное подключение всех рабочих станций к файл-серверу невозможно. Чтобы решить эту проблему, в сетях используются концентраторы, которые являются наиболее распространенными сетевыми устройствами.

Вообще говоря, термин *концентратор* используется вместо термина *повторитель*, когда речь идет об устройстве, которое служит центром сети (рис. 3.2). Ниже перечислены наиболее важные особенности концентраторов:

- § усиливают сигналы;
- § распространяют сигналы в сети;
- § не выполняют фильтрацию;
- § не занимаются маршрутизацией и коммутацией;
- § используются как точки концентрации в сети.

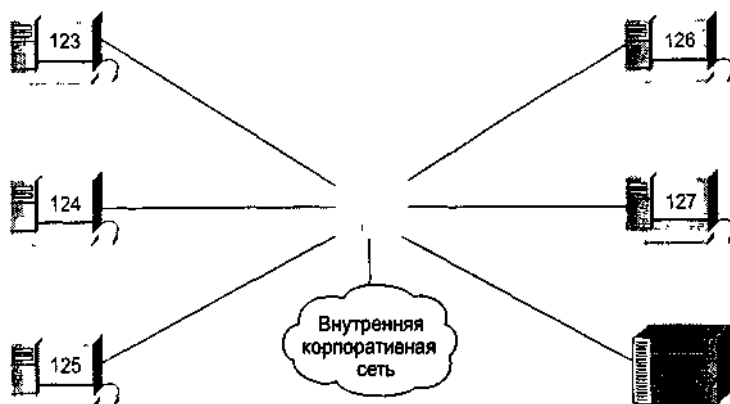


Рис. 3.2. Концентратор — наиболее распространенное сетевое устройство, которое служит центром сети

Концентратор можно представить себе в виде устройства, которое содержит множество независимых, но связанных между собой модулей сетевого оборудования.

В локальных сетях концентраторы ведут себя как мультипортовые повторители. В таких случаях концентраторы используются, чтобы разделить сетевые носители и обеспечить множественное подключение.

Недостатком использования концентратора является то, что он не может фильтровать сетевой трафик. *Фильтрацией* называется процесс, в ходе которого в сетевом трафике контролируются определенные характеристики, например, адрес источника, адрес получателя или протокол, и на основании установленных критериев принимается решение — пропускать трафик дальше или игнорировать его. В концентраторе данные, поступившие на один порт, передаются дальше на все порты. Следовательно, концентратор передает данные во все участки или сегментам сети, независимо от того, должны они туда направляться или нет.

Если имеется только один кабель, связывающий все устройства в сети, или если сегменты сети связаны только нефилтующими устройствами (например, концентраторами), несколько пользователей могут попытаться послать данные в один и тот же момент времени. Если одновременно пытаются передавать несколько узлов, то возникает *конфликт*. В этом случае

данные от разных устройств сталкиваются друг с другом и повреждаются. Область сети, в пределах которой сформировался пакет данных и возник конфликт, называют *доменом конфликта*. Одним из методов решения проблемы слишком большого трафика и большого числа конфликтов в сети является использование мостов.

Мосты

Мосты работают на уровне 2 (канальном) эталонной модели OSI и не занимаются исследованием информации от верхних уровней. Назначение мостов состоит в том, чтобы устранить ненужный трафик и уменьшить вероятность возникновения конфликтов. Это достигается путем разделения сети на сегменты и за счет фильтрации трафика по пункту назначения или MAC-адресу.

Мосты фильтруют трафик только по MAC-адресу, поэтому они могут быстро пропускать трафик, представляющий любой протокол сетевого уровня. Так как мосты проверяют только MAC-адрес, протоколы не имеют для них значения. Как следствие, мосты отвечают только за то, чтобы пропускать или не пропускать пакеты дальше, основываясь при этом на содержащихся в них MAC-адресах. Можно выделить следующие наиболее важные особенности мостов.

- Они более интеллектуальны, чем концентраторы, т.е. могут анализировать входящие пакеты и пропускать (или не пропускать) их дальше на основании адресной информации.
- Принимают и пропускают пакеты данных между двумя сетевыми сегментами.
- Управляют широковещательными пакетами в сети.
- Имеют и ведут внутренние таблицы адресов.

Пример использования моста показан на рис. 3.3.

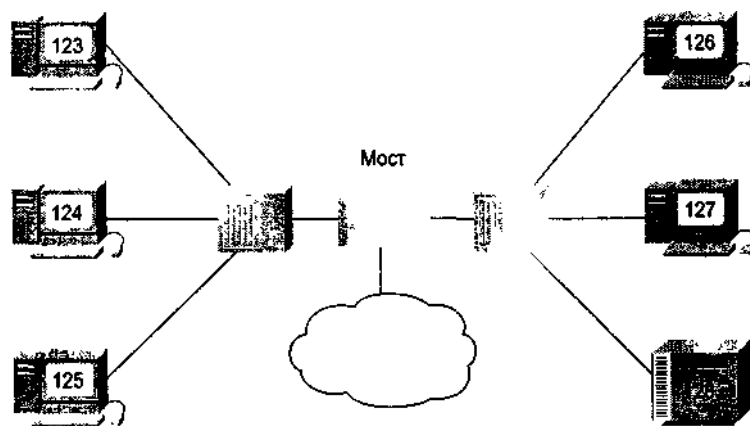


рис. 3.3. Мост может использоваться для соединения сегментов сети

Представим, что госпожа Джонс имеет в своем классе 30 учащихся. Она знает, в каком клубе состоит каждый ученик, так как эта информация содержится в классном журнале рядом с фамилией каждого ученика. Каждый понедельник преподаватели получают список объявлений клубов и оглашают его перед учащимися. В этот понедельник госпожа Джонс обнаружила, что все объявления предназначены только для членов туристического клуба. Сверившись с классным журналом, она увидела, что в ее классе нет членов этого клуба. Поэтому госпожа Джонс не стала зачитывать объявления туристического клуба своим ученикам.

В этой аналогии госпожа Джонс играет роль моста, так как она фильтрует сообщения и принимает решение о зачитывании объявлений на основании информации о членстве учеников в клубах. В этом примере информация о том, в каких клубах состоят ученики, имеет тот же смысл, что и MAC-адреса, используемые мостами.

Чтобы фильтровать и, соответственно, выборочно пропускать сетевой трафик, мосты строят

таблицы соответствия всех MAC-адресов, находящихся в сети и других сетях.

При поступлении данных на вход моста он сравнивает адрес получателя, содержащийся в пакете данных, с MAC-адресами в своей таблице. Если мост обнаружит, что MAC-адрес пункта назначения данных расположен в том же сегменте сети, что и отправитель, то он не пропустит данные в другой сегмент (рис. 3.4).

Если же мост обнаружит, что MAC-адрес получателя данных не относится к тому же сегменту сети, что и адрес отправителя, то мост пропустит данные во все остальные сегменты сети (рис. 3.5). Поэтому мосты могут существенно уменьшать трафик между сетевыми сегментами, устранив ненужный трафик.

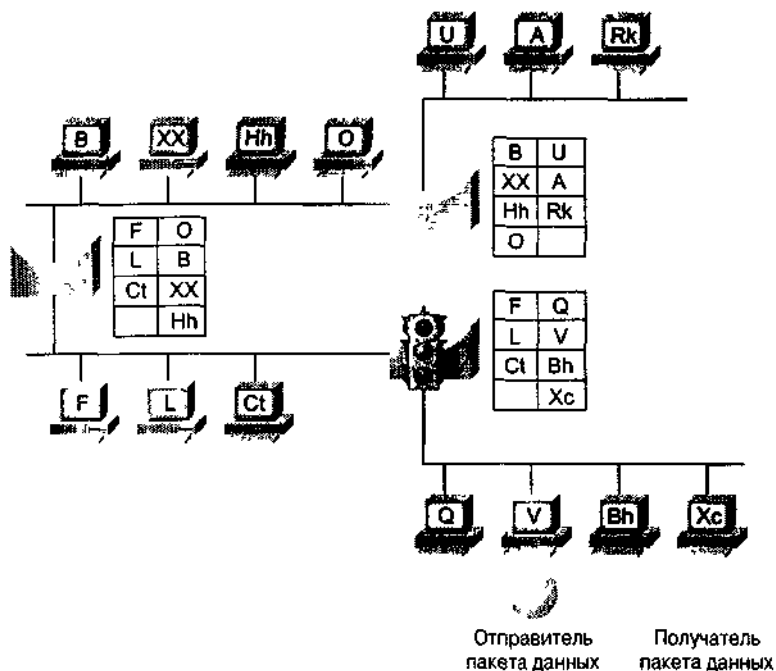


Рис 3.4. Мосты не пропускают данные в другие сегменты сети, если MAC-адреса отправителя и получателя относятся к одному сегменту. В этом примере пакет данных порождается компьютером V и имеет пунктом назначения компьютер Xc

Маршрутизаторы

Другим типом устройств межсетевого взаимодействия являются маршрутизаторы. Как было сказано выше, мосты прежде всего используются для соединения сегментов сети. Маршрутизаторы же используются для объединения отдельных сетей и для доступа к Internet.

Они обеспечивают сквозную маршрутизацию при прохождении пакетов данных и маршрутизацию трафика между различными сетями на основании информации сетевого протокола или уровня 3 и способны принимать решение о выборе оптимального маршрута движения данных в сети (рис 3.6). С помощью маршрутизаторов также может быть решена проблема чрезмерного широковещательного трафика, так как они не переадресовывают дальше широковещательные кадры, если им это не предписано.

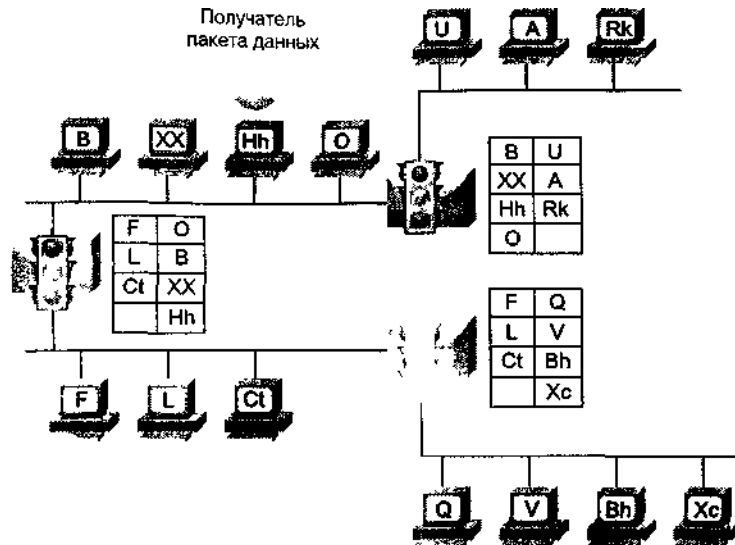


Рис 3 5 Мосты пропускают данные в другие сегменты сети, если MAC-адреса отправителя и получателя относятся к различным сегментам сети В этом примере пакет данных передается компьютером V и имеет пунктом назначения компьютер Hh.

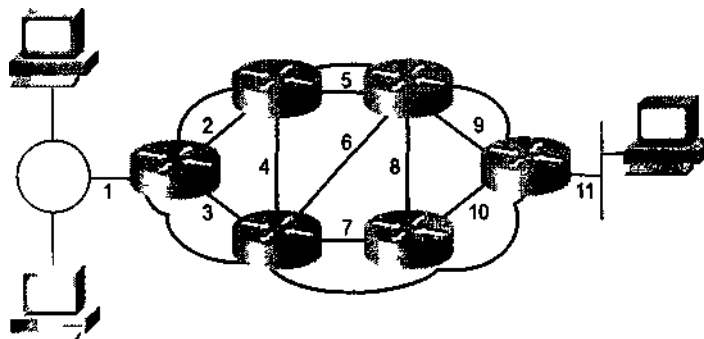


Рис 3 6 Маршрутизаторы используют уровень 3 для определения оптимального маршрута доставки данных в сети и помогают сдерживать объем широковещательных пакетов

Маршрутизаторы и мосты отличаются друг от друга в нескольких аспектах. Во-первых, мостовые соединения осуществляются на канальном уровне, в то время как маршрутизация выполняется на сетевом уровне эталонной модели OSI. Во-вторых, мосты используют физические или MAC-адреса для принятия решения о передаче данных. Маршрутизаторы для принятия решения используют различные схемы адресации, существующие на уровне 3. Они используют адреса сетевого уровня, также называемые логическими, или IP-адресами (*Internet Protocol*). Поскольку IP-адреса реализованы в программном обеспечении и соотносятся с сетью, в которой находится устройство, иногда адреса уровня 3 называют еще *протокольными* или *сетевыми адресами*. Физические или MAC-адреса обычно устанавливаются производителем сетевого адаптера и зашиваются в адаптере на аппаратном уровне; IP-адреса обычно назначаются сетевым администратором.

Чтобы маршрутизация была успешной, необходимо, чтобы каждая сеть имела уникальный номер. Этот уникальный номер сети включен в IP-адрес каждого устройства, подключенного к сети (рис 3 7, табл. 3.1)

Таблица 3.1. Адреса сетей и узлов

Адрес сети	Адрес узла
1	1
	2
	3

2	1
3	1

Рассмотрим уникальную сеть А с подключенными к ней четырьмя устройствами, IP-адреса которых — А1, А2, А3 и А4 (рис. 3.8). Поскольку интерфейс, с помощью которого маршрутизатор подключается к сети, является частью этой сети, порт, через который маршрутизатор подключается к сети А, будет иметь IP-адрес А5.

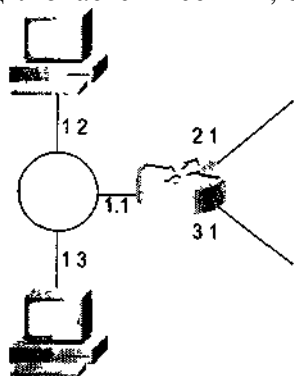


Рис 3 7. Уникальный номер сети включается в IP-адрес, который присваивается каждому узлу, подключенному к сети

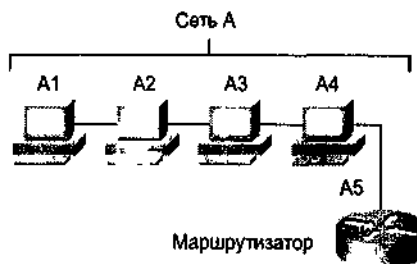


Рис 3 8 Сеть А с четырьмя подключенными к ней устройствами

Предположим теперь, что есть сеть В, содержащая четыре устройства, которая подключена к другому интерфейсу того же маршрутизатора (рис. 3.9) IP-адреса устройств в этой сети будут В1, В2, В3 и В4, а IP-адрес второго интерфейса маршрутизатора — В5.

Предположим далее, что данные были посланы из одной сети в другую.

Отправитель находится в сети А, получатель — в сети В, и к маршрутизатору подключены сети А, В, С и D Когда логически сгруппированный модуль информации, называемый *кадром (фреймом)*, достигает маршрутизатора, последний выполняет следующие функции.

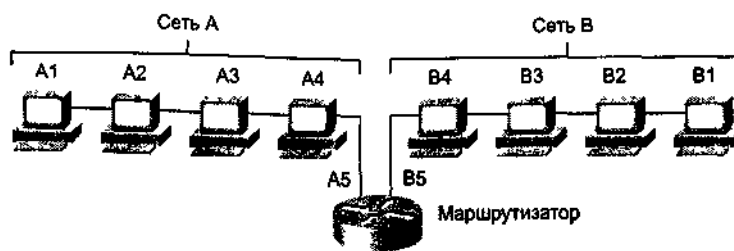


Рис. 3.9. Сеть В также содержит четыре устройства

1. Определяет и отбрасывает канальный заголовок и трейлер, которые содержатся в кадре. Канальным заголовком называется информация, которая прикрепляется к данным в ходе инкапсуляции и содержит MAC-адреса отправителя и получателя. Это позволяет маршрутизатору исследовать сетевой уровень, чтобы определить сеть адресата.
2. Сверяется со своей таблицей маршрутизации, которая содержит маршруты к конкретным сетям, и определяет порт, через который ему необходимо отправить данные, чтобы те добрались до сети пункта назначения.

Таким образом, в примере, показанном на рис. 3.10, маршрутизатор пошлет данные из Сети А в сеть В через порт с IP-адресом В5. Однако перед фактической отправкой данных из порта В5 маршрутизатор инкапсулирует данные в соответствующий канальный кадр.

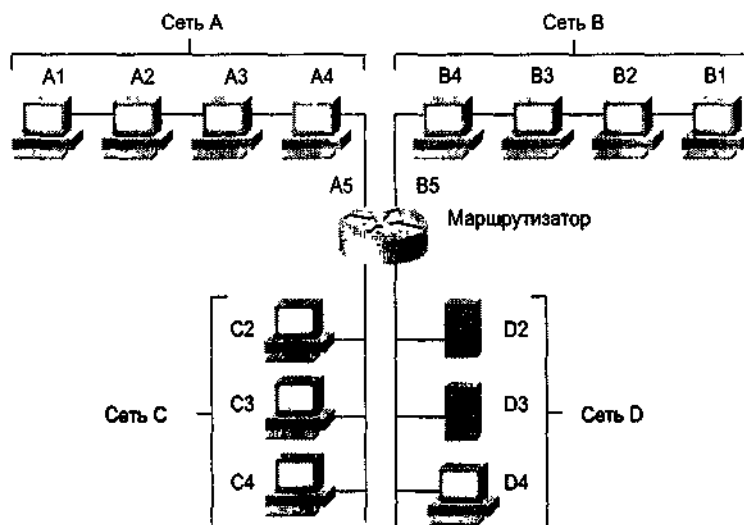


Рис. 3.10. Маршрутизатор определяет путь прохождения данных из сети А сеть В по IP-адресу В5

Резюме

- Сетевыми устройствами называются аппаратные средства, используемые для объединения сетей.
- Повторители принимают ослабленный сигнал, очищают его от помех, усиливают и отправляют дальше в сеть.
- Термин *концентратор* используется вместо термина *повторитель*, когда речь идет об устройстве, которое служит центром сети.
- Область сети, в пределах которой пакет данных порождается и вступает в конфликт, называется *доменом конфликтов*.
- Мосты устраняют лишний трафик и уменьшают вероятность возникновения конфликтов. Это достигается за счет разделения сети на сегменты и фильтрации трафика по адресу станции или MAC-адресу.
- Маршрутизаторы способны принимать интеллектуальные решения о выборе оптимального маршрута доставки данных в сети.

Контрольные вопросы

1. Для чего используются межсетевые устройства?
 - A. Позволяют увеличивать число узлов, протяженность сети и объединять отдельные сети.
 - B. Повышают скорость передачи данных и уменьшают уровень электромагнитных помех в зданиях.
 - C. Обеспечивают для сигнала резервные пути доставки, тем самым предотвращая его потерю и повреждение.
 - D. Позволяют объединять устройства во всем здании.
2. Какое из описаний узла является наилучшим?
 - A. Устройство, определяющее оптимальный маршрут движения трафика по сети.
 - B. Устройство, которое устанавливает, поддерживает и завершает сеансы между приложениями и управляет обменом данными между объектами уровня представлений.
 - C. Устройство, которое синхронизирует взаимодействующие приложения и согласует процедуры восстановления после ошибок и проверки целостности данных.
 - D. Конечная точка сетевого соединения или общий стык двух или более линий, который служит в качестве контрольной точки.
3. Какая из проблем может быть легко устранена с помощью повторителя?
 - A. ...
 - B. ...
 - C. ...
 - D. ...

- A. Слишком много типов несовместимого оборудования в сети.
 - B. Слишком большой трафик в сети.
 - C. Слишком низкая скорость передачи данных.
 - D. Слишком много узлов и/или недостаточно кабеля.
4. Какое из описаний сигнала является наилучшим?
- A. Электрические импульсы, представляющие данные.
 - B. Усиление данных.
 - C. Преобразование данных.
 - D. Официально установленные правила и процедуры.
5. Какой недостаток имеет использование концентратора?
- A. Не может увеличить рабочие расстояния в сети.
 - B. Не может фильтровать сетевой трафик.
 - C. Не может посылать ослабленный сигнал через сеть.
 - D. Не может усиливать ослабленные сигналы.
6. Какое из описаний конфликта в сети является наилучшим?
- A. Результат передачи данных в сеть двумя узлами независимо друг от друга.
 - B. Результат одновременной передачи данных в сеть двумя узлами.
 - C. Результат повторной передачи данных в сеть двумя узлами
 - D. Результат невыполнения передачи данных в сеть двумя узлами.
7. Какое описание термина "домен конфликтов" является наилучшим?
- A. Область сети, в которой распространяются конфликтующие пакеты данных.
 - B. Область сети, которая ограничивается мостами, маршрутизаторами или коммутаторами
 - C. Область сети, в которой установлены маршрутизаторы и концентраторы.
 - D. Область сети, в которой используется фильтрация.
8. Что происходит, если мост обнаруживает, что адрес назначения, содержащийся в пакете данных, находится в том же сегменте сети, что и источник?
- A. Он пересылает данные в другие сегменты сети.
 - B. Он не пропускает данные в другие сегменты сети.
 - C. Он пропускает данные между двумя сегментами сети.
 - D. Он пропускает пакеты между сетями, использующими различные протоколы.
9. Для чего служит маршрутизатор?
- A. Сравнивает информацию из таблицы маршрутизации с IP-адресом пункта назначения, содержащимся в пакете данных, и переправляет пакет в нужную подсеть и узел.
 - B. Сравнивает информацию из таблицы маршрутизации с IP-адресом пункта назначения, содержащимся в пакете данных, и переправляет пакет в нужную подсеть.
 - C. Сравнивает информацию из таблицы маршрутизации с IP-адресом пункта назначения, содержащимся в пакете данных, и переправляет пакет в нужную сеть.
 - D. Сравнивает информацию из таблицы маршрутизации с IP-адресом пункта назначения, содержащимся в пакете данных, и переправляет пакет в нужный сегмент сети.
10. Какое сетевое устройство способно решить проблему чрезмерного широкополосного трафика?
- A. Мост.
 - B. Маршрутизатор.
 - C. Концентратор.
 - D. Фильтр.

Глава 4

Локальные и глобальные сети

В этой главе..

- Функционирование локальных сетей (LAN)
- Поток данных в локальной сети, использующей стандарты Ethernet/802.3
- Общие задачи глобальных сетей (WAN)
- Главные компоненты WAN
- Общие методы канальной инкапсуляции, связанные с синхронными последовательными линиями связи

Введение

В главе 3, "Сетевые устройства", были рассмотрены сетевые устройства, которые могут быть использованы для фильтрации трафика в сети и уменьшения размеров доменов конфликтов, в пределах которых существует вероятность взаимного влияния пакетов друг на друга

В этой главе будут рассмотрены технологии локальных и глобальных сетей, стандарты и сетевые устройства, действующие на физическом, канальном и сетевом уровнях эталонной модели OSI

Локальные вычислительные сети

Локальные вычислительные сети (ЛВС) — это высокоскоростные сети с малым количеством ошибок, которые охватывают небольшие географические пространства (до нескольких тысяч метров) ЛВС объединяют рабочие станции, терминалы и периферийные устройства в одном здании или другой пространственно ограниченной области Локальные сети обеспечивают множеству подключенных настольных устройств (обычно ПК) доступ к среде передачи данных с высокой пропускной способностью Они подключают компьютеры и службы к общей среде уровня 1 К устройствам локальной сети относятся следующие устройства (рис 4 1)

- *Мосты* Подключают сегменты локальной сети и помогают фильтровать трафик
- *Концентраторы* Концентрируют соединения локальной сети и позволяют использовать в качестве среды передачи данных витую пару
- *Коммутаторы Ethernet* Обеспечивают сегментам и настольным системам полнодуплексную связь и выделенную полосу пропускания
- *Маршрутизаторы* Обеспечивают большое количество сервисов, включая организацию взаимодействия сетей и управление широковещанием

Наиболее распространенными технологиями ЛВС являются Ethernet, Fiber Distributed Data Interface (FDDI) и Token Ring, которые применяются практически во всех существующих локальных сетях (рис 4 2)

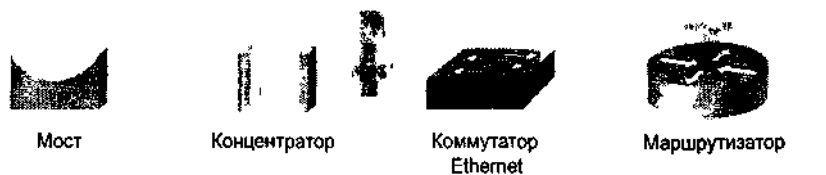


Рис 4 1 К устройствам локальных сетей относятся мосты, концентраторы, коммутаторы Ethernet и маршрутизаторы

Стандарты локальных сетей определяют вид кабельных систем и сигналы на физическом и канальном уровнях эталонной модели OSI В этой книге будут рассмотрены стандарты Ethernet и IEEE 802 3, так как именно в соответствии с этими стандартами работают большинство локальных сетей.

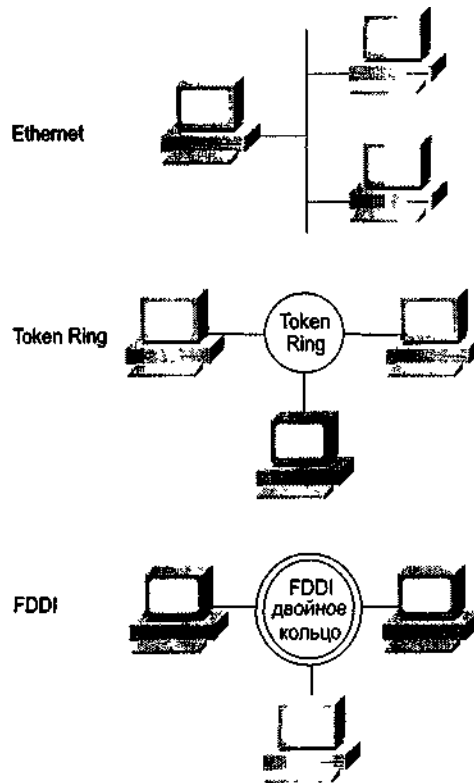


Рис. 4.2 Наиболее широко в локальных сетях используются технологии Ethernet, FDDI и Token Ring

Сетевые стандарты Ethernet и IEEE 802.3

Ethernet был разработан Исследовательским центром корпорации Xerox в Пало Альто (PARC) в 1970 году и является на сегодняшний день наиболее популярным стандартом. Миллионы устройств и узлов подключены к сетям, использующим Ethernet. Первым локальным сетям требовалась очень небольшая пропускная способность для выполнения простых сетевых задач, существовавших в то время, — отправка и прием электронной почты, передача файлов данных и обработка заданий по выводу на печать.

Ethernet стал основой для спецификации IEEE 802.3, которая была выпущена в 1980 году Институтом инженеров по электротехнике и электронике. Вскоре после этого компании Digital Equipment Corporation, Intel Corporation и Xerox Corporation совместно разработали и выпустили спецификацию Ethernet версии 2.0, которая была в значительной степени совместима со стандартом IEEE 802.3. На сегодняшний день Ethernet и IEEE 802.3 являются наиболее распространенными стандартами локальных вычислительных сетей.

Сети на основе Ethernet используются для транспортировки данных между различными устройствами — компьютерами, принтерами и файл-серверами. Технология Ethernet дает возможность устройствам коллективно пользоваться одними и теми же ресурсами, т.е. все устройства могут пользоваться одной средой доставки. *Средой доставки* называется метод передачи и приема данных. Например, рукописное письмо может быть послано с использованием различных способов доставки: через почтовую службу, через курьерскую службу доставки Federal Express или по факсу. Электронные данные могут передаваться по медному кабелю, по тонкому или толстому коаксиальному кабелю, по беспроводным линиям связи и т.д.

ЛВС и физический уровень

Ethernet должен был заполнить нишу между глобальными, низкоскоростными сетями и

специализированными сетями машинных залов, передающими данные с высокой скоростью, но на очень ограниченные расстояния. Ethernet хорошо подходит для приложений, когда локальные коммуникации должны выдерживать периодически возникающие высокие нагрузки на пиковых скоростях передачи данных.

Стандарты Ethernet и IEEE 802.3 определяют локальные сети с шинной топологией, работающие в монополосном режиме со скоростью передачи 10 Мбит/с. Такие ЛВС называют ЮBase. На рис. 4.3 показан вариант комбинирования трех существующих стандартов выполнения разводки в сетях.

- *10Base2*. Известен как тонкий Ethernet; допускает протяженность сетевых сегментов на коаксиальном кабеле до 185 метров.
- *10Base5*. Известен как толстый Ethernet; допускает протяженность сетевых сегментов на коаксиальном кабеле до 500 метров
- *10BaseT* Использует для передачи кадров недорогой кабель на основе витой пары.

Стандарты ЮBaseS и 10Base2 обеспечивают доступ нескольким станциям в одном сегменте ЛВС. Станции подключаются к сегменту с помощью кабеля, который одним концом соединяется с интерфейсом блока подключения (*attachment unit interface, AUI*) на станции, а другим — с трансивером, подключаемым к коаксиальному кабелю Ethernet. Трансивер еще называют *устройством подключения к среде передачи данных (media attachment unit, MAU)*

Поскольку стандарт ЮBaseT обеспечивает доступ только для одной станции, то в локальных сетях на базе ЮBaseT станции почти всегда подключаются к концентратору или сетевому коммутатору. При подобной конфигурации принято считать, что концентратор или сетевой коммутатор относится к тому же сегменту, что и подключенные к нему станции

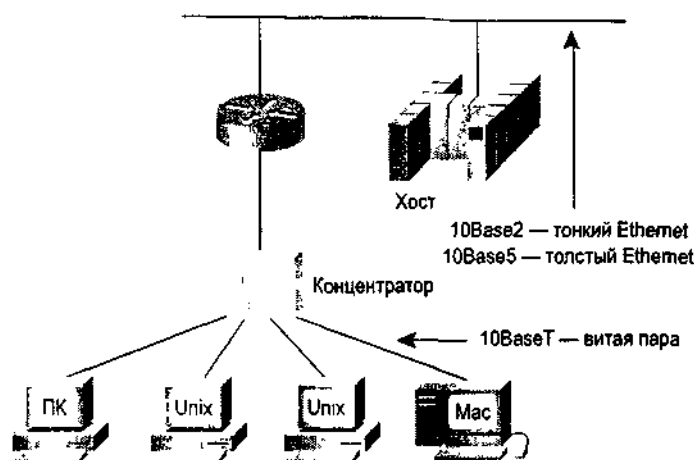


Рис. 4.3. Сеть может объединять в себе различные типы доступа, задаваемые стандартом Ethernet/802.3

ЛВС и канальный уровень

Канальные уровни протоколов Ethernet и 802.3 обеспечивают транспортировку данных по физическому каналу, непосредственно соединяющему два соединенных устройства. Например, как показано на рис. 4.4, три устройства могут напрямую быть связаны друг с другом с помощью сети Ethernet. Рядом с компьютером Macintosh (слева) и компьютером на базе процессора Intel (в центре на рисунке) указаны их *адреса управления доступом к среде передачи данных* (MAC-адреса), используемые канальным уровнем. Маршрутизатор, расположенный справа, также использует MAC-адреса каждого из своих сетевых интерфейсов. Для обозначения интерфейса маршрутизатора, работающего по протоколу 802.3, используется аббревиатура, принятая в *Межсетевой операционной системе корпорации Cisco (Cisco Interwork Operating System, IOS)*, — символ E, за которым указывается номер интерфейса. Например, E0 — это имя интерфейса 802.3 под номером 0 (см. рис. 4.4).

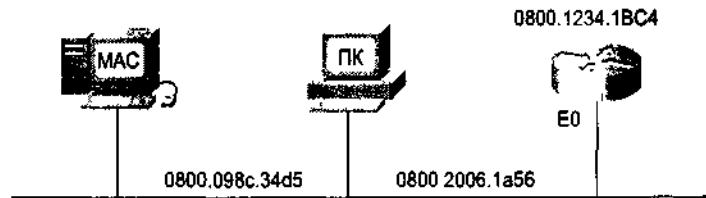


Рис. 4.4. В маршрутизаторах Cisco Ethernet/802.3-канал передачи данных использует интерфейс, название которого состоит из символа E и порядкового номера

Как работает сеть Ethernet/802.3

В сети Ethernet данные, посылаемые одним узлом, проходят через весь сегмент. По мере движения данные принимаются и анализируются каждым узлом. Когда сигнал достигает конца сегмента, он поглощается специальным оконечным элементом. Это необходимо для того, чтобы предотвратить движение сигнала в обратном направлении. В каждый отдельный момент времени в локальной сети возможна только одна передача. Например, в сети с линейной шинной топологией пакет данных передается от станции А к станции D (рис. 4.5). Этот пакет принимается всеми станциями. Станция D распознает свой адрес и обрабатывает кадр. Станции В и С не распознают свои MAC-адреса и игнорируют кадр.

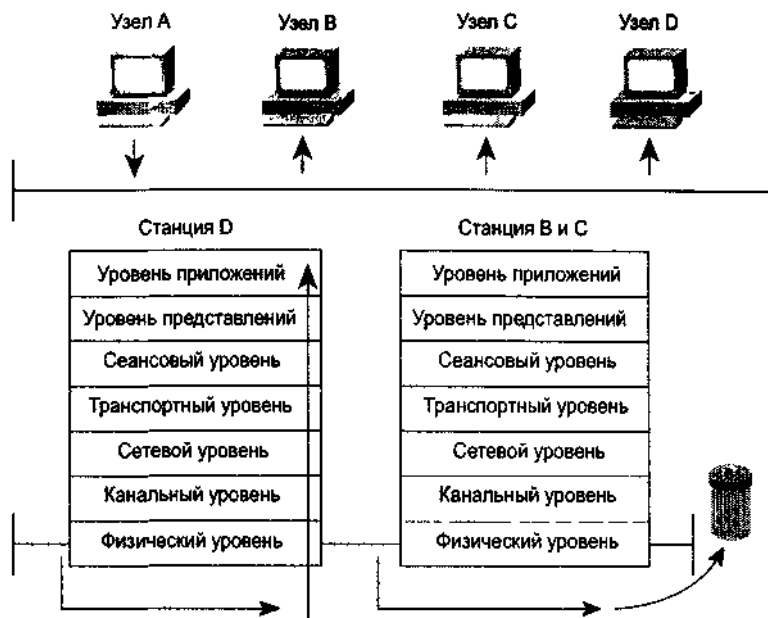


Рис. 4.5 Станция D распознает свой адрес и принимает кадр; станции В и С не распознают свой MAC-адреса и игнорируют его

Широковещание в сети Ethernet/802.3

Широковещание является мощным инструментом, который позволяет отправлять один кадр одновременно многим станциям. В режиме широковещания используется канальный адрес пункта назначения, состоящий из всех единиц (FFFF. FFFF. FFFF — в шестнадцатеричной системе). К примеру, если станция А передает кадр, используя в качестве адреса пункта назначения адрес, состоящий из всех единиц, то станции В, С и D должны принять этот кадр и передать его верхним Уровням для дальнейшей обработки (рис. 4.6). Широковещание может серьезно влиять на производительность станций, излишне отвлекая их. По этой причине широковещание должно применяться, только если MAC-адрес не известен или если данные предназначены для всех станций.

ЛВС и сетевой уровень

Технология Ethernet является *технологией коллективного использования среды передачи данных*. Это означает, что все устройства в сети должны следить за передачами в сети и конкурировать или договариваться о возможности, или праве, на передачу. Это также означает, что в один и тот же момент времени в сети возможна только одна передача. Имеется некоторое сходство между движением данных в сети и движением, которое происходит на автострате, где водители и их автомобили (устройства) договариваются об использовании автостраты (носителя), применяя при этом сигналы поворота, скорость и т.п., чтоб перевозить (передать) пассажиров (данные) из одного места в другое.



Рис. 4.6. Широковещание позволяет отправлять один кадр одновременно многим станциям, используя специальный канальный адрес пункта назначения

Как было сказано в главе 3, "Сетевые устройства", если более чем один узел пытается осуществить передачу, имеет место конфликт. Вследствие этого данные от разных устройств сталкиваются между собой и повреждаются. Если устройство обнаруживает, что имеет место конфликт, то его сетевой адаптер выдает сигнал повторной передачи с задержкой. Поскольку задержка перед повторной передачей определяется алгоритмом, величина этой задержки различна для каждого устройства в сети. Таким образом, вероятность повторного возникновения конфликта уменьшается. Однако, если трафик в сети очень напряженный, повторные конфликты приводят к повторным передачам с задержкой, что вызывает значительное замедление работы сети.

Множественный доступ с контролем несущей и обнаружением конфликтов

Сегодня термин *стандартный Ethernet* чаще всего применяется для описания всех ЛВС, использующих технологию Ethernet (технологию коллективного использования среды передачи данных), которая в общем случае удовлетворяет требованиям спецификаций Ethernet, включая спецификации стандарта IEEE 802.3. Чтобы использовать принцип коллективной работы со средой передачи данных, в Ethernet применяется протокол *множественного доступа с контролем несущей и обнаружением конфликтов* (*carrier sense multiple access/collision detection, CSMA/CD*),

Использование протокола CSMA/CD позволяет устройствам договариваться о правах на передачу.

CSMA/CD является методом доступа, который позволяет только одной станции осуществлять передачу в среде коллективного использования. Задачей стандарта Ethernet является обеспечение качественного сервиса доставки данных. Не все устройства могут осуществлять передачу на равных правах в течение всего времени, поскольку это может привести к возникновению конфликтов. Однако стандартные сети Ethernet, использующие протокол CSMA/CD, учитывают все запросы на передачу и определяют, какие устройства могут передавать в данный момент и в какой последовательности смогут осуществлять передачу все остальные устройства, чтобы все они получали адекватное обслуживание.

Перед отправкой данных узел "прослушивает" сеть, чтобы определить, можно ли осуществлять передачу, или сеть сейчас занята. Если в данный момент сеть никем не используется, узел осуществляет передачу. Если сеть занята, узел переходит в режим ожидания. Возникновение конфликтов возможно в том случае, если два узла, "прослушивая" сеть, обнаруживают, что она свободна, и одновременно начинают передачу. В этом случае возникает конфликт, данные повреждаются и узлам необходимо повторно передать данные позже. Алгоритмы задержки определяют, когда конфликтующие узлы могут осуществлять повторную передачу. В соответствии с требованиями CSMA/CD, каждый узел, начав передачу, продолжает "прослушивать" сеть на предмет обнаружения конфликтов, узнавая таким образом о необходимости повторной передачи.

Метод CSMA/CD работает следующим образом (рис. 4.7): если узел хочет осуществить передачу, он проверяет сеть на предмет того, не передает ли в данный момент другое устройство. Если сеть свободна, узел начинает процесс передачи. Пока идет передача, узел контролирует сеть, удостоверившись, что в этот же момент времени не передает никакая другая станция. Два узла могут начать передачу почти одновременно, если обнаружат, что сеть свободна. В этом случае возникает конфликт, что показано на рис. 4.7, вверху.

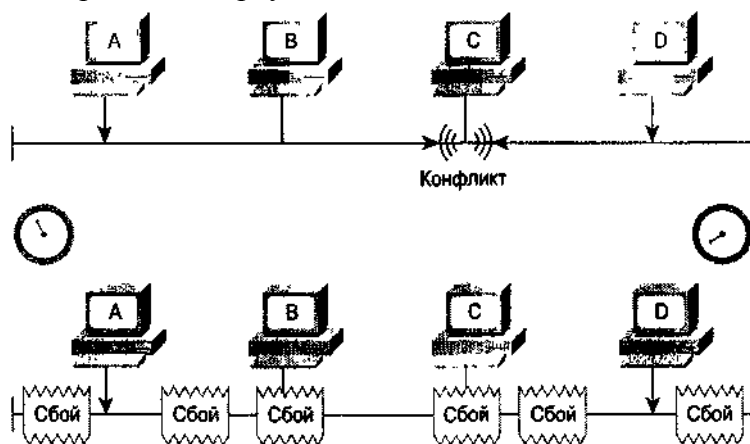


Рис. 4.7. Благодаря сигналу "Наличие конфликта" о возникающих конфликтах узнают все узлы сети

Когда передающий узел узнает о конфликте, он передает сигнал "Наличие конфликта", делающий конфликт достаточно долгим для того, чтобы его могли распознать все другие узлы сети. После этого все передающие узлы прекращают отправку кадров на выбираемый случайным образом отрезок времени, называемый *временем задержки повторной передачи*. По истечении этого периода осуществляется повторная передача. Если последующие попытки также заканчиваются неудачно, узел повторяет их до 16 раз, после чего отказывается от передачи.

Время задержки для каждого узла разное. Если различие в длительности этих периодов задержки достаточно велико, то повторную передачу узлы начнут уже не одновременно. С каждым последующим конфликтом время задержки удваивается, вплоть до десятой попытки, тем самым уменьшая вероятность возникновения конфликта при повторной передаче. С 10-й по 16-ю попытку узлы время задержки больше не увеличивают, поддерживая его постоянным.

Глобальные сети

Глобальные сети работают за пределами географических возможностей ЛВС, используя последовательные соединения различных типов для обеспечения связи в пределах значительных географических областей. Доступ к глобальным сетям обеспечивают региональные операторы, такие как Sprint и MCI. Операторы могут предоставлять круглосуточное или временное подключение к сети, а также доступ через последовательные интерфейсы, работающие с различными скоростями.

Устройства глобальных сетей

По определению, глобальные сети объединяют устройства, расположенные на большом удалении друг от друга. К устройствам глобальных сетей относятся следующие (рис. 4.8).

- *Маршрутизаторы*, обеспечивающие большое количество сервисов, включая организацию межсетевого взаимодействия и интерфейсные порты WAN.
- *Коммутаторы*, которые подключают полосу для передачи голосовых сообщений, данных и видео.
- *Модемы*, которые служат интерфейсом для голосовых сервисов; *устройства управления каналом/цифровые сервисные устройства (channel service units/digital service units, CSU/DSUs)*, которые являются интерфейсом для сервисов T1/E1; *терминальные адаптеры и оконечные сетевые устройства 1 (terminal adapter / network termination 1, TA/NT 1)*, которые служат интерфейсом для служб *цифровой сети с интеграцией услуг (Integrated Services Digital Network, ISDN)*.
- *Коммуникационные серверы (communication servers)*, которые концентрируют входящие и исходящие пользовательские соединения по коммутируемым каналам связи.

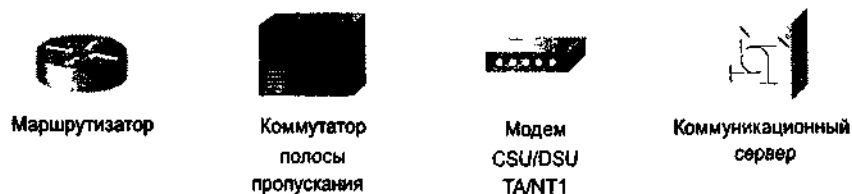


Рис. 4.8. Основными устройствами WAN являются маршрутизаторы, широкополосные коммутаторы, модемы и коммуникационные серверы

Стандарты глобальных сетей

Определением, разработкой и внедрением стандартов в области глобальных сетей занимаются следующие организации.

- Международный телекоммуникационный союз (International Telecommunication Union, ITU), ранее — Международный консультативный комитет по телеграфии и телефонии (Consultative Committee for International Telegraphy and Telephony, CCITT).
- Международная организация по стандартизации (International Organization for Standardization, ISO)
- Рабочая группа по инженерным проблемам Internet (Internet Engineering Task Force, IETF).
- Ассоциация электронной промышленности (Electronic Industries Association, EIA).

Стандарты глобальных сетей обычно описывают требования канального и физического уровней.

Протоколы физического уровня WAN описывают, как обеспечить электрическое, механическое, операционное и функциональное подключение к WAN-сервисам. Как правило, эти сервисы предоставляются *провайдером услуг глобальной сети (WAN service providers)*,

например, региональными и национальными операторами связи, почтовыми, телефонными и телеграфными агентствами.

Протоколы канального уровня WAN описывают, каким образом кадры переносятся между системами по одному каналу передачи данных. Они включают протоколы, обеспечивающие работу через службы двухточечной и многоточечной связи, а также службу множественного доступа по коммутируемым каналам типа Frame Relay.

Глобальные сети и физический уровень

Физический уровень WAN описывает интерфейс между терминальным оборудованием (Data Terminal Equipment, DTE) и оборудованием передачи данных (Data Communications Equipment, DCE). К терминальному оборудованию относятся устройства, которые входят в интерфейс "пользователь-сеть" со стороны пользователя и играют роль отправителя данных, получателя данных или и того и того вместе. Устройства DCE обеспечивают физическое подключение к сети, пропуск трафика и задание тактовых сигналов для синхронизации обмена данными между устройствами DCE и DTE (рис. 4.9). Обычно устройство DCE расположено у сервис-провайдера, а DTE — подключаемое устройство. В этой модели сервисы предоставляются DTE-устройствам с помощью модемов или устройств CSU/DSU.

Интерфейс "пользователь-сеть" определяется несколькими стандартами физического уровня.

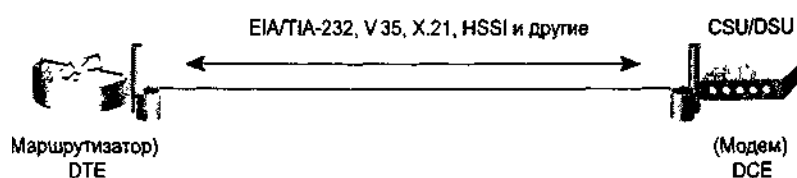


Рис 4.9. Сервисы доступны DTE-устройствам через модемы или устройства CSU/DSU

- *EIA/TIA-232* — общий стандарт интерфейса физического уровня, разработанный EIA и TIA, который поддерживает скорость передачи данных в несбалансированном канале до 64 Кбит/с. Этот стандарт очень похож на спецификацию V.24 и ранее был известен как RS-232.
- *EIA/TIA-449* — популярный интерфейс физического уровня, разработанный EIA и TIA. По существу, это более быстрая (до 2 Мбит/с) версия стандарта EIA/TIA-232, позволяющая работать с кабелями большей длины.
- *V.24* — стандарт для интерфейса физического уровня между терминальным оборудованием (DTE) и оборудованием передачи данных (DCE). Он был разработан ИТУ-Т. По сути, V.24 — то же самое, что и стандарт EIA/TIA-232.
- *V.35* — разработанный ИТУ-Т стандарт, который описывает синхронный протокол физического уровня, используемый для связи между устройствами доступа к сети и пакетной сетью. Наибольшее распространение V.35 получил в США и Европе. Он рекомендован для скоростей передачи данных вплоть до 48 Кбит/с.
- *X.21* — разработанный ИТУ-Т стандарт, который используется для последовательной связи по синхронным цифровым линиям. В основном протокол X.21 используется в Европе и Японии.
- *G.703* — разработанные ИТУ-Т электрические и механические спецификации для связи между оборудованием телефонных компаний и терминальным оборудованием (DTE) с использованием байонетных ВМС-разъемов и на скоростях, соответствующих каналу типа E1.

- EIA-530 — описывает две электрические реализации протокола EIA/TIA-449: RS-442 и RS-423.

Глобальные сети и канальный уровень

Существует несколько методов канальной инкапсуляции, связанных с линиями синхронной последовательной передачи данных (рис 4.10).

- HDLC (High-level Data Link Control — высокоуровневый протокол управления каналом).
- Frame Relay.
- PPP (Point-to-Point Protocol — протокол связи "точка-точка").
- ISDN.

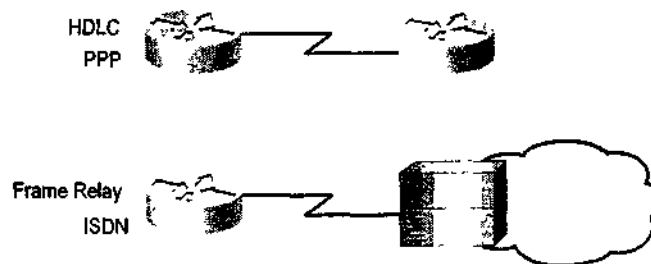


Рис. 4.10. Канальная инкапсуляция для линий синхронной последовательной передачи данных, включая протоколы HDLC, Frame Relay, PPP и ISDN

HDLC

HDLC — это битово-ориентированный протокол, разработанный Международной организацией по стандартизации (ISO). HDLC описывает метод инкапсуляции в каналах синхронной последовательной связи с использованием символов кадров и контрольных сумм. HDLC является ISO-стандартом, реализации которого различными поставщиками могут быть несовместимы между собой по причине различий в способах его реализации, и поэтому этот стандарт не является общепринятым для глобальных сетей. Протокол HDLC поддерживает как двухточечную, так и многоточечную конфигурации.

Frame Relay

Протокол Frame Relay предусматривает использование высококачественного цифрового оборудования. Используя упрощенный механизм формирования кадров без коррекции ошибок, Frame Relay может отправлять информацию канального уровня намного быстрее, чем другие протоколы глобальных сетей. Frame Relay является стандартным протоколом канального уровня при организации связи по коммутируемым каналам, позволяющим работать сразу с несколькими виртуальными каналами, в которых используется инкапсуляция по методу HDLC. Frame Relay является более эффективным протоколом, чем протокол X.25, для замены которого он и был разработан.

PPP

Протокол PPP обеспечивает соединение маршрутизатор—маршрутизатор и хост-сеть как по синхронным, так и по асинхронным каналам. PPP содержит поле типа протокола для идентификации протокола сетевого уровня.

ISDN

ISDN является набором цифровых сервисов для передачи голоса и данных. Разработанный телефонными компаниями, этот протокол позволяет передавать по телефонным сетям данные, голос и другие виды трафика.

Резюме

- Глобальные сети (WAN) используются для объединения локальных сетей, разделенных значительными географическими расстояниями.
- Глобальные сети работают на физическом и канальном уровнях эталонной модели OSI.
- Глобальные сети обеспечивают обмен пакетами данных между локальными сетями и поддерживающими их маршрутизаторами.
- Существует несколько методов канальной инкапсуляции, связанных с синхронными последовательными линиями:
 - HDLC
 - Frame Relay
 - PPP
 - ISDN

Контрольные вопросы

1. Какое из приведенных ниже утверждений не является справедливым по отношению к ЛВС?
 - A. Охватывают большие географические пространства,
 - B. Обеспечивают множеству пользователей доступ к среде передачи данных с высокой полосой пропускания.
 - C. Обеспечивают постоянное подключение к локальным сервисам.
 - D. Объединяют физически смежные устройства.
2. Как по-другому называется кабель IOBaseS?
 - A. Толстый Ethernet.
 - B. Телефонный провод.
 - C. Тонкий Ethernet.
 - D. Коаксиальный Ethernet.
3. Какой тип кабеля используется в сетях IOBaseT?
 - A. Оптоволоконный или неэкранированная витая пара.
 - B. Оптоволоконный или коаксиальный кабель.
 - C. Витая пара.
 - D. Коаксиальный кабель.
4. Какое из утверждений справедливо по отношению к сетям CSMA/CD?
 - A. Данные от передающего узла проходят через всю сеть. По мере движения данные принимаются и анализируются каждым узлом.
 - B. Сигналы посылаются непосредственно получателю, если его MAC- и IP-адрес известны отправителю.
 - C. Данные от передающего узла поступают к ближайшему маршрутизатору, который направляет их непосредственно адресату.
 - D. Сигналы всегда посылаются в режиме широковещания.
5. Какое из описаний широковещания является наилучшим?
 - A. Отправка одного кадра многим станциям одновременно.
 - B. Отправка одного кадра всем маршрутизаторам для одновременного обновления таблиц маршрутизации.
 - C. Отправка одного кадра всем маршрутизаторам одновременно.
 - D. Отправка одного кадра всем концентраторам и мостам одновременно.
6. Какое из описаний глобальных сетей является наилучшим?
 - A. Используются для объединения локальных сетей, разделенных значительными географическими расстояниями.
 - B. Объединяют рабочие станции, терминалы и другие устройства, расположенные в пределах города.
 - C. Объединяют локальные сети, расположенные в пределах большого здания.
 - D. Объединяют автоматизированные рабочие места, терминалы и другие устройства, расположенные в пределах здания.
7. На каких уровнях эталонной модели OSI работают глобальные сети?
 - A. Физический уровень и уровень приложений.
 - B. Физический и канальный уровни.
 - C. Канальный и сетевой уровни.
 - D. Канальный уровень и уровень представлений.
8. Чем глобальные сети отличаются от локальных?
 - A. Обычно существуют в определенных географических областях.
 - B. Обеспечивают высокоскоростные сервисы с множественным доступом.
 - C. Используют маркеры для регулирования сетевого трафика.
 - D. Используют службы операторов связи.
9. Какое из описаний протокола PPP является наилучшим?
 - A. Предусматривает использование высококачественного цифрового оборудования и является самым быстрым протоколом глобальных сетей.

- B. Поддерживает многоточечные и двухточечные соединения, а также использует символы кадра и контрольные суммы.
 - C. Обеспечивает соединение маршрутизатор-маршрутизатор и хост-сеть как по синхронным, так и асинхронным линиям связи.
 - D. Это цифровой сервис для передачи голоса и данных по существующим телефонным линиям.
10. Какое из описаний ISDN является наилучшим?
- A. Это цифровой сервис для передачи голоса и данных по существующим телефонным линиям.
 - B. Обеспечивает соединение маршрутизатор-маршрутизатор и хост-сеть как по синхронным, так и асинхронным линиям связи.
 - C. Использует высококачественное цифровое оборудование и является самым быстрым протоколом глобальных сетей.
 - D. Поддерживает многоточечные и двухточечные соединения, а также использует символы кадра и контрольные суммы.

Глава 5

IP-адресация

В этой главе...

- Что такое IP-адрес
- Представление чисел в двоичной системе исчисления
- Представление IP-адреса с помощью точечно-десятичной нотации
- Присвоение каждой сети в Internet уникального адреса
- Две составные части IP-адреса
- Понятия классов сетевых адресов
- Зарезервированные сетевые IP-адреса
- Понятие подсети и адреса подсети

Введение

В главе 3, "Сетевые устройства", рассказывалось, что сетевые устройства используются для объединения сетей. Было выяснено, что повторители восстанавливают форму и усиливают сигнал, а затем отправляют его дальше по сети. Вместо повторителя может использоваться концентратор, который также служит центром сети.

Кроме того, говорилось, что область сети, в пределах которой формируются пакеты и возникают конфликты, называется доменом конфликтов; что мосты устраняют ненужный трафик и минимизируют вероятность возникновения конфликтов путем деления сети на сегменты и фильтрации трафика на основе MAC-адресов. В заключение речь шла о том, что маршрутизатор способен принимать решение о выборе наилучшего пути доставки данных по сети.

В этой главе будут рассмотрены IP-адресация и три класса сетей в схеме IP-адресации; будет рассказано, что некоторые IP-адреса зарезервированы ARIN и не могут быть присвоены ни одной сети. В заключение будут рассмотрены подсеть, маска подсети и их схемы IP-адресации.

Обзор адресации

В главе 2, "Физический и канальный уровни", говорилось, что MAC-адресация существует на канальном уровне эталонной модели OSI, и поскольку большинство компьютеров имеют одно физическое подключение к сети, то они имеют один MAC-адрес. MAC-адреса обычно уникальны для каждого сетевого подключения. Перед тем как отправить пакет данных ближайшему устройству в сети, передающее устройство должно знать MAC-адрес назначения. Поэтому механизм определения местоположения компьютеров в сети является важным компонентом любой сетевой системы. В зависимости от используемой группы протоколов применяются различные схемы адресации. Другими словами, адресация Apple Talk отличается от IP-адресации, которая, в свою очередь, отличается от адресации OSI, и т.д.

В сетях используются две схемы адресации. Одна из этих схем, MAC-адресация, была рассмотрена ранее. Второй схемой является IP-адресация. Как следует из названия, IP-адресация базируется на протоколе IP (Internet Protocol). Каждая ЛВС должна иметь свой уникальный IP-адрес, который является определяющим элементом для осуществления межсетевого взаимодействия в глобальных сетях.

В IP-сетях конечная станция связывается с сервером или другой конечной станцией. Каждый узел имеет IP-адрес, который представляет собой уникальный 32-битовый логический адрес. IP-адресация существует на уровне 3 (сетевом) эталонной модели OSI. В отличие от MAC-адреса, которые обычно существуют в плоском адресном пространстве, IP-адреса имеют иерархическую структуру.

Каждая организация, представленная в списке сети, видится как одна уникальная сеть, с которой сначала надо установить связь и только после этого можно будет связаться с каждой отдельной хост-машиной этой организации. Как показано на рис. 5.1, каждая сеть имеет свой адрес, который относится ко всем хост-машинам, принадлежащим данной сети. Внутри сети каждая хост-машина имеет свой уникальный адрес.

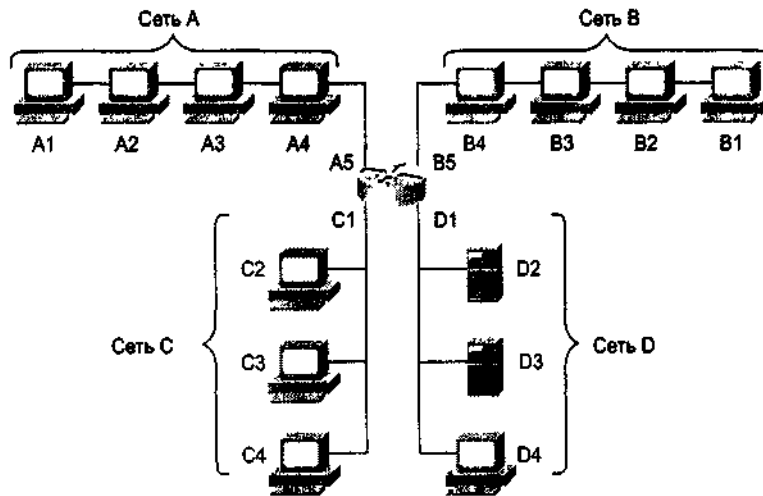


Рис. 5.1. Уникальная адресация позволяет конечным станциям связываться между собой

IP-адрес устройства состоит из адреса сети, к которой принадлежит устройство, и адреса устройства внутри этой сети. Следовательно, если устройство переносится из одной сети в другую, его IP-адрес должен быть изменен так, чтобы отразить это перемещение (рис. 5.2-5.5).

Так как IP-адреса имеют иерархическую структуру, в некотором смысле подобную структуре телефонных номеров или почтовых кодов, то он более удобен для организации адресов компьютеров, чем MAC-адреса, имеющие плоскую структуру, подобно номерам карточек социального страхования IP-адреса могут устанавливаться программно и поэтому более гибки в использовании, в отличие от MAC-адресов, которые прошиваются аппаратно. Обе схемы адресации являются важными для эффективной связи между компьютерами.

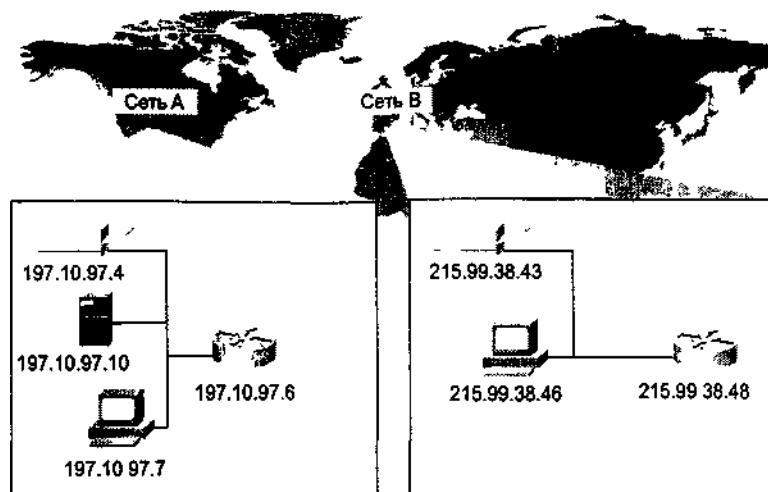


Рис. 5.2. В сети А находится сервер с адресом 197.10.97.10, который нужно перенести в сеть В

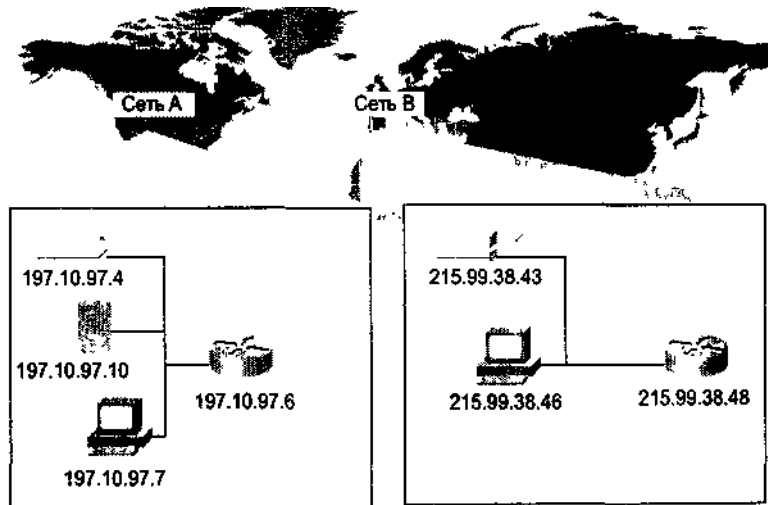


Рис. 5.3. Файл-сервер с адресом 197.10.97.10 удален из сети А

IP-адреса имеют сходство с почтовыми адресами, которые описывают местонахождение адресата, включая страну, город, улицу, номер дома и имя. Хорошим примером плоского адресного пространства является принятая в США система присвоения номеров персональным карточкам социального страхования, когда каждому человеку присваивается отдельный уникальный номер. Человек может перемещаться по стране и получать новые логические адреса — город, улицу, номер дома и почтовый индекс, — но у него будет оставаться все тот же номер карточки социального страхования.

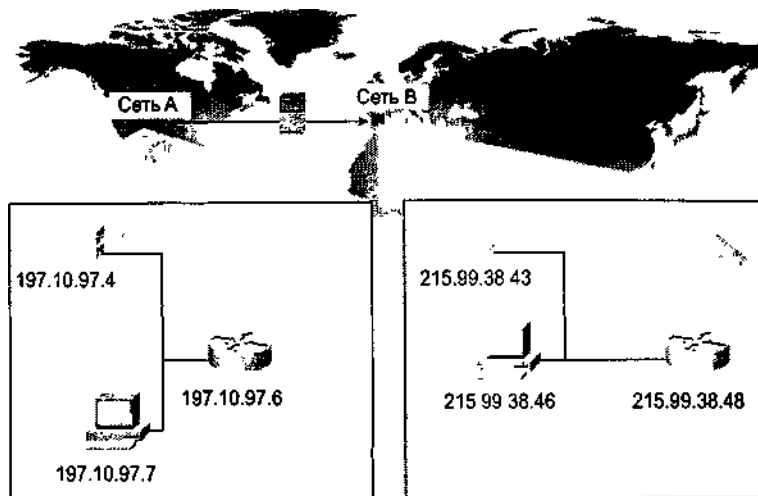


Рис. 5.4. Сервер доставлен на другой континент

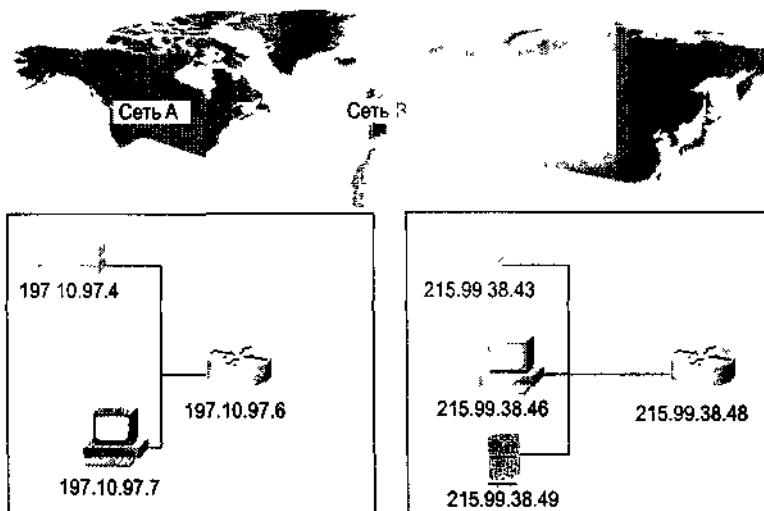


Рис. 5.5. Файл-сервер подключен к сети В, и ему присвоен новый адрес 215.99.38.49

IP-адресация позволяет данным находить пункт назначения в сети Internet. Причина, по которой IP-адреса записываются в виде битов, состоит в том, что содержащаяся в них информация должна быть понятной компьютерам. Для того чтобы данные могли передаваться в среде передачи данных, они должны быть сначала преобразованы в электрические импульсы. Когда компьютер принимает эти электрические импульсы, он распознает только два состояния: наличие или отсутствие напряжения в кабеле. Поскольку распознаются только два состояния, то для представления любых данных, передаваемых по сети, может быть использована схема на основе двоичной математики (рис. 5.6). В этой схеме для связи между компьютерами используются числа 0 и 1.

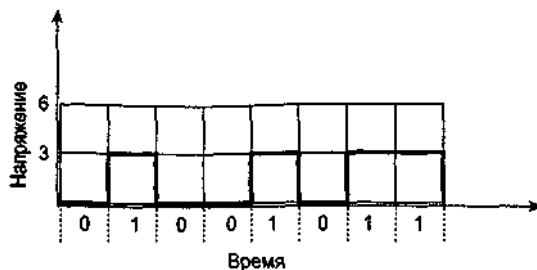


Рис. 5.6. Для представления данных, передаваемых в среде передачи, используются единицы и нули

Двоичная система счисления

Наиболее часто встречающейся и, вероятно, наиболее известной читателю является десятичная система счисления, которая основана на возведении в степень числа 10: 10^1 , 10^2 , 10^3 , 10^4 и т.д. 10^1 — это то же самое, что и 10×1 , или 10. 10^2 — то же самое, что и 10×10 , или 100. 10^3 — то же самое, что и $10 \times 10 \times 10$ или 1000. Двоичная система исчисления базируется на возведении в степень числа 2: 2^1 , 2^2 , 2^3 , 2^4 и т.д.

IP-адрес представляет собой 32-разрядное двоичное число, записанное в виде четырех октетов, т.е. четырех групп, каждая из которых состоит из восьми двоичных знаков (нулей и единиц). Таким образом, в IP-адресе, записанном как 11000000.00000101.00100010.00001011, первый октет представляет собой двоичное число 11000000, второй октет — двоичное число 00000101, третий октет — двоичное число 00100010, четвертый октет — двоичное число 00001011 (рис. 5.7).

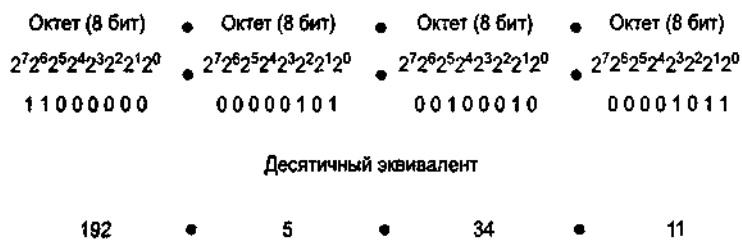


Рис. 5.7. IP-адрес выражается в виде двоичных чисел, состоящих из нулей и единиц

Так как двоичная система основана на возведении в степень числа 2, каждая позиция в октете представляет различные степени от 2. Величина показателя степени 2 назначается каждому разряду двоичного числа, начиная с крайнего правого. Чтобы определить, чему равно двоичное число, необходимо сложить значения всех разрядов в октете. Следовательно, для двоичного числа первого октета, показанного на рис. 5.7 (11000000), справедливо следующее:

- 0 умножается на 2^0 (1), что равно 0
- 0 умножается на 2^1 (2), что равно 0
- 0 умножается на 2^2 (4), что равно 0
- 0 умножается на 2^3 (8), что равно 0

- 0 умножается на 2^4 (16), что равно 0
- 0 умножается на 2^5 (32), что равно 0
- 1 умножается на 2^6 (64), что равно 64
- 1 умножается на 2^7 (128), что равно 128

Таким образом, двоичное число 11000000 равно десятичному числу 192.

Двоичная IP-адресация

Достаточно трудно запомнить число, состоящее из 8 цифр, не говоря уже о числах из 32 цифр, которые используются в IP-адресах. Поэтому для обозначения 32-битовых чисел в IP-адресах используются десятичные числа. Это называется представлением в десятичной форме с разделением точками.

В представлении в десятичной форме с разделением точками IP-адреса, или точечно-десятичные адреса, записываются следующим образом (рис. 5.8): каждое десятичное число представляет один байт из четырех, составляющих весь IP-адрес.

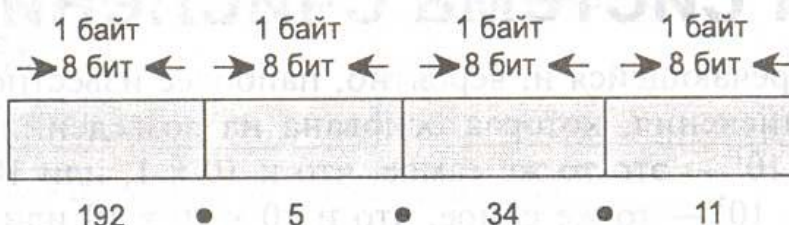


Рис. 5.8. Четырехбайтовый IP-адрес состоит из 4 однобайтовых октетов

Чтобы перевести IP-адрес 11000000.00000101.00100010.00001011 в этот упрощенный формат, для начала его надо представить в виде 4 отдельных байтов (по 8 бит); другими словами, IP-адрес необходимо разделить на 4 октета:

```
11000000
    00000101
      00100010
        00001011
```

Затем каждое из этих 8-битовых чисел преобразовывается в его десятичный эквивалент. В результате двоичное число 11000000.00000101.00100010.00001011 преобразуется в точечно-десятичное число 192.5.34.11.

Классы IP-адресов

Благодаря тому, что каждая сеть, подключенная к Internet, имеет уникальный сетевой адрес, данные могут найти требуемый адресат в Internet. Для того чтобы каждый сетевой адрес был уникальным и отличался от любого другого номера, организация под названием American Registry for Internet Numbers (Американский реестр Internet-номеров, ARIN) выделяет компаниям блоки IP-адресов в зависимости от размера их сетей. Адрес ARIN в Internet — www.arin.net.

Каждый IP-адрес состоит из двух частей: номера сети и номера хоста (рис. 5.9). Сетевой номер идентифицирует сеть, к которой подключено устройство. Номер хоста идентифицирует устройство в этой сети.

ARIN определяет три класса IP-адресов. Класс А составляют IP-адреса, зарезервированные для правительственных учреждений, класс В — IP-адреса для компаний среднего уровня и класс С — для всех остальных организаций. Если записать IP-адреса класса А в двоичном формате, то первый

бит всегда будет равен 0 (рис. 5.10). Если записать IP-адреса класса В в двоичном формате, то первые два бита всегда будут 0 и 1. Если записать IP-адреса класса С в двоичном формате, то первые три бита всегда будут 1, 1 и 0.

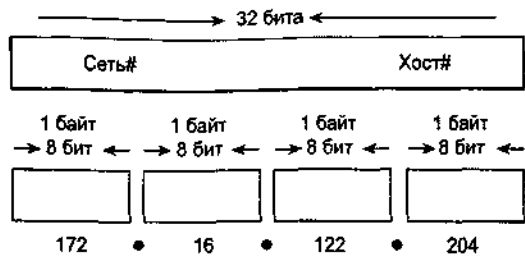


Рис. 5.9. IP-адрес состоит из номера сети и номера хоста

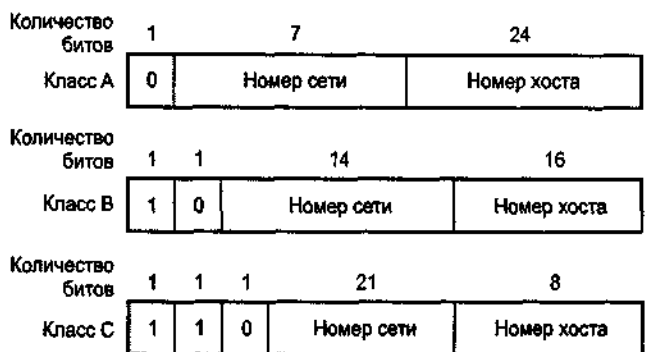
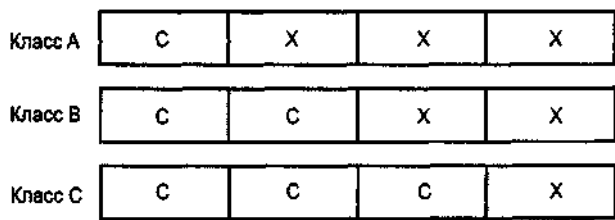


Рис. 5.10. Общий вид IP-адресов классов А, В и С

Зарезервированные классы сетей

Выше были рассмотрены три класса сетевых адресов, которые назначаются ARIN (рис. 5.11). На самом деле существует пять классов сетевых адресов. Но только три из них — классы А, В и С — используются коммерчески. Два других класса сетевых адресов зарезервированы.



Класс D: для групповой адресации

Класс E: для исследований

С= номер сети, присвоенный ARIN

Х= номер хоста, присвоенный сетевым администратором

Рис. 5.11. ARIN присваивает три типа сетевых адресов

Максимально возможное значение каждого октета IP-адреса равно 255 (рис. 5.12). Следовательно, это десятичное число могло бы быть присвоено первому октету сети любого класса. На практике применяются только числа до 223. Возникает вопрос: почему при максимально допустимом значении 255 для каждого октета используются только числа до 223? Причина проста: часть номеров резервируется для экспериментальных целей и потребностей групповой адресации. Эти номера не могут быть присвоены сетям. Поэтому в первом октете IP-адресов значения с 224 по 255 для решения сетевых задач не используются.

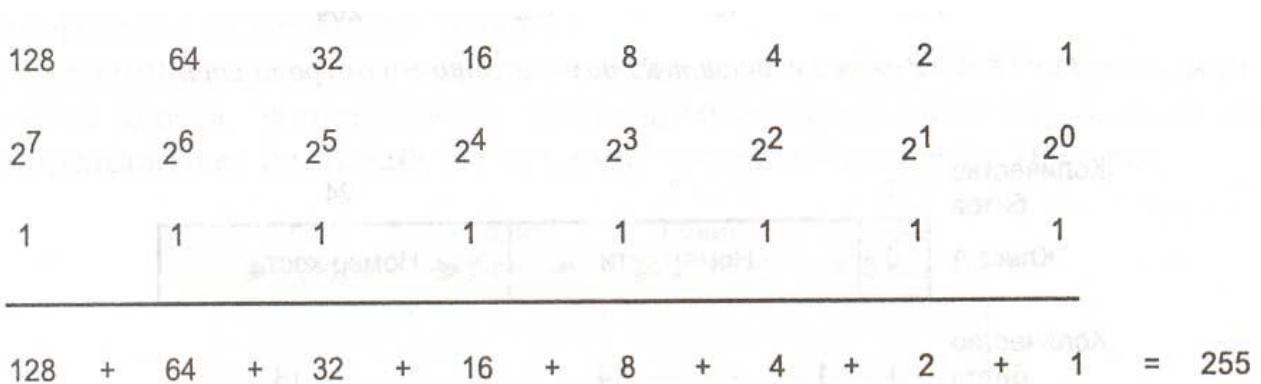


Рис. 5.12. Максимально возможное значение в каждом октете IP-адреса — 255

Кроме этих зарезервированных адресов резервируются также все IP-адреса, у которых в той части адреса, которая обозначает адрес хост-машины, содержатся только нули или единицы.

В приведенных ранее примерах IP-адреса использовались только по отношению к устройствам, подключенным к сети. Иногда необходимо обратиться ко всем устройствам в сети, или, другими словами, к самой сети. Однако довольно сложно выписать адреса всех устройств в сети. Можно было бы использовать только два адреса с дефисом между ними, для того чтобы показать, что обращение осуществляется ко всем устройствам в заданном диапазоне чисел, но и это достаточно сложно. Вместо этого придуман более простой метод обращения ко всей сети. В соответствии с соглашением, в схемах IP-адресации любой IP-адрес, который заканчивается всеми двоичными нулями, резервируется для адреса этой сети. Примером адреса сети класса А может быть IP-адрес 113.0.0.0. Когда маршрутизаторы направляют данные через Internet, они руководствуются при этом IP-адресами сетей.

Примером адреса сети класса В может быть IP-адрес 176.10.0.0. Следует заметить, что десятичные числа занимают первые два октета адреса сети класса В. Это объясняется тем, что оба октета назначаются ARIN и обозначают номер сети. Только два последних октета содержат нули. Это связано с тем, что числа в этих октетах обозначают номера хостов, зарезервированные для устройств, подключаемых к сети. Следовательно, для того, чтобы обратиться ко всем устройствам в этой сети, т.е. к самой сети, сетевой адрес должен иметь нули в двух последних октетах. Поскольку адрес 176.10.0.0 зарезервирован для адреса сети (рис. 5.13), он никогда не будет использоваться в качестве IP-адреса какого-либо устройства, подключенного к этой сети.

Процесс, в ходе которого источник отправляет данные всем устройствам в сети, называется широковещанием. Для того чтобы все устройства в сети обратили внимание на широковещание, должен использоваться такой IP-адрес, который смогли бы распознать и признать своим все устройства в сети. Следовательно, для сети 176.10.0.0, показанной на рис. 5.13, адресом широковещания может быть адрес 176.10.255.255.

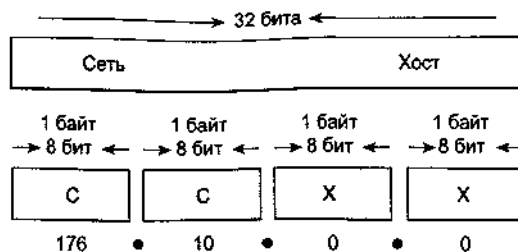


Рис. 5.13. Зарезервированный сетевой адрес 176.10.0.0 никогда не используется в качестве IP-адреса какого-либо устройства, подключенного к этой сети

Когда кадр (который является разновидностью данных) достигает маршрутизатора, последний выполняет несколько функций. Во-первых, маршрутизатор отделяет содержащийся в кадре канальный заголовок. В канальном заголовке находятся MAC-адреса источника данных и

получателя. После этого маршрутизатор проверяет заголовок сетевого уровня, в котором содержится IP-адрес сети назначения. Далее, маршрутизатор сверяется со своей таблицей, чтобы определить, через какой из своих портов нужно отправить данные, чтобы они достигли сети назначения.

При транспортировке данных через Internet одна сеть видит другую как отдельную сеть и не имеет при этом подробной информации о ее внутренней структуре. Это помогает поддерживать размеры таблиц маршрутизации небольшими.

Однако внутри сети могут видеть себя совсем по-другому. Чтобы обеспечить сетевым администраторам максимальную гибкость настройки, сети — особенно большие — часто разделяют на маленькие, называемые *подсетями* (*subnets*). Например, можно разделить IP-адреса класса В между многими подсетями.

Адресация подсетей

Как и номера хост-машин в сетях класса А, класса В и класса С адреса подсетей задаются локально. Обычно это выполняет сетевой администратор. Так же, как и другие IP-адреса, каждый адрес подсети является уникальным. Использование подсетей никак не отражается на том, как внешний мир видит эту сеть, но в пределах организации подсети рассматриваются как дополнительные структуры.

Для примера, сеть 172.16.0.0 (рис. 5.14) разделена на 4 подсети: 172.16.1.0, 172.16.2.0, 172.16.3.0 и 172.16.4.0. Маршрутизатор определяет сеть назначения, используя адрес подсети, тем самым ограничивая объем трафика в других сегментах сети.

С точки зрения адресации, подсети являются расширением сетевого номера (рис. 5.15). Сетевые администраторы задают размеры подсетей, исходя из потребностей организации и роста.

Адрес подсети включает номера сети, подсети и хост-машины внутри подсети. Благодаря этим трем уровням адресации подсети обеспечивают сетевым администраторам повышенную гибкость настройки.

Чтобы создать адрес подсети, сетевой администратор "заимствует" биты из поля хост-машин и переопределяет их в качестве поля подсетей (рис. 5.16). Количество "заимствованных" битов можно увеличивать до тех пор, пока не останется 2 бита. Поскольку в поле хостов сетей класса В имеются только 2 октета, для создания подсетей можно заимствовать до 14 бит. Сети класса С имеют только один октет в поле хостов. Следовательно, в сетях класса С для создания подсетей можно заимствовать до 6 бит.

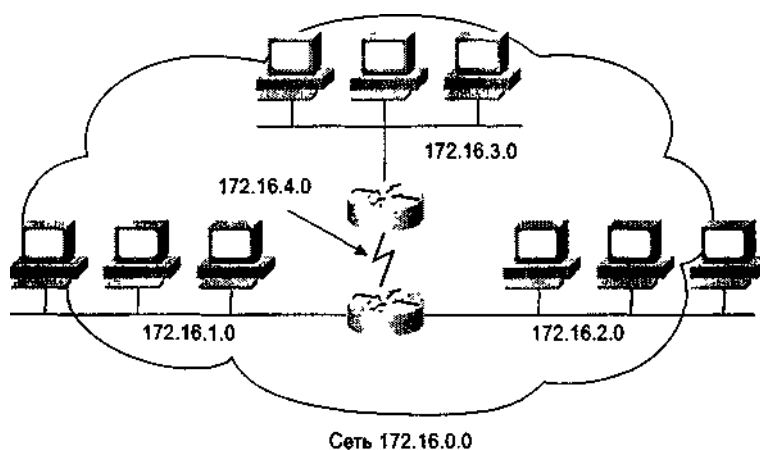


Рис. 5.14. Сеть 172.16.0.0 состоит из четырех подсетей

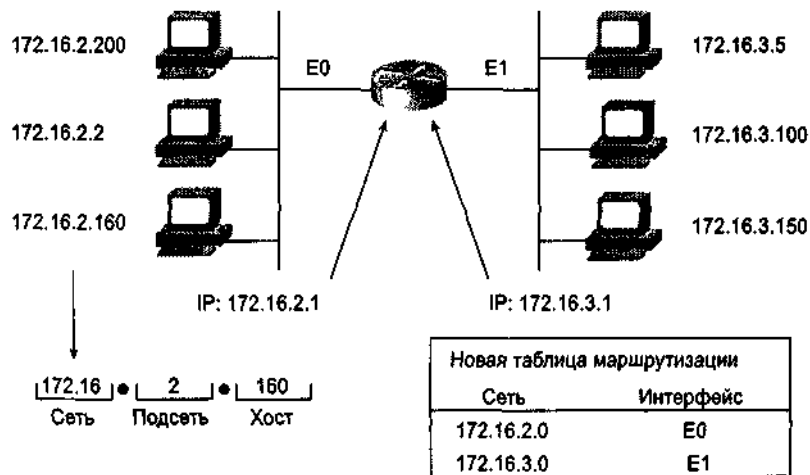


Рис. 5.15. Адресация подсетей расширяет сетевой номер путем создания подсетей

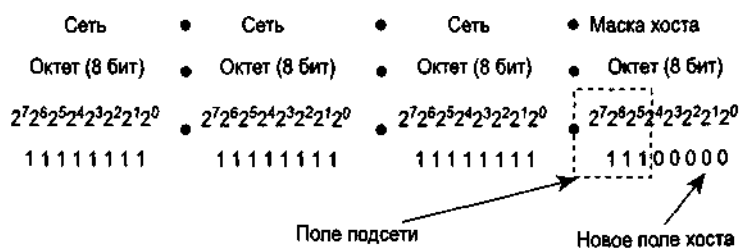


Рис. 5.16. Биты заимствуются из поля хост-машины и переопределяются в качестве поля подсети

Чем больше бит заимствуется из поля хоста, тем меньше бит в октете можно использовать для задания номера хоста. Таким образом, каждый раз, когда заимствуется 1 бит из поля хоста, число адресов хостов, которые могут быть заданы, уменьшается на степень числа 2.

Чтобы понять смысл вышесказанного, рассмотрим сеть класса C. Все 8 бит в последнем октете используются для поля хостов. Следовательно, возможное количество адресов равно 2^8 , или 256.

Представим, что эту сеть разделили на подсети. Если из поля хостов заимствовать 1 бит, количество бит, которое можно использовать для адресации хостов, уменьшится до 7. Если записать все возможные комбинации нулей и единиц, можно убедиться, что число хостов, которые можно адресовать, стало равно 2^7 , или 128.

Если в сети класса C из поля хостов заимствовать 2 бита, то количество бит, которое можно использовать для адресации хостов, уменьшится до 6. Общее число хостов, которое можно адресовать, станет равным 2^6 , или 64.

Адреса в подсети, зарезервированные для широковещания

IP-адреса, которые заканчиваются всеми двоичными единицами, зарезервированы для широковещания. Это утверждение справедливо и для подсетей. Рассмотрим сеть класса C с номером 197.15.22.0, которая разделена на восемь подсетей (табл. 5.1).

Таблица 5.1. Последний октет сети класса C, разделенной на восемь подсетей

Подсеть	Двоичные числа в поле подсети	Диапазон двоичных чисел в поле хостов	Диапазон десятичных чисел в поле хостов
Первая	000	00000-11111	0-31

Вторая	001	00000-1 1111	.32-.63
Третья	010	00000-1 1111	.64-.95
Четвертая	011	00000-1 1111	.96-. 127
Пятая	100	00000-1 1111	.128-. 159
Шестая	100	00000-1 1111	160-.191
Седьмая	101	00000-1 1111	.192-.223
Восьмая	110	00000-11111	.224- 225

Обратите внимание на IP-адрес 192.15.22.31. На первый взгляд он ничем не похож ни на зарезервированный адрес сети, ни на адрес для широковещания. Однако, поскольку сеть разделена на восемь подсетей, первые 3 бита заимствуются для задания номера подсети. Это означает, что только последние 5 бит могут использоваться для поля хостов. Обратите внимание, что все 5 бит записаны в виде двоичных единиц. Следовательно, этот IP-адрес является зарезервированным адресом широковещания для первой подсети сети 197.15.22.0.

Адреса в подсети, зарезервированные для номеров подсетей

IP-адреса, которые заканчиваются всеми двоичными нулями, зарезервированы для номера сети. Это утверждение справедливо и для подсетей. Чтобы убедиться в этом, можно еще раз обратиться к сети класса C с номером 197.15.22.0, разделенной на 8 подсетей (см. табл. 5.1).

Маскирование подсетей

Подсети скрыты от внешнего мира с помощью масок, называемых *масками подсети*, функцией которых является сообщить устройствам, в какой части адреса содержится номер сети, включая номер подсети, а в какой — номер хост-машины.

Маски подсетей используют тот же формат, что и IP-адресация. Другими словами, маска имеет длину 32 бита и разделена на 4 октета. Маски подсетей имеют все единицы в части, отвечающей сети и подсети, и все нули в части, отвечающей хост-машине. По умолчанию, если нет заимствованных битов, маска подсети сети класса В будет иметь вид 255.255.0.0. Если же заимствовано 8 бит, маской подсети той же сети класса В будет 255.255.255.0 (рис. 5.17 и 5.18). Поскольку для сетей класса В только 2 октета относятся к полю хост-машин, то для создания подсетей может быть задействовано до 14 бит. В сетях класса С только один октет относится к полю хост-машин, поэтому для создания подсетей в сетях класса С может быть заимствовано до 6 бит.

Чтобы решить эту задачу, маршрутизатор определяет по IP-адресу назначения, какая его часть относится к полю сети, какая часть — к полю подсети и, наконец, какая к полю хоста. Следует помнить, что маршрутизатор воспринимает IP-адреса не в виде десятичных чисел, а в виде двоичного числа 10000011.0110110.00000010.00000010.

Маршрутизатор знает, что маска подсети Cisco имеет вид 255.255.255.0, и воспринимает это число как 11111111.11111111.11111111.00000000. Маска подсети показывает, что в сети компании Cisco 8 бит заимствовано для создания подсетей. Затем маршрутизатор берет два этих адреса — IP-адрес назначения, содержащийся в Данных, и адрес маски подсети сети компании — и выполняет побитно операцию логического умножения (AND).

Если логически умножаются 1 и 1, на выходе получается 1. Если хотя бы один из операндов равен 0, на выходе получается 0. Поэтому, после того, как маршрутизатор произведет операцию AND, часть адреса, соответствующая хостам, будет отброшена. Маршрутизатор смотрит на оставшуюся часть, которая представляет собой номер сети, включая подсеть, а затем сверяется с собственной таблицей маршрутизации и пытается сопоставить номер сети, включая подсеть, с интерфейсом. Если соответствие найдено, маршрутизатор знает, какой из интерфейсов нужно использовать. Затем маршрутизатор через соответствующий интерфейс передает данные в подсеть, которая содержит IP-адрес назначения.

Чтобы лучше понять, как осуществляется операция логического умножения, рассмотрим работу маршрутизатора с различными видами масок подсети применительно к одной и той же сети. Возьмем сеть класса В с сетевым номером 172.16.0.0. После оценки потребностей сети сетевой администратор принимает решение заимствовать 8 бит для того, чтобы создать подсети. Как упоминалось выше, маска подсети в этом случае имеет вид 255 . 255 . 255 . 0.

Представим, что из внешней сети данные посылаются по IP-адресу 172.16.2.120. Чтобы определить, куда направить данные, маршрутизатор производит операцию логического умножения между адресом назначения и маской подсети. После этого часть адреса, соответствующая хостам, будет отброшена, а оставшаяся будет представлять собой номер сети, включая подсеть. Таким образом, данные были адресованы устройству, которое идентифицируется двоичным числом 01111000.

Теперь возьмем ту же сеть, 172.16.0.0. На этот раз сетевой администратор принимает решение заимствовать только 7 бит, чтобы создать подсети. В двоичной форме маска подсети для этого случая будет иметь вид 11111111.11111111.11111110.00000000.

Планирование подсетей

Сети, изображенной на рис 5 19, присвоен адрес класса С 201.222.5.0. Предположим, необходимо организовать 20 подсетей, по 5 хостов в каждой. Можно разделить последний октет на части подсети и хостов и определить, какой вид будет иметь маска подсети. Размер поля подсети выбирается исходя из требуемого количества подсетей. В этом примере выбор 29-битовой маски дает возможность иметь 2^{21} подсетей. Адресами подсетей являются все адреса, кратные 8 (например, 201.222.5.16, 201.222.5.32 и 201.222.5.48).

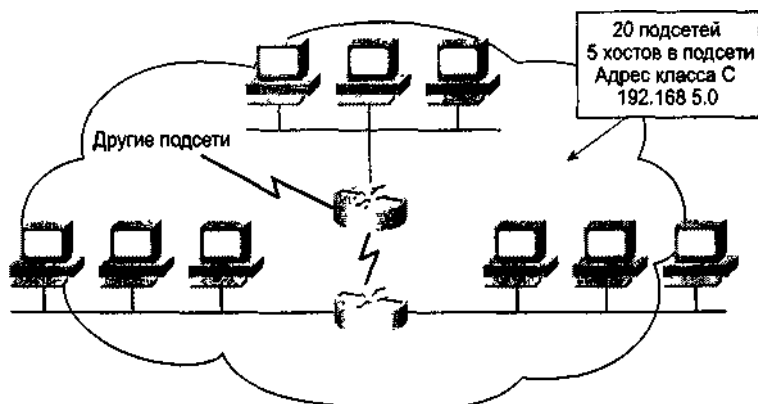


Рис 5 19 Необходимо разделить сеть на 20 подсетей (по 5 хостов в каждой)

Оставшиеся биты в последнем октете используются для поля хост-машин. Для данного примера требуемое количество хост-машин равно 5, поэтому поле хост-машин должно содержать минимум 3 бита. Номера хост-машин могут быть 1, 2, 3 и т.д. Окончательный вид адресов формируется путем сложения начального адреса кабеля сети/подсети и номера хост-машины. Таким образом, хост-машины подсети 201.222.5.16 будут адресоваться как 201.222.5.17, 201.222.5.18, 201.222.5.19 и т.д. Номер хоста 0 зарезервирован в качестве адреса кабеля, а значение номера хоста, состоящее из одних единиц, резервируется для широковещания.

Пример планирования подсетей в сетях класса В

Табл. 5.2 является примером таблицы, используемой для планирования подсетей. На рис. 5.20 показано комбинирование входящих IP-адресов с маской подсети для получения номера подсети.

Таблица 5.2. Планирование подсетей сети класса В

Количество бит для подсетей	Номер маски подсети	Количество подсетей	Количество хост-машин
2	255.255.192.0	2	16,385
3	255.255.224.0	6	8,190
4	255.255.240.0	14	4,094
5	255.255.248.0	30	2,046
6	255.255.252.0	62	1,022
7	255.255.254.0	126	510
8	255.255.255.0	254	254
9	255.255.255.128	510	126
10	255.255.255.192	1,022	62
11	255.255.255.224	2,046	30
12	255.255.255.240	4,094	14
13	255.255.255.248	8,190	6
14	255.255.255.252	16,382	2

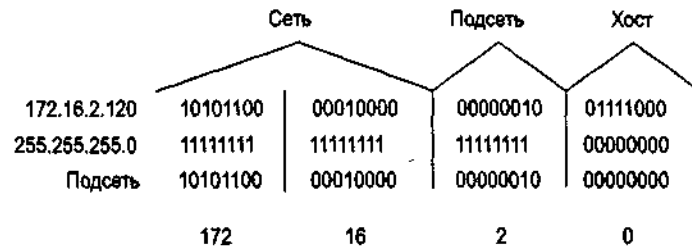
Пример планирования подсетей в сетях класса С

В табл. 5.3 представлена сеть класса С, которая поделена на подсети для обеспечения адресации 6 хост-машин и 30 подсетей; на рис. 5.21 показан пример планирования подсетей с 5-битовой маской подсети.

Таблица 5.3. Пример сети класса С, разделенной на подсети

Количество бит для подсетей	Номер маски подсети	Количество подсетей	Количество хостов
2	255.255.192.0	2	62
3	255.255.224.0	6	30
4	255.255.240.0	14	14
5	255.255.248.0	30	6
6	255.255.252.0	62	2

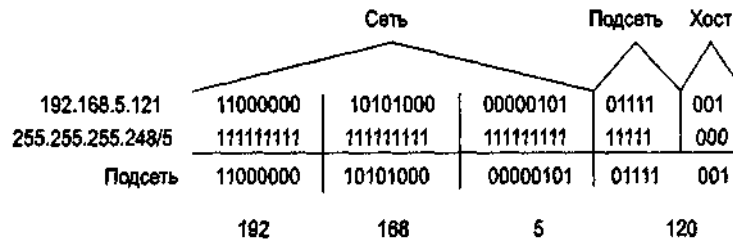
IP-адрес хоста: 172.16.2.120
Маска подсети: 255.255.255.0



- Адрес подсети: 172.16.2.0
- Адреса хостов: 172.16.2.1-172.16.2.254
- Адреса широковещания: 172.16.2.255
- 8 бит для создания подсетей

Рис. 5.20. Пример планирования подсетей в сети класса В. Выделение 8 бит для подсетей позволяет адресовать до 254 подсетей и 254 хостов

IP-адрес хоста: 192.168.5.121
Маска подсети: 255.255.255.248



- Адрес подсети: 192.168.5.120
- Адреса хостов: 192.168.5.121-192.168.5.126
- Адреса широковещания: 192.168.5.127
- 5 бит для создания подсетей

Рис. 5.21. Пример планирования подсетей в сети класса С с выделением 5 бит для подсетей. Адресуются 30 подсетей и 6 хост-машин

Резюме

- § IP-адреса базируются на протоколе IP (Internet Protocol) и являются уникальными 32-битовыми логическими адресами, которые относятся к уровню 3 (сетевому) эталонной модели OSI.
- IP-адрес содержит адрес самого устройства, а также адрес сети, в которой это устройство находится.
 - Поскольку IP-адреса имеют иерархическую структуру (как телефонные номера или почтовые индексы), их удобнее использовать в качестве адресов компьютеров, чем MAC-адреса, которые являются плоскими адресами (как номера карточек социального страхования).
 - IP-адреса представляют собой 32-битовые значения, которые записываются в виде четырех октетов (групп по 8 бит) и содержат двоичные числа, состоящие из нулей и единиц.
 - В десятичной форме представления с разделением точками каждый байт 4-байтового IP-адреса записывается в виде десятичного числа.
 - ARIN резервирует IP-адреса класса А для правительственных учреждений во всем мире, IP-адреса класса В — для компаний среднего размера и IP-адреса класса С — для всех остальных организаций. Еще два класса сетей являются зарезервированными.
 - IP-адреса, которые содержат все нули или все единицы в хостовой части адреса, являются зарезервированными.
 - Для того чтобы обеспечить сетевым администраторам максимальную гибкость настройки, сети — особенно большие — разделяют на несколько небольших сетей, называемых подсетями.
 - Подсети скрыты от внешних сетей с помощью так называемых масок подсети.

Контрольные вопросы

1. Сколько бит содержит IP-адрес?
 - A. 4
 - B. 8
 - C. 16

- D. 32
2. Какую роль в IP-адресе играет номер сети?
- A. Задаёт сеть, к которой принадлежит хост-машина.
- B. Задаёт идентификатор компьютера в сети.
- C. Задаёт адресуемый узел в подсети.
- D. Задаёт сети, с которыми может связываться устройство.
3. Какую роль в IP-адресе играет номер хост-машины?
- A. Задаёт идентификатор компьютера в сети.
- B. Задаёт адресуемый узел в подсети.
- C. Задаёт сеть, к которой принадлежит хост-машина.
- D. Задаёт хост-машины, с которыми может связываться устройство.
4. Какое десятичное число является эквивалентом двоичного числа 11111111?
- A. 8
- B. 128
- C. 254
- D. 255
5. Что такое подсеть?
- A. Часть сети, которая является зависимой системой по отношению к главной сети.
- B. Небольшая сеть, работающая в пределах более крупной сети и позволяющая объединить разные типы устройств.
- C. Небольшая часть крупной сети.
- D. Небольшая сеть, которая содержит базу данных всех MAC-адресов в сети.
6. Какая часть адреса 182.54.4.233 обозначает подсеть?
- A. 182
- B. 54
- C. 4
- D. 233
7. Если сеть класса C разделена на подсети и имеет маску 255.255.255.192, то какое максимальное количество подсетей можно создать?
- A. 2
- B. 4
- C. 6
- D. 8
8. IP-адрес хост-машины — 192.168.5.121, маска подсети — 255.255.255.248. Какой адрес имеет сеть этого хоста?
- A. 192.168.5.12
- B. 192.169.5.121
- C. 192.169.5.120
- D. 192.168.5.120
9. Какая часть IP-адреса 205.129.12.5 представляет хост-машину?
- A. 205
- B. 205.129
- C. 5
- D. 12.5
10. Какая часть IP-адреса 129.219.51.18 представляет сеть?
- A. 129.215
- B. 129
- C. 14.1
- D. 1

Глава 6

ARP и RARP

В этой главе

- Что такое ARP
- ARP-запросы, ARP-таблицы, ARP-ответы и кадры ARP-запросов
- Обновление ARP-таблиц RARP
- RARP-серверы, RARP-запросы и кадры RARP-ответов
- Какие межсетевые устройства имеют ARP-таблицы
- Определение шлюза по умолчанию

Введение

В главе 5 "IP-адресация", говорилось, что в Internet каждая сеть видит другую как одну отдельную сеть и не имеет сведений о ее внутренней структуре. Таким образом, устройства из внешних сетей видят только номера сети и хоста устройства, находящегося в другой сети. С точки зрения внутренней структуры сеть может рассматриваться как группа небольших сетей, называемых подсетями. IP-адреса устройств представляют собой совокупность номеров сети, подсети и хоста. Для адресации подсетей используются уникальные 32-битовые адреса, которые создаются путем заимствования битов из поля хоста. Адреса подсетей видимы для других устройств этой же сети, но невидимы для внешних сетей, поскольку подсети используют специальные маски, называемые масками подсети.

В этой главе будет рассказано о том, каким образом устройства в локальных вычислительных сетях используют *протокол преобразования адреса (Address Resolution Protocol, ARP)* .. перед отправкой данных адресату. Будет рассказано, что происходит, если устройство из одной сети не знает MAC-адрес устройства в другой сети. Также будет рассмотрен *протокол обратного преобразования адреса (Reverse Address Resolution Protocol, RARP)*, который используется устройствами, если они не знают собственных IP-адресов.

ARP

Протоколы определяют, передаются ли данные через сетевой уровень к верхним уровням эталонной модели OSI. В основном, для того чтобы это произошло, необходимо, чтобы пакет данных содержал MAC- и IP-адрес пункта назначения. Если в пакете данных отсутствует один из этих адресов, данные не будут переданы на верхние уровни. Таким образом, MAC- и IP-адрес служат для своего рода проверки и дополнения друг друга.

Когда отправитель определил IP-адрес получателя (рис 6.1), он смотрит в свою ARP-таблицу, для того чтобы узнать его MAC-адрес. Если источник обнаруживает, что MAC- и IP-адрес получателя присутствуют в его таблице, он устанавливает соответствие между ними, а затем использует их в ходе инкапсуляции данных. После этого пакет данных по сетевой среде отправляется адресату (рис 6.2).

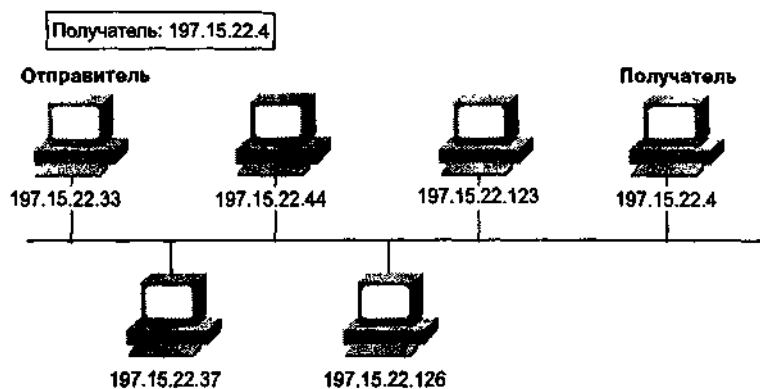


Рис 6.1. Источник сверяется со своей ARP-таблицей после того, как определит IP-адрес пункта назначения

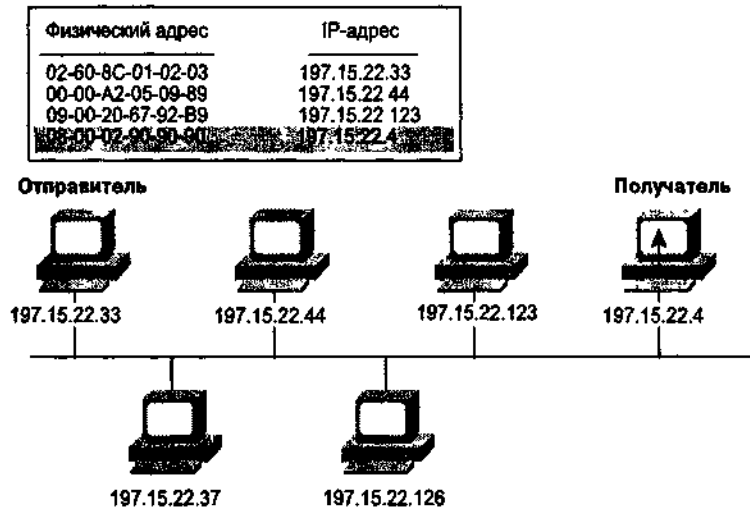


Рис. 6.2 Данные принимаются получателем, после того как установлено соответствие между MAC- и IP-адресами и инкапсулированы данные

ARP-запросы

В примере, показанном на рис. 6.3, отправитель хочет отправить данные другому устройству. Он знает IP-адрес получателя, но MAC-адрес получателя в его ARP-таблице отсутствует. Поэтому устройство инициирует процесс, называемый *ARP-запросом*, который позволяет определить этот MAC-адрес. Сначала устройство создает пакет ARP-запроса и посылает его всем устройствам в сети. Для того чтобы пакет ARP-запроса был замечен всеми устройствами в сети, источник использует MAC-адрес широковещания. Адрес широковещания, используемый в схеме MAC-адресации, имеет значение F во всех разрядах. Таким образом, MAC-адрес широковещания имеет вид FF-FF-FF-FF-FF-FF.

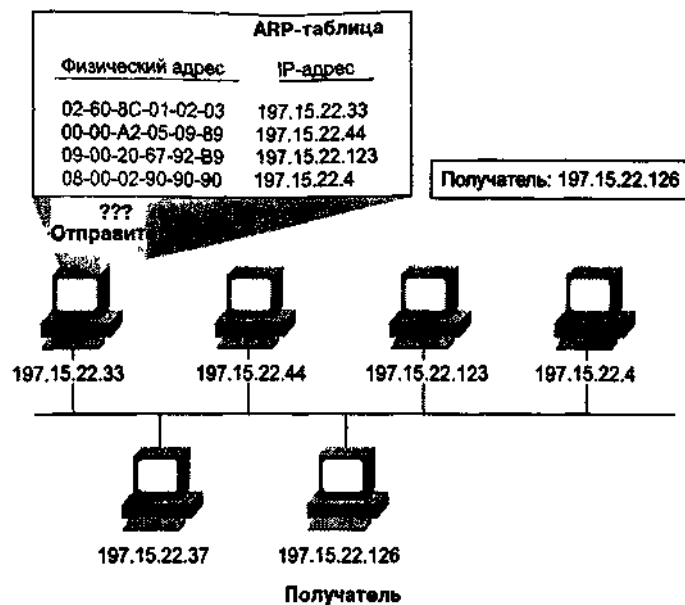


Рис. 6.3. Отправитель не может обнаружить MAC-адрес получателя в своей ARP-таблице

ARP-запросы структурированы определенным способом. Поскольку протокол ARP функционирует на нижних уровнях эталонной модели OSI, сообщение, в котором содержится ARP-запрос, должно быть инкапсулировано внутри кадра протокола аппаратных средств. Таким образом, кадр ARP-запроса состоит из двух частей: заголовка и ARP-сообщения (рис. 6.4). Кроме того, заголовок кадра может быть затем разделен на MAC- и IP-заголовок (рис. 6.5).

Заголовок кадра	<p style="text-align: center;">ARP-сообщение Какой у вас MAC-адрес?</p>
-----------------	--

Рис 64. Кадр ARP-запроса состоит из заголовка и ARP'-сообщения

MAC-заголовок		IP-заголовок		Сообщение ARP-запроса Какой у вас MAC-адрес?
Получатель	Отправитель	Получатель	Отправитель	
FF-FF-FF-FF-FF-FF	02-60-8C-0 1-02-03	197.15.22.126	197.15.22.33	

Рис. 6 5. Заголовок кадра состоит MAC- и IP-заголовка

ARP-ответы

Поскольку пакет ARP-запроса посылается в режиме широковещания, его принимают все устройства в локальной сети и передают для анализа на сетевой уровень. Если IP-адрес устройства соответствует IP-адресу пункта назначения, содержащемуся в ARP-запросе, устройство откликается путем отправки источнику своего MAC-адреса. Этот процесс называется ARP-ответом. В примере, показанном на рис. 6.3, источник 197.15.22.33 запрашивает MAC-адрес получателя, имеющего IP-адрес 197.15.22.126. Получатель 197.15.22.126 принимает ARP-запрос и откликается путем отправки ARP-ответа, содержащего его MAC-адрес.

MAC-заголовок		IP-заголовок		Сообщение ARP-запроса Вот мой MAC-адрес
Получатель	Отправитель	Получатель	Отправитель	
02-60-8C-01-02-03	08-00-02-89-90-80	197.15.22.33	197.15.22.126	

Рис. 6.6. Структура ARP-ответа включает MAC- и IP-заголовок, а также сообщение ARP-ответа.

Когда устройство, создавшее ARP-запрос, получает ответ, оно извлекает MAC-адрес из MAC-заголовка и обновляет свою ARP-таблицу. Теперь, когда устройство имеет всю нужную ему информацию, оно может добавить к данным MAC- и IP-адрес пункта назначения. Устройство использует эту новую структуру кадра для инкапсуляции данных перед отправкой их по сети (рис. 6.7).

Когда данные достигают адресата, производится сравнение на канальном уровне. Канальный уровень убирает MAC-заголовок и передает данные на следующий уровень эталонной модели OSI — сетевой. Сетевой уровень анализирует данные и обнаруживает, что его IP-адрес соответствует IP-адресу назначения, содержащемуся в IP-заголовке данных. Сетевой уровень убирает IP-заголовок и передает данные следующему более высокому уровню — транспортному (уровень 4). Этот процесс повторяется, пока остаток пакета не достигнет приложения, где данные будут прочитаны.

MAC-заголовок		IP-заголовок		Данные
Получатель	Отправитель	Получатель	Отправитель	
08-00-02-89-90-80	02-60-8C-0 1-02-03	197.15.22.126	197.15.22.33	

Рис.6.7. Перед отправкой данных через сеть данные инкапсулируются с использованием новой структуры кадра


ARP-таблицы

Любое устройство в сети, принимающее широковещательный ARP-запрос, видит содержащуюся в нем информацию. Устройства используют информацию от источника для обновления своих таблиц. Если бы устройства не содержали ARP-таблиц, процесс создания ARP-запросов и ответов имел бы место каждый раз, когда устройство хотело передать данные другому устройству в сети. Это было бы чрезвычайно неэффективно и могло бы привести к слишком большому трафику в сети. Чтобы избежать этого, каждое устройство имеет свою ARP-таблицу.

Некоторые устройства поддерживают таблицы, в которых содержатся MAC- и IP-адреса всех

устройств, подключенных к той же сети. Эти таблицы — просто разделы в оперативной памяти каждого устройства. Они называются ARP-таблицами, поскольку содержат карту соответствия IP-адресов MAC-адресам (рис. 6.8). В большинстве случаев ARP-таблицы кэшируются в памяти и поддерживаются автоматически. Ситуации, когда сетевой администратор модифицирует записи в ARP-таблице вручную, редки. Каждый компьютер в сети содержит собственную ARP-таблицу. Каждый раз, когда устройство хочет передать данные по сети, оно использует для этого информацию, содержащуюся в его ARP-таблице.

ARP-таблицы должны периодически обновляться, чтобы оставаться актуальными. Процесс обновления таблиц включает не только добавление, но и удаление информации. Поскольку отправка данных по сети возможна только при использовании последней, наиболее свежей информации, устройства удаляют все данные из ARP-таблицы, возраст которых превышает установленный. Этот процесс называют *удалением по возрасту*.



Физический адрес	IP-адрес
02-60-8C-01-02-03	197.15.22.33
00-00-A2-05-09-89	197.15.22.44
09-00-20-87-92-B9	197.15.22.123
08-00-02-90-90-90	197.15.22.4

Рис. 6.8. Каждый компьютер в сети содержит ARP-таблицу

Чтобы заменить информацию, удаленную из таблицы, устройство постоянно выполняет обновления с помощью сведений, получаемых как от собственных запросов, так и от запросов, поступающих от других устройств в сети. Тот факт, что протокол ARP позволяет устройствам поддерживать рабочие ARP-таблицы актуальными, помогает в ограничении объема широковещательного трафика в локальной сети.

RARP

Как было сказано выше, для того, чтобы сетевое устройство могло отправить данные на уровень 4 (транспортный) эталонной модели OSI, необходимы и MAC-, и IP-адрес. Таким образом, MAC- и IP-адрес служат для проверки и дополнения друг друга. Чтобы получатель, принимающий данные, знал, кто их отправил, пакет данных должен содержать MAC- и IP-адреса источника. А что произойдет, если источник знает свой MAC-адрес, но не знает своего IP-адреса? Протокол, который используют устройства, если не знают своего IP-адреса, называется *протоколом обратного преобразования адреса (Reverse Address Resolution Protocol, RARP)*. Как и ARP, RARP связывает MAC-адреса с IP-адресами, чтобы сетевое устройство могло использовать их для инкапсуляции данных перед отправкой в сеть. Для использования данного протокола в сети должен присутствовать RARP-сервер, отвечающий на RARP-запросы (рис 6.9).

RARP-запросы

Представим, что источник хочет послать данные другому устройству. Однако источник знает свой MAC-адрес, но не может обнаружить собственный IP-адрес в своей ARP-таблице. Чтобы получатель мог оставить у себя данные, передать их на верхние уровни эталонной модели OSI и распознать устройство, которое отправило данные, источник должен включить в пакет данных свои MAC- и IP-адреса. Поэтому источник инициирует процесс, называемый RARP-запросом, позволяющий ему определить собственный IP-адрес. Для этого устройство создает пакет RARP-запроса и посылает его в сеть. Для того чтобы пакет ARP-запроса был замечен всеми устройствами в сети, источник использует IP-адрес широковещания.

RARP-запросы имеют такую же структуру, как и ARP-запросы (рис. 6.10). Следовательно, RARP-запрос состоит из MAC- и IP-заголовка, а также сообщения RARP-запроса. Единственное отличие в формате RARP-пакета заключается в том, что заполнены MAC-адреса источника и получателя, а

поле IP-адреса источника — пустое. Поскольку сообщение передается в режиме широковещания, т.е. всем устройствам в сети, адрес назначения записывается в виде всех двоичных единиц.

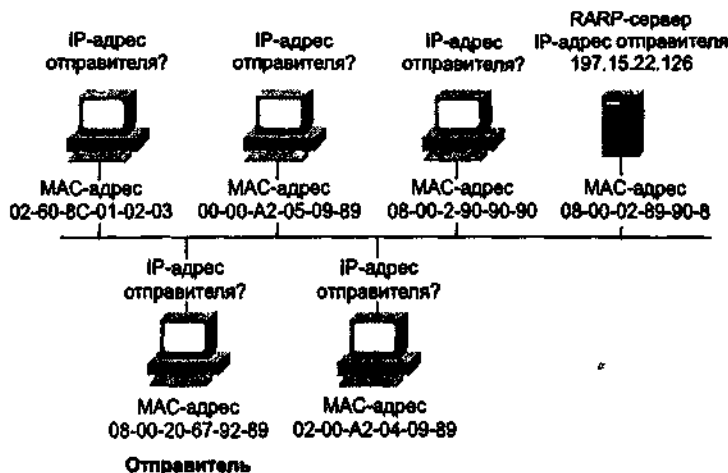


Рис. 6.9. Для ответов на RARP-запросы необходим RARP-сервер

MAC-заголовок		IP-заголовок		Сообщение RARP-запроса Какой у меня IP-адрес?
Получатель	Отправитель	Получатель	Отправитель	
00-40-33-2B-35-77	01-60-8C-01-02-03	1111111	????????	

Рис. 6.10. ARP- и RARP-запросы и имеют одинаковую структуру

Так как RARP-запрос посылается в режиме широковещания, его видят все устройства в сети. Однако только специальный RARP-сервер может отозваться на RARP-запрос. RARP-сервер служит для отправки RARP-ответа, в котором содержится IP-адрес устройства, создавшего RARP-запрос.

RARP-ответы

RARP-ответы имеют такую же структуру, как и ARP-ответы. RARP-ответ состоит из сообщения RARP-ответа, MAC- и IP-заголовка. Когда устройство, создавшее RARP-запрос, получает ответ, оно обнаруживает свой IP-адрес. На рис. 6.11 показано, что происходит в ситуации, когда сервер с IP-адресом 197.15.22.126 откликается на IP-запрос от бездисковой рабочей станции с MAC-адресом 08-00-20-67-92-89.

Когда устройство, создавшее RARP-запрос, получает ответ, оно копирует свой IP-адрес в кэш-память, где тот будет храниться на протяжении всего сеанса работы. Однако, когда терминал будет выключен, эта информация снова исчезнет. Пока же сеанс продолжается, бездисковая рабочая станция, создавшая запрос, может использовать полученную таким способом информацию для отправки и приема данных.

Маршрутизаторы и ARP-таблицы

Ранее говорилось, что порт или интерфейс, с помощью которого маршрутизатор подключен к сети, рассматривается как часть этой сети. Следовательно, интерфейс маршрутизатора, подключенный к сети, имеет тот же IP-адрес, что и сеть (рис. 6.12). Поскольку маршрутизаторы, как и любые другие устройства, принимают и отправляют данные по сети, они также строят ARP-таблицы, в которых содержатся отображения IP-адресов на MAC-адреса.

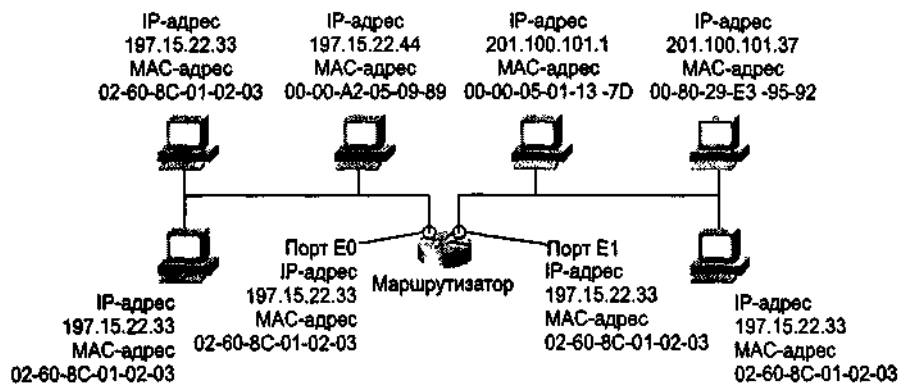


Рис. 6.13. ARP-таблица, построенная маршрутизатором

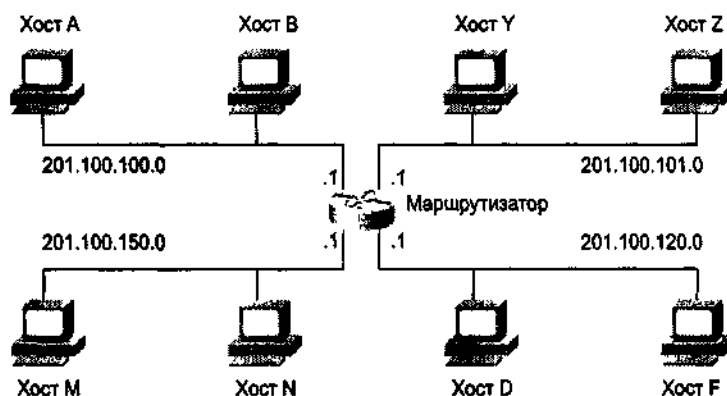
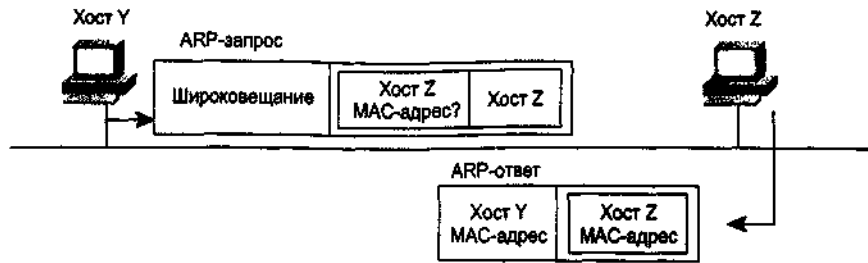


Рис. 6.14. Порты также заносятся в таблицу маршрутизации

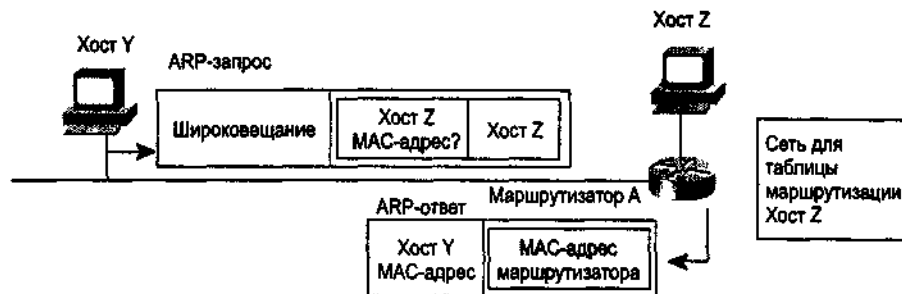
Шлюз по умолчанию

Если источник расположен в сети с номером, который отличается от номера сети назначения, и источник не знает MAC-адрес получателя, то для того, чтобы доставить данные получателю, источник должен воспользоваться услугами маршрутизатора. Если маршрутизатор используется подобным образом, то его называют *шлюзом по умолчанию (default gateway)*. Чтобы воспользоваться услугами шлюза по умолчанию, источник инкапсулирует данные, помещая в них в качестве MAC-адреса назначения MAC-адрес маршрутизатора. Так как источник хочет доставить данные устройству, а не маршрутизатору, то в заголовке в качестве IP-адреса назначения используется IP-адрес устройства, а не маршрутизатора (рис. 6.16).

Когда маршрутизатор получает данные, он убирает информацию канального уровня, использованную при инкапсуляции. Затем данные передаются на сетевой уровень, где анализируется IP-адрес назначения. После этого маршрутизатор сравнивает IP-адрес назначения с информацией, которая содержится в таблице маршрутизации. Если маршрутизатор обнаруживает отображение IP-адреса пункта назначения на соответствующий MAC-адрес и приходит к выводу, что сеть назначения подключена к одному из его портов, он инкапсулирует данные, помещая в них информацию о новом MAC-адресе, и передает их по назначению.



Пример 1: TCP/IP адресат локальный



Пример 2: TCP/IP адресат нелокальный

Рис. 6.15. Данные переправляются маршрутизатором к пункту их назначения

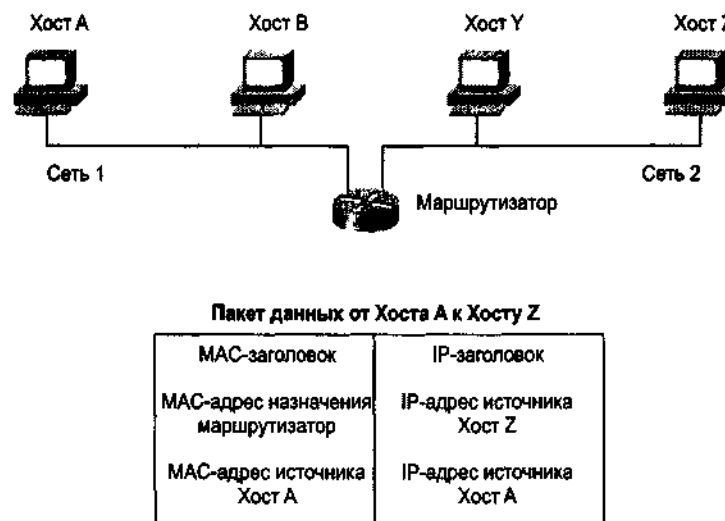


Рис. 6.16 Для доставки данных используется IP-адрес пункта назначения

Резюме

- Все устройства в локальной сети должны следить за ARP-запросами, но только те устройства, чей IP-адрес совпадает с IP-адресом, содержащимся в запросе, должны откликнуться путем сообщения своего MAC-адреса устройству, создавшему запрос.
- Если IP-адрес устройства совпадает с IP-адресом, содержащимся в ARP-запросе, устройство откликается, посылая источнику свой MAC-адрес. Эта процедура называется ARP-ответом.
- Если источник не может обнаружить MAC-адрес пункта назначения в своей ARP-таблице, он создает ARP-запрос и отправляет его в широковещательном режиме всем устройствам в сети.
- Если устройство не знает собственного IP-адреса, оно использует протокол RARP.
- Когда устройство, создавшее RARP-запрос, получает ответ, оно копирует свой IP-адрес в кэш-память, где этот адрес будет храниться на протяжении всего сеанса работы.
- Маршрутизаторы, как и любые другие устройства, принимают и отправляют данные по сети, поэтому они также строят ARP-таблицы, в которых содержатся отображения IP-адресов на MAC-адреса.

- Если источник расположен в сети с номером, который отличается от номера сети назначения, и источник не знает MAC-адрес получателя, то для того, чтобы доставить данные получателю, источник должен использовать маршрутизатор в качестве шлюза по умолчанию.

Контрольные вопросы

- Какой Internet-протокол используется для отображения IP-адресов на MAC-адреса?
 - TCP/IP
 - RARP
 - ARP
 - AARP
- Кто инициирует ARP-запросы?
 - Устройство, которое не может обнаружить IP-адрес назначения в своей ARP-таблице.
 - RARP-сервер, в ответ на запрос устройства, работающего со сбоями.
 - Бездисковые рабочие станции с пустым кэшем.
 - Устройство, которое не может обнаружить MAC-адрес пункта назначения в своей ARP-таблице.
- Какое из описаний ARP-таблицы является наилучшим?
 - Метод уменьшения сетевого трафика путем создания списка коротких путей и маршрутов к часто встречающимся пунктам назначения.
 - Способ маршрутизации данных в пределах сети, разделенной на подсети.
 - Протокол, который выполняет преобразование информации на уровне приложений.
 - Раздел оперативной памяти каждого устройства, в котором содержится карта соответствия MAC- и IP-адресов.
- Какое из описаний ARP-ответа является наилучшим?
 - Процесс отправки устройством своего MAC-адреса в ответ на ARP-запрос.
 - Кратчайший маршрут между отправителем и получателем.
 - Обновление ARP-таблиц путем перехвата и чтения сообщений, движущихся по сети.
 - Метод обнаружения IP-адреса, основанный на использовании MAC-адреса и RARP-серверов.
- Как называются две части заголовка кадра?
 - MAC- и IP-заголовок.
 - Адрес отправителя и ARP-сообщение.
 - Адрес пункта назначения и RARP-сообщение.
 - Запрос и пакет данных.
- Для чего важна актуальность ARP-таблиц?
 - Для тестирования каналов в сети.
 - Для ограничения объема широковещания.
 - Для сокращения затрат времени сетевого администратора на обслуживание сети.
 - Для разрешения конфликтов адресации.
- Зачем осуществляются RARP-запросы?
 - Источник знает свой MAC-адрес, но не знает IP-адрес.
 - Пакету данных необходимо найти кратчайший маршрут между отправителем и получателем.
 - Администратору необходимо вручную сконфигурировать систему.
 - Канал в сети нарушен, поэтому необходимо активизировать резервную систему.
- Что содержится в RARP-запросе?
 - MAC-заголовок, IP-заголовок и сообщение ARP-запроса.
 - MAC-заголовок, RARP-заголовок и пакет данных.
 - RARP-заголовок, MAC- и IP-адрес.
 - RARP-заголовок и ARP-трейлер.
- Какая из функций является уникальной для маршрутизаторов?
 - Они устанавливают зависимость между MAC-адресами и IP-адресами.
 - Они принимают широковещательные сообщения и отправляют запрашиваемую информацию.

- C. Они строят ARP-таблицы, которые описывают все сети, подключенные к ним.
 - D. Они отвечают на ARP-запросы.
10. Что происходит, если маршрутизатор не может обнаружить адрес пункта назначения?
- A. Он обращается к ближайшему серверу имен, где содержится полная ARP-таблица.
 - B. Он посылает ARP-запрос RARP-серверу.
 - C. Он находит MAC-адрес другого маршрутизатора и передает данные этому маршрутизатору.
 - D. Он отправляет пакет данных через ближайший порт, который запрашивает RARP-сервер.

Глава 7

Топологии

В этой главе

- Определение понятия *топология*
- Шинная топология, ее преимущества и недостатки
- Топология "звезда", ее преимуществ и недостатки
- Внешние терминаторы
- Активные и пассивные концентраторы
- Характеристики топологии "расширенная звезда", определение
- длины кабеля для топологии "звезда" и способы увеличения размеров области охватываемой сетью с топологией "звезда"
- Аттенюация

Введение

В главе 6, "ARP и RARP", было рассказано, каким образом устройства в локальных сетях используют протокол преобразования адреса ARP перед отправкой данных получателю. Было также выяснено, что происходит, если устройство в одной сети не знает адреса управления доступом к среде передачи данных (MAC-цреса) устройства в другой сети. В этой главе рассказывается о топологиях, используемых при создании сетей.

Топология

В локальной вычислительной сети (ЛВС) все рабочие станции должны быть соединены между собой. Если в ЛВС входит файл-сервер, он также должен быть подключен к рабочим станциям. Физическая схема, которая описывает структуру локальной сети, называется *топологией*. В этой главе описываются три типа топологий шинная, "звезда" и "расширенная звезда" (рис 7.1, 7.2)

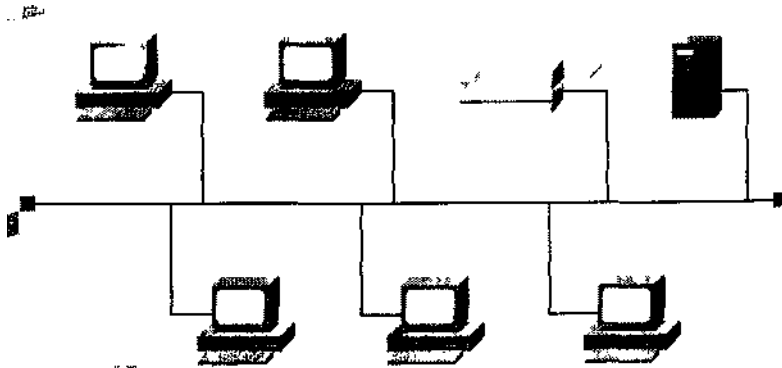


Рис 7.1 Шинная топология типична для ЛВС Ethernet, включая 10Base2 и 10Base5

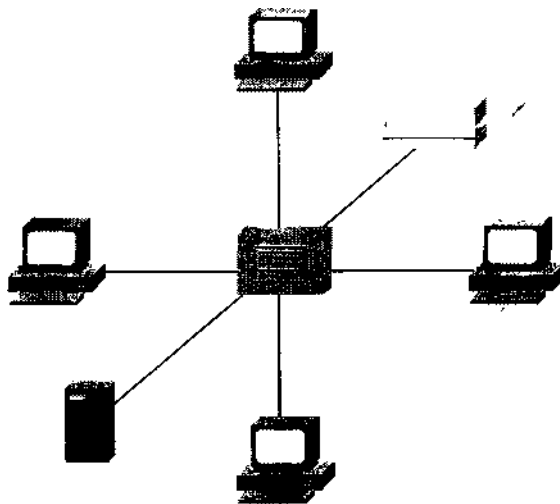


Рис. 7.2. Топология "звезда" типична для сетей Ethernet и Token Ring, которые используют в качестве центра сети концентратор, коммутатор или повторитель

Шинная топология

Шинная топология представляет собой топологию, в которой все устройства локальной сети подключаются к линейной сетевой среде передачи данных. Такую линейную среду часто называют каналом, шиной или трассой. Каждое устройство, например, рабочая станция или сервер, независимо подключается к общему шинному кабелю с помощью специального разъема (рис. 7.3). Шинный кабель должен иметь на конце согласующий резистор, или терминатор, который поглощает электрический сигнал, не давая ему отражаться и двигаться в обратном направлении по шине.

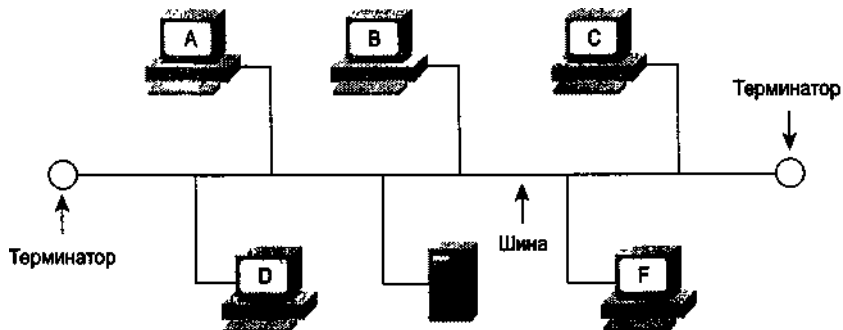


Рис. 7.3. Электрические сигналы в шинном кабеле поглощаются терминатором

Передача сигнала в сети с шинной топологией

Когда источник передает сигналы в сетевую среду, они движутся в обоих направлениях от источника (рис. 7.4). Эти сигналы доступны всем устройствам в ЛВС. Как уже известно из предыдущих глав, каждое устройство проверяет проходящие данные. Если MAC- или IP-адрес пункта назначения, содержащийся в пакете данных, не совпадает с соответствующим адресом этого устройства, данные игнорируются. Если же MAC- или IP-адрес пункта назначения, содержащийся в пакете данных, совпадает с соответствующим адресом устройства, то данные копируются этим устройством и передаются на канальный и сетевой уровни эталонной модели OSI.

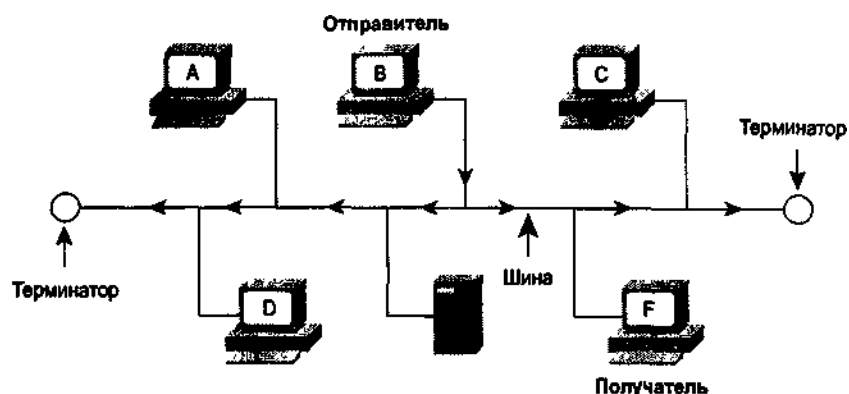


Рис. 7.4. Данные, передаваемые по сети с шинной топологией, движутся в обоих направлениях

На каждом конце кабеля устанавливается терминатор (рис. 7.4). Когда сигнал достигает конца шины, он поглощается терминатором. Это предотвращает отражение сигнала и повторный прием его станциями, подключенными к шине.

Для того чтобы гарантировать, что в данный момент передает только одна станция, в сетях с шинной топологией используется механизм обнаружения конфликтов, иначе, если несколько станций одновременно попытаются осуществить передачу, возникнет конфликт. В случае возникновения конфликта данные от каждого устройства взаимодействуют друг с другом (т.е. импульсы напряжения от каждого из устройств будут одновременно присутствовать в общей шине), и таким образом, данные от обоих устройств будут повреждаться. Область сети, в пределах которой был создан пакет и возник конфликт, называется *доменом конфликта*. В шинной топологии, если устройство обнаруживает, что имеет место конфликт, сетевой адаптер обрабатывает режим повторной передачи с задержкой. Поскольку величина задержки перед повторной передачей определяется с помощью алгоритма, она будет различна для каждого устройства в сети, и, таким образом, уменьшается вероятность повторного возникновения конфликта.

Преимущества и недостатки шинной топологии

Типичная шинная топология имеет простую структуру кабельной системы с короткими отрезками кабелей. Поэтому по сравнению с другими топологиями стоимость ее реализации невелика. Однако низкая стоимость реализации компенсируется высокой стоимостью управления. Фактически, самым большим недостатком шинной топологии является то, что диагностика ошибок и изолирование сетевых проблем могут быть довольно сложными, поскольку здесь имеются несколько точек концентрации.

Так как среда передачи данных не проходит через узлы, подключенные к сети, потеря работоспособности одного из устройств никак не сказывается на других устройствах. Хотя использование всего лишь одного кабеля может рассматриваться как достоинство шинной топологии, однако оно компенсируется тем фактом, что кабель, используемый в этом типе топологии, может стать критической точкой отказа. Другими словами, если шина обрывается, то ни одно из подключенных к ней устройств не сможет передавать сигналы.

Топология "звезда"

В сетях, использующих топологию "звезда", сетевой носитель соединяет центральный концентратор с каждым устройством, подключенным к сети. Физический вид топологии "звезда" напоминает радиальные спицы, исходящие из центра колеса (рис. 7.5). В этой топологии используется управление из центральной точки, а связь между устройствами, подключенными к сети, осуществляется посредством двухточечных линий между каждым устройством и центральным каналом или концентратором.

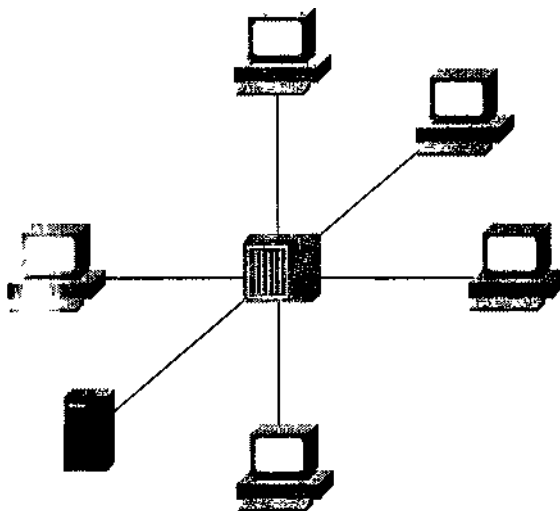


Рис. 7.5. Топология "звезда" имеет сходство с радиальными спицами колеса

Весь сетевой трафик в звездообразной топологии проходит через концентратор. Вначале данные посылаются концентратору, а затем концентратор переправляет их устройству в соответствии с адресом, содержащимся в данных.

В сетях с топологией "звезда" концентратор может быть активным или пассивным. Активный концентратор не только соединяет участки среды передачи, но и регенерирует сигнал, т.е. работает как многопортовый повторитель. Благодаря выполнению регенерации сигналов, активный концентратор позволяет данным перемещаться на более значительные расстояния. В отличие от активного концентратора, пассивный только соединяет участки сетевой среды передачи данных.

Преимущества и недостатки топологии "звезда"

Большинство проектировщиков сетей считают топологию "звезда" самой простой с точки зрения проектирования и установки. Это объясняется тем, что сетевая среда выходит непосредственно из концентратора и прокладывается к месту установки рабочей станции. Другим достоинством этой топологии является простота обслуживания: единственной областью концентрации является центр сети. Также топология "звезда" позволяет легко диагностировать проблемы и изменять схему прокладки. Кроме того, к сети, использующей топологию "звезда", легко добавлять рабочие станции. Если один из участков сетевой среды передачи данных обрывается или закорачивается, то теряет связь только устройство, подключенное к этой точке. Остальная часть сети будет функционировать нормально. Короче говоря, топология "звезда" считается наиболее надежной.

В некотором смысле достоинства топологии "звезда" могут считаться и ее недостатками. Например, наличие отдельного отрезка кабеля для каждого устройства позволяет легко диагностировать отказы, однако, это же приводит и к увеличению количества отрезков. В результате повышается стоимость установки сети с топологией "звезда". Другой пример: концентратор может упростить обслуживание, поскольку все данные проходят через эту центральную точку; однако, если концентратор выходит из строя, то перестает работать вся

сеть.

Область покрытия сети с топологией "звезда"

Максимально допустимая длина отрезков сетевого кабеля между концентратором и любой рабочей станцией (их еще называют *горизонтальной кабельной системой*) составляет 100 метров. Величина максимальной протяженности горизонтальной кабельной системы устанавливается Ассоциацией электронной промышленности (Electronic Industries Association, EIA) и Ассоциацией телекоммуникационной промышленности (Telecommunications Industry Association, TIA). Эти две организации совместно создают стандарты, которые часто называют стандартами EIA/TIA. В частности, для технического выполнения горизонтальной кабельной системы был и остается наиболее широко используемым стандарт EIA/TIA-568B.

В топологии "звезда" каждый отрезок горизонтальной кабельной системы выходит из концентратора, во многом напоминая спицу колеса. Следовательно, локальная сеть, использующая этот тип топологии, может покрывать область 200x200 метров. Понятно, бывают случаи, когда область, которая должна быть покрыта сетью, превышает размеры, допускаемые простой топологией "звезда". Представим себе здание размером 250x250 метров. Сеть с простой звездообразной топологией, отвечающая требованиям к горизонтальной кабельной системе, устанавливаемым стандартом EIA/TIA-568B, не может полностью покрыть здание с такими размерами. Как показано на рис. 7.6, рабочие станции находятся за пределами области, которая может быть накрыта простой звездообразной топологией, и, как и изображено, они не являются частью этой сети.

Когда сигнал покидает передающую станцию, он чистый и легко различимый. Однако по мере движения в среде передачи данных сигнал ухудшается и ослабевает (рис. 7.7) — чем длиннее кабель, тем хуже сигнал; это явление называется *аттенюацией*. Поэтому, если сигнал проходит расстояние, которое превышает максимально допустимое, нет гарантии, что сетевой адаптер сможет этот сигнал прочитать.

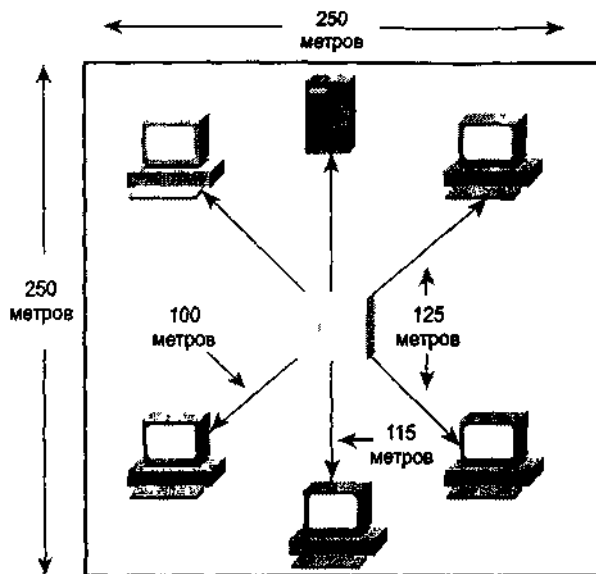


Рис 7.6 Максимально допустимая длина сетевого носителя между концентратором и любой рабочей станцией составляет 100 метров

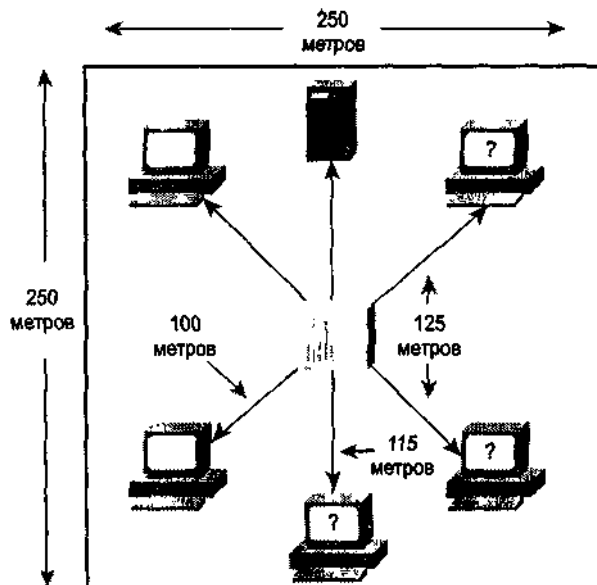


Рис 7.7 По мере движения в сетевой среде передачи данных сигнал ухудшается

Топология "расширенная звезда"

Если простая звездообразная топология не может покрыть предполагаемую область сети, то ее можно расширить путем использования межсетевых устройств, которые не дают проявляться эффекту аттенюации, результирующая топология называется топологией "расширенная звезда".

Еще раз представим себе здание размером 250x250 метров. Для того чтобы звездообразная топология могла эффективно использоваться в этом здании, ее необходимо расширить. За счет увеличения длины кабелей горизонтальной кабельной системы это делать нельзя, поскольку нельзя превышать рекомендуемую максимальную длину кабеля. Вместо этого можно использовать сетевые устройства, которые препятствуют деградации сигнала.

Чтобы сигналы могли распознаваться принимающими устройствами, используются повторители, которые берут ослабленный сигнал, очищают его, усиливают и отправляют дальше по сети. С помощью повторителей можно увеличить расстояние, на которое может простираться сеть (рис. 7.8). Повторители работают в тандеме с сетевыми носителями и, следовательно, относятся к физическому уровню эталонной модели OSI.

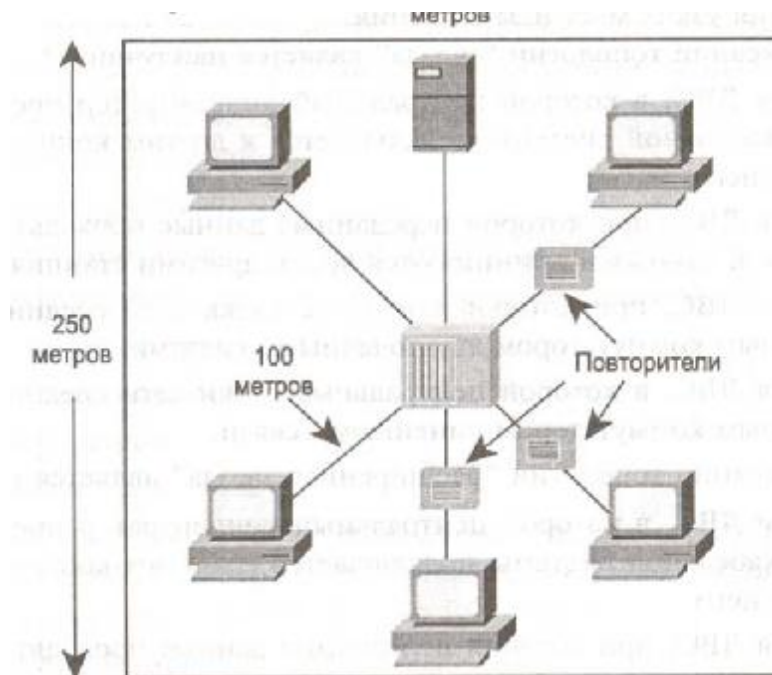


Рис. 7.8. Повторители увеличивают расстояние, на котором может функционировать сеть с топологией "звезда". Это видно на примере сети, использующей топологию "расширенной звезды"

Резюме

- Физическая схема структуры локальной сети называется топологией.
- Шинная топология представляет собой топологию, в которой все устройства локальной сети подключаются к линейной сетевой среде передачи данных. Типичная шинная топология имеет простую структуру кабельной системы с короткими отрезками кабелей.
- В локальных сетях, использующих топологию "звезда", отрезки сетевого кабеля соединяют центральный концентратор с каждым устройством, подключенным к сети.
- Максимально допустимая длина отрезка кабеля в сети с топологией "звезда" составляет 100 метров.
- Топология "звезда" может расширяться путем использования межсетевых устройств, которые предотвращают ослабление сигнала.

Контрольные вопросы

1. Какое из описаний термина "топология" является наилучшим?
 - A. Соединение компьютеров, принтеров и других устройств с целью организации обмена данными между ними.
 - B. Физическое расположение узлов сети и сетевой среды передачи данных внутри сетевой структуры предприятия.
 - C. Тип сети, который не допускает возникновения конфликтов пакетов данных.
 - D. Метод фильтрации сетевого трафика с целью уменьшения вероятности возникновения узких мест и замедления.
2. Какое из описаний топологии "звезда" является наилучшим?
 - A. Топология ЛВС, в которой центральный концентратор посредством вертикальной кабельной системы подключается к другим концентраторам, зависящим от него.
 - B. Топология ЛВС, при которой переданные данные проходят всю длину среды передачи

- данных и принимаются всеми другими станциями.
- C. Топология ЛВС, при которой конечные точки сети соединяются с общим центральным коммутатором двухточечными связями.
- D. Топология ЛВС, в которой центральные точки сети соединяются с общим центральным коммутатором линейными связями.
3. Какое из описаний топологии "расширенная звезда" является наилучшим?
- A. Топология ЛВС, в которой центральный концентратор посредством вертикальной кабельной системы подключается к другим концентраторам, зависящим от него.
- B. Топология ЛВС, при которой переданные данные проходят всю длину среды передачи данных и принимаются всеми другими станциями.
- C. Топология ЛВС, при которой конечные точки сети соединяются с общим центральным коммутатором двухточечными связями.
- D. Топология ЛВС, в которой центральные точки сети соединяются с общим центральным коммутатором линейными связями.
4. Какое из описаний терминатора является наилучшим?
- A. Секция сети, имеющая только один маршрут входа и выхода.
- B. Устройство, которое подавляет скачки напряжения до того, как они попадают на дорогостоящее оборудование.
- C. Устройство, которое устанавливается на концах тупиковых звеньев сети для отражения сигналов назад в сеть.
- D. Устройство, которое обеспечивает электрическое сопротивление на конце линии передачи для поглощения сигналов.
5. Как передается сигнал в сети с шинной топологией?
- A. Когда источник отправляет сигнал в среду передачи данных, тот движется линейно от источника.
- B. Когда источник отправляет сигнал в среду передачи данных, тот движется в обоих направлениях от источника.
- C. Сигналы в сети с шинной топологией доступны только устройству получателю.
- D. Когда источник отправляет сигнал в среду передачи данных, тот движется в одном направлении от источника.
6. Как в сетях с шинной топологией производится повторная передача с задержкой?
- A. Это делает ближайший к месту конфликта мост.
- B. Это делает терминатор.
- C. Это делается сетевым адаптером каждого устройства в том сегменте, где произошла коллизия.
- D. Это делает ближайший к месту конфликта маршрутизатор.
7. Какое преимущество дает использование топологии "звезда"?
- A. Высокая надежность.
- B. Естественная избыточность.
- C. Низкая стоимость.
- D. Требуется минимальный объем среды передачи данных.
8. Какой максимальный размер области, покрываемой сетью с топологией "звезда"?
- A. 99 x 99 метров.
- B. 100 x 100 метров.
- C. 100 x 200 метров.
- D. 200 x 200 метров.
9. Что происходит с сигналом, если длина отрезка горизонтальной кабельной системы превышает размер, устанавливаемый стандартом EIA/TIA-568B?
- A. Сигнал прерывается.
- B. Сигнал ослабевает.
- C. Сигнал движется только на установленное максимальное расстояние, а затем останавливается.
- D. Рабочие станции не посылают сообщения узлам, которые находятся на расстоянии больше максимально допустимого.
10. Что можно сделать, если размеры здания превышают установленную максимальную длину

кабеля?

- A. Добавить удвоитель сигнала.
- B. Пойти на использование более длинного кабеля.
- C. Добавить повторители.
- D. Добавить еще один концентратор.

Глава 8

Структурированная кабельная система и электропитание в сетях

В этой главе

- Некоторые стандарты, используемые проектировании сетей
- Кабель Категории 5
- Гнездо RJ45, способы его использования и установки
- Запрессовочные приспособлений
- Комната для коммуникационного оборудования
- Определение понятий ГРС и ПРС
- Коммутационная панель
- Тестирование кабелей
- Кабельная система магистрального канала ЛВС Ethernet
- Почему необходимо заземлять вычислительные устройства
- Причины электрических шумов
- Подавитель всплесков напряжения
- Источники бесперебойного питания

Введение

В главе 1 "Организация сети и эталонная модель OSI", отмечалось, что вследствие того, что компании при создании своих сетей использовали большое количество разных сетевых технологий, обмен информацией между такими сетями, использующими разные спецификации и способы практической реализации, стал затруднен. Там же было показано, что, создав модель взаимодействия открытых систем (модель OSI), Международная организация по стандартизации (ISO) предоставила производителям набор стандартов. Как известно, стандарты — это наборы правил или процедур, которые либо общеприняты, либо официально определены и играют роль своего рода концептуального плана, призванного обеспечить большую совместимость и степень взаимодействия сетевых технологий различных типов, производимых многими компаниями во всем мире.

В данной главе «рассказывается о других организациях, выпускающих стандарты на спецификации сетевых сред передачи данных, используемых в ЛВС. Здесь также будет рассказано о структурированной кабельной системе и об электрических спецификациях, используемых в ЛВС. Кроме того, в данной главе описаны некоторые методы выполнения разводки и подводки электропитания, используемые при создании сетей.

Стандарты сетевых сред передачи данных

До недавнего времени существовала в некоторой степени путанная смесь стандартов, управляющих различными аспектами сетевых сред передачи данных. Эти стандарты охватывали диапазон от правил противопожарной безопасности и строительных норм до подробных спецификаций электрических характеристик. Другие стандарты описывали методы тестирования, которые бы обеспечивали безопасную эксплуатацию и работоспособность сети. Первые стандарты, разработанные для сетевых сред передачи данных, представляли собой в основном корпоративные стандарты, созданные различными компаниями. Позднее произошло объединение многочисленных организаций и правительственных учреждений в движение за регламентацию и введение спецификаций типа кабеля, который можно использовать в сетях.

Для целей настоящей книги наибольший интерес представляют стандарты сетевых сред передачи данных, разрабатываемые и выпускаемые Институтом инженеров по электротехнике и электронике (Institute of Electrical and Electronic Engineers, IEEE), лабораторией по технике безопасности (Underwriters Laboratories, UL), Ассоциацией электронной промышленности (Electrical Industries Association, EIA) и Ассоциацией телекоммуникационной индустрии (Telecommunications Industry Association, TIA). Две последние организации совместно выпустили целый список стандартов, которые часто называют EIA/TIA-стандартами. Кроме этих групп и организаций выпуском спецификаций и технических требований, которые могут оказать влияние на тип кабеля, используемого в локальной сети, занимаются местные, окружные и национальные правительственные органы и учреждения.

Стандарты EIA/TIA-568B

Из всех упомянутых организаций наибольшее влияние на стандарты сетевых сред передачи данных оказала группа EIA/TIA. EIA/TIA-стандарты разрабатывались таким образом, чтобы указать минимальный набор требований, которые бы позволили применять различные изделия от разных производителей. Более того, эти стандарты разрабатывались так, чтобы можно было планировать и создавать локальные сети, даже не зная конкретного оборудования, которое будет устанавливаться. Таким образом, EIA/TIA-стандарты оставляют проектировщику ЛВС право выбора вариантов и пространство для расширения проекта. В частности, стандарты технических характеристик сетевой среды передачи данных EIA/TIA-568B были и продолжают

оставаться наиболее используемыми.

EIA/TIA-стандарты определяют шесть элементов кабельной системы для ЛВС: горизонтальная кабельная система, телекоммуникационные монтажные шкафы, магистральная кабельная система, помещения для оборудования, рабочие области и входные средства. В данной главе рассматривается горизонтальная кабельная система.

Горизонтальная кабельная система

Стандарты EIA/TIA-568B определяют *горизонтальную кабельную систему* как сетевую среду передачи данных, которая лежит между телекоммуникационной розеткой и горизонтальным кросс-соединением. Этот элемент включает сетевую среду передачи данных, проходящую по горизонтали, телекоммуникационную розетку или разъем, механические неразъемные соединения в монтажном шкафу и коммутационные шнуры или перемычки в монтажном шкафу. Другими словами, под термином горизонтальная кабельная система понимается сетевая среда передачи данных, лежащая в области от коммутационного шкафа до рабочей станции. На рис. 8.1 показаны кабели, обычно используемые в промежутке от монтажного шкафа до рабочей станции.

Стандарты EIA/TIA-568B содержат спецификации, определяющие технические характеристики кабеля. Они требуют прокладки двух кабелей: одного для обычной телефонной связи и другого для передачи данных, причем каждый из них должен иметь свое выходное гнездо. Из этих двух кабелей для телефонной связи должен использоваться кабель UTP с четырьмя витыми парами. В спецификациях этих стандартов определены пять категорий кабеля: категория 1, категория 2, категория 3, категория 4 и категория 5. Из них только кабели категорий 3—5 признаются годными для использования в ЛВС. Сегодня же наиболее часто рекомендуемым и используемым является кабель категории 5.

Спецификации на кабельную систему

О сетевых средах передачи данных для пяти категорий кабелей уже говорилось в данной книге. Это — кабели STP и UTP, оптоволоконный и коаксиальный кабели. Что касается кабеля STP, то стандарт EIA/TIA-568B для горизонтальной кабельной системы требует прокладки кабеля с двумя витыми парами и волновым сопротивлением 150 Ом. Для кабеля UTP стандарт требует прокладки кабеля с четырьмя витыми парами и волновым сопротивлением 100 Ом (рис. 8.2).

При применении оптоволоконного кабеля стандарт требует использования кабеля 62,5/125 мкм с двумя многомодовыми световодами. Его внешний вид показан на рис. 8.3. 50-омный коаксиальный кабель (рис. 8.4) хотя и допускается стандартом EIA/TIA-568B в качестве сетевой среды передачи данных, при установке новых сетей уже не рекомендуется.

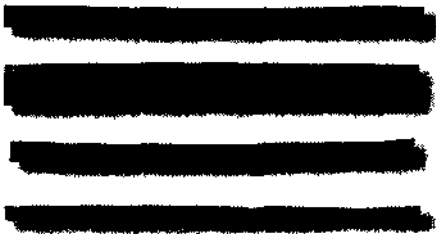


Рис. 8.1. Маркировка кабелей типа экранированная витая пара (STP) и неэкранированная витая пара (UTP) в соответствии с требованиями UL



Рис. 8.2. 100-омный кабель UTP, содержащий четыре витые пары



Рис. 8.3. Этот оптоволоконный кабель 62,5/125 мкм имеет два многомодовых световода



Рис. 8.4. Использование 50-омного коаксиального кабеля в новых проектах ЛВС не рекомендуется

В соответствии со стандартом EIA/TIA-568B максимальная длина отрезка кабеля в горизонтальной кабельной системе составляет 90 метров (или 295 футов). Это справедливо для всех кабелей UTP категории 5. Стандарт также определяет, что длина коммутационных шнуров или кроссовых перемычек в кросс-соединении горизонтальной кабельной системы не может превышать 6 метров, или 20 футов. Кроме того, стандарт EIA/TIA-568B допускает еще трехметровые (9,8 фута) соединительные кабели, которые используются для подключения оборудования, находящегося в рабочей области. Общая длина соединительных кабелей и кроссовых перемычек, используемых в горизонтальной кабельной системе, не может превышать 10 метров, или 33 фута.

Для горизонтальной кабельной системы стандарт EIA/TIA-568B требует наличия в каждой рабочей области минимум двух телекоммуникационных выходов или соединителей. Этот телекоммуникационный выход/соединитель поддерживается двумя кабелями. Первый кабель — это 100-омный кабель UTP с четырьмя витыми парами категории 3 или выше с соответствующим соединителем (рис. 8.5). Вторым кабелем может быть любой из следующих: 100-омный кабель UTP с четырьмя витыми парами и соответствующим соединителем, 150-омный кабель STP с соответствующим соединителем, коаксиальный кабель с соответствующим соединителем или двухсветоводный оптоволоконный кабель 62,5/125 мкм с соответствующим соединителем.



Рис. 8.5. Кабель UTP категории 5 и гнездовой разъем RJ45

Гнездовые разъемы телекоммуникационного выхода

Стандарт EIA/TIA-568B определяет, что в телекоммуникационном выходе горизонтальной кабельной системы для создания соединения с кабелем UTP категории 5 должен использоваться гнездовой разъем типа RJ45, имеющий прорези с цветовым кодированием. Для создания электрического соединения проводники запрессовываются в эти прорези. Гнездо также имеет соответствующую вилку, которая выглядит как стандартный разъем для подключения телефона. Однако гнездовой разъем RJ45 имеет восемь штырьков, а не четыре, как стандартная телефонная вилка, поскольку он должен разместить четыре витые пары кабеля UTP категории 5.

Установка гнездового разъема RJ45

Телекоммуникационный выход, описываемый для горизонтальной кабельной системы, обычно устанавливается на стене. Стандарт EIA/TIA-568B определяет два способа установки,

которые могут использоваться для монтажа гнездового разъема RJ45: установка на поверхность и установка заподлицо.

Установка разъема RJ45 на поверхность

Монтаж на стену устанавливаемых на поверхность гнездовых разъемов может осуществляться с помощью коробки с нанесенным на заднюю стенку клеевым составом.

Если выбирается этот метод монтажа, то следует иметь в виду, что после того, как коробки будут установлены, их перемещение уже невозможно. Это необходимо учитывать, если в будущем предвидятся изменения в предназначении помещения или в конфигурации. Другим методом, который может быть использован для установки разъемов RJ45 на поверхность, является применение коробок с винтовым креплением. При любом из этих методов разъем просто размещается в пространстве коробки.

Многие фирмы, занимающиеся монтажом сетей, предпочитают использовать разъемы RJ45, устанавливаемые на поверхность, так как они легче в установке. Благодаря тому, что они устанавливаются на поверхности стены, не требуется делать врезки в стену. Если стоимость трудозатрат является фактором при монтаже ЛВС, то это тоже может свидетельствовать в пользу таких разъемов. Кроме того, в некоторых ситуациях, например в зданиях со стенами из бетонных панелей, устанавливаемые на поверхность разъемы могут оказаться единственным приемлемым выбором.

Установка разъемов RJ45 заподлицо

До установки разъемов RJ45 в стену заподлицо следует учесть несколько факторов. Например, методы, используемые для врезки в стену с облицовочными панелями, отличаются от методов, применяемых в тех случаях, когда стена отделана штукатуркой. Поэтому важно заранее определить тип материала, из которого сделана стена. Следует также избегать размещения разъемов там, где они могут мешать отделке дверных или оконных проемов. Наконец, необходимо определить, будет ли разъем устанавливаться в коробку или с помощью низковольтной установочной скобы.

При установке разъема в облицовочную панель следует выбирать место, которое находится на высоте 12—18 дюймов (30—45 см) от пола. После того как место выбрано, необходимо посверлить в панели небольшое отверстие, а затем убедиться, что в выбранной точке сзади за ней нет каких-нибудь помех для установки. Для этого следует согнуть кусочек проволоки, вставить его в отверстие и повернуть по кругу.

Совет

Каждый раз, проводя работы на стене, в потолке или на чердаке, необходимо отключать напряжение от всех цепей, проходящих через рабочую область. Если нет уверенности в том, что вам известны все провода, проходящие через ту часть здания, где вы работаете, то необходимо следовать хорошему правилу: отключать все электропитание

Если разъем устанавливается в деревянный плинтус, то не следует делать отверстие под коробку в нижних 2 дюймах (5 см) плинтуса. При попытке установить коробку в этом месте нижний крепежный брус обшивки не даст возможности установить коробку, в которой должен будет стоять разъем, в плинтус. Выбрав место установки коробки, следует воспользоваться ей в качестве шаблона и обвести ее контур. Перед тем как выпиливать по контуру, необходимо просверлить в каждом углу начальные отверстия. Для прорезки от отверстия к отверстию можно воспользоваться либо узкой ножовкой, либо лобзиком.

После подготовки отверстия под разъем можно установить его в стену. Если разъем устанавливается в коробку, то сначала следует взять кабель и пропустить его через одну из прорезей в коробке. Затем надо вставить коробку в отверстие и надавить на нее. Коробка

плотно прижмется к поверхности стены после того, как будут затянуты винты, находящиеся сверху и снизу коробки.

Если разъем устанавливается с помощью низковольтной установочной скобы, то сначала надо приложить скобу к отверстию в стене. Гладкая сторона должна смотреть наружу. Чтобы скоба прихватилась к стене, необходимо сначала отжать верхний и нижний фланцы скобы назад. После этого первый следует отжать вверх, а второй — вниз. Теперь скоба должна быть надежно установлена.

Разводка

Производительность ЛВС непосредственно связана с тем, насколько хороши соединения. Если в горизонтальной кабельной системе в телекоммуникационных выходах используются гнездовые разъемы RJ45, то для достижения оптимальной производительности сети критически важной является последовательность выполнения разводки.

Примечание

Под *последовательностью выполнения разводки* здесь понимается то, какие провода подключаются на какую выходную клемму.

Чтобы понять, как это работает, посмотрите на разъем RJ45, внешний вид которого показан на рис. 8.5. Этот разъем имеет цветовую кодировку; цвета голубой, зеленый, коричневый и оранжевый соответствуют проводам в каждой из четырех витых пар кабеля UTP категории 5. Чтобы начать укладку проводов, сначала необходимо удалить на конце кабеля оболочку — приблизительно от 1,5 до 2 дюймов (3,8—4 см). Старайтесь удалять не больше оболочки, чем это необходимо. Если будет снят слишком большой кусок, то скорость передачи данных уменьшится. Теперь надо уложить провода в центре разъема. Необходимо всегда удерживать провода в центре, потому что если они перекосятся, скорость передачи данных замедлится. Также необходимо следить за тем, чтобы часть кабеля с оболочкой заходила внутрь корпуса разъема по крайней мере на 1/8 дюйма (0,3 см).

Затем надо разделить витые пары. Заметим, что первый цвет, который находится с левой стороны разъема, — голубой. Найдите витую пару с голубым проводом и расплетите ее. Уложите голубой провод в прорезь слева, обозначенную голубым цветом. Второй провод этой пары уложите справа в прорезь, обозначенную голубым и белым. Цвет кодировки следующей прорези на правой стороне разъема — зеленый. Найдите витую пару с зеленым проводом. Расплетите ее так, чтобы высвободился достаточный для работы отрезок провода. Уложите зеленый провод в обозначенную зеленым прорезь справа. Второй провод этой пары укладывается слева в прорезь, обозначенную зеленым и белым цветом. Продолжайте это подобным образом до тех пор, пока все провода не будут совмещены с прорезями с соответствующей цветовой кодировкой. После завершения этого шага можно приступить к запрессовке проводов в разъем.

Запрессовочные приспособления

Для запрессовки проводов в разъем необходимо использовать *запрессовочное приспособление*. Оно представляет собой устройство пружинного действия, которое вдавлиывает провод между металлическими контактами разъема, одновременно сдирая с него изоляционное покрытие. Это гарантирует хороший электрический контакт между проводом и контактами внутри разъема. Запрессовочное приспособление также отрезает лишний провод. Используя приспособление, режущее лезвие следует размещать с внешней стороны разъема. Если оно окажется внутри разъема, то провод будет отрезаться короче, чем это надо, чтобы он доходил до точки соединения. В этом случае никакого электрического соединения не получится.

Совет

Если наклонить рукоятку запрессовочного приспособления немного наружу, то оно будет обрезать лучше. Если после использования запрессовочного приспособления кусочек провода останется неотделенным, то для его удаления просто легонько покрутите его.

После завершения запрессовки всех проводов необходимо надеть на разъем пружинные зажимы и защелкнуть их. Чтобы разъем зафиксировался в лицевой панели, необходимо надавить на него с задней стороны. Делая это, необходимо удостовериться, что правая сторона разъема смотрит вверх. Затем надо лицевую панель прикрепить винтами к коробке или к установочной скобе. Если используется разъем, устанавливаемый на поверхность, то следует помнить, что коробка может вмещать фут или два (30-60 см) лишнего кабеля. Если необходимо хранить лишний кабель за коробкой, надо либо протиснуть его через крепежные хомуты, либо вскрыть вмещающий его кабельный канал, чтобы затем уложить остаток лишнего кабеля в стене. Если используется разъем, устанавливаемый заподлицо, то все, что следует сделать, — это затолкать лишний кабель назад в стенку.

Прокладка кабелей

Соединяя кабель с разъемом, следует помнить, что необходимо снимать ровно столько оболочки кабеля, сколько необходимо для заделки концов проводов. Чем на большей длине провода оголены, тем хуже будет качество соединения, а это приведет к потере сигнала. Кроме того, провода в каждой витой паре следует оставлять свитыми как можно ближе к точке подсоединения. Именно перевивка проводов и обеспечивает подавление радиочастотных и электромагнитных помех. Для кабелей UTP категории 4 максимально допустимая длина развилки составляет 1 дюйм (2,54 см). Для кабелей UTP категории 5 эта длина составляет 1/2 дюйма (1,27 см).

Если при прокладке необходимо изогнуть кабель, то радиус изгиба не должен превышать четырех диаметров кабеля (и никогда не следует изгибать кабель на угол, превышающий 90°). Если по одной трассе проходит несколько кабелей, то их следует стянуть вместе, воспользовавшись для этого кабельными хомутами. В тех случаях, когда для монтажа и закрепления кабеля необходимо использовать кабельные хомуты, накладывать их надо так, чтобы они могли слегка скользить по кабелю. Размещать хомуты вдоль кабеля следует через случайные промежутки. Ни в коем случае нельзя крепить кабель слишком плотно, так как это может повредить его. Закрепляя кабельные хомуты, следует минимизировать скручивание оболочки кабеля. Если кабель будет скручен слишком сильно, то это может закончиться порванной оболочкой. Нельзя допускать пережатия или перелома кабеля на петле. Если это произойдет, то данные будут перемещаться медленно и ЛВС будет работать с меньшей пропускной способностью.

Работая с кабелем, необходимо избегать его растягивания. При превышении тянущего усилия в 25 фунтов (11,3 кг) провода внутри кабеля могут раскрутиться. А, как уже говорилось, если пары проводов становятся не перевитыми, то это может привести к внешним и перекрестным помехам. И самое главное, никогда нельзя огибать кабелем углы. Очень важно также оставлять достаточный запас кабеля. Следует помнить, что несколько футов лишнего кабеля — это не такая уж большая цена за необходимость перекладки отрезка кабеля из-за ошибок, приведших к его растягиванию. Большинство установщиков кабелей избегают этой проблемы, оставляя достаточный запас, так что кабель может быть проложен до этажа и еще остается 2 или 3 фута с его обоих концов. Другие монтажники следуют практике оставлять так называемый *служебный виток*: несколько лишних футов кабеля, свитых в кольцо и размещаемых за навесным потолком или в другом укромном месте.

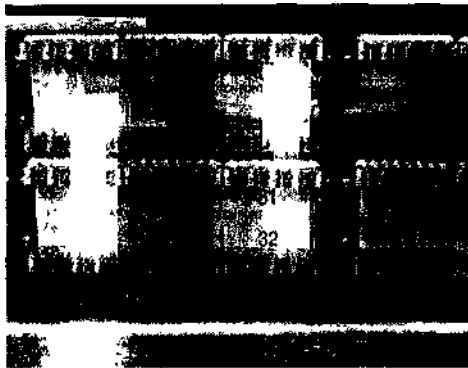


Рис. 8.6. Для заделки и крепления кабеля следует использовать кабельные хомуты, кабельные опорные балки, монтажные колодки и съемные обвязки фирмы Velcro

Для заделки и крепления кабеля необходимо использовать подходящие и рекомендуемые методики, включая применение кабельных хомутов, кабельных опорных балок, монтажных колодок и съемных пластмассовых обвязок фирмы Velcro. Никогда не следует использовать для позиционирования кабеля скобкошпигательный пистолет. Скобки могут проколоть оболочку кабеля, что приведет к потере соединения. Всегда надо помнить, что можно и чего нельзя делать при установке кабеля. На рис. 8.6 показан пример правильной установки кабеля.

Документирование и маркировка

При установке кабелей важно документировать процесс. Поэтому после установки кабелей необходимо обязательно оформить так называемую *схему нарезки*, которая представляет собой грубый чертеж прокладки отрезков кабелей. На ней также указываются номера учебных классов, офисов и других помещений, куда проложены кабели. Позднее можно будет обратиться к этой схеме нарезки для маркировки соответствующими номерами всех телекоммуникационных выходов и кабелей на монтажной панели в комнате для коммутационного оборудования. Для документирования кабельных отрезков можно также отвести страничку в журнале, что позволит иметь еще один уровень документации на все установленные кабели.

Стандарт EIA/TIA-606 требует, чтобы каждому физическому оконечному блоку был присвоен свой уникальный идентификатор, который должен быть указан на каждом физическом оконечном блоке или на прикрепляемой к нему этикетке. При использовании идентификаторов в рабочей области конец линии для подключения станции должен быть снабжен этикеткой, которую можно разместить на лицевой панели гнезда, на корпусе или на самом соединителе. Независимо от того, клеятся этикетки или вставляются, все они должны отвечать требованиям стандарта UL969 по удобочитаемости, устойчивости к стиранию и качеству крепления.

Следует избегать маркировки кабелей, телекоммуникационных выходов и монтажной панели этикетками типа "Кабинет математики г-на Зиммермана" или "Кабинет химии г-на Снайдера". Это может сбить с толку, если кому-либо несколько лет спустя надо будет выполнить какую-нибудь работу, связанную с сетевой средой передачи данных. Вместо этого необходимо использовать этикетки, которые останутся понятными и годы спустя.

Многие сетевые администраторы вводят в этикетки номера комнат, в которых они устанавливаются. Последние затем присваиваются каждому кабелю, входящему в данную комнату. Некоторые системы маркировки, особенно в случае очень больших сетей, предусматривают и цветовое кодирование. Например, голубые этикетки могут использоваться для идентификации тех кабелей, принадлежащих горизонтальной кабельной системе, которые проходят только в комнате для коммутационного оборудования, а зеленые этикетки — для идентификации кабелей, идущих в рабочую область.

Чтобы понять, как это работает, представим, что в комнате 1012 проложены четыре кабеля.

На схеме нарезки эти кабели будут обозначены 1012А, 1012В, 1012С и 1012D (рис. 8.7). Лицевые панели гнезд, где кабели 1012А, 1012В, 1012С и 1012D соединяются со шнурами подключения рабочих станций, также будут снабжены этикетками, соответствующими каждому кабелю (см. рис. 8.7).

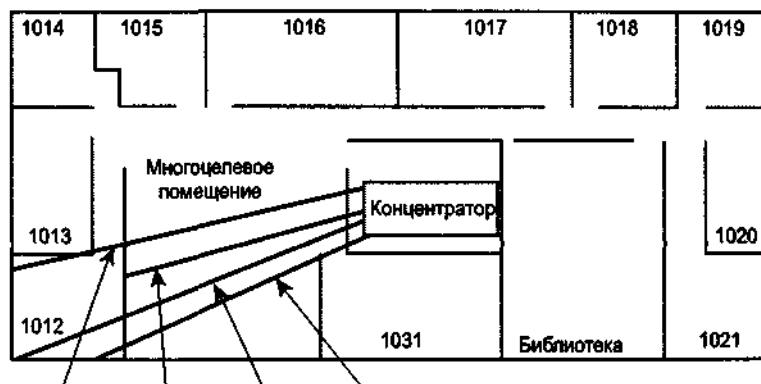


Рис. 8.7. На этой схеме нарезки показаны кабели, обозначенные как 1012А, 1012В, 1012С и 1012D

Точки подсоединения кабеля на коммутационной панели в комнате для коммутационного оборудования тоже должны снабжаться этикетками. Подключения на коммутационной панели желательно размещать так, чтобы этикетки шли в возрастающем порядке. Это позволит легко диагностировать проблемы и найти их место возникновения, если они возникнут в будущем. Наконец, как показано на рис. 8.6, и сам кабель должен на каждом конце иметь соответствующую этикетку.

Помещение для коммутационного оборудования

После успешной прокладки кабелей горизонтальной кабельной системы необходимо сделать соединения в помещении для коммутационного оборудования. Помещение для коммутационного оборудования представляет собой специально спроектированную комнату, используемую для коммутирования сети передачи данных или телефонной сети. Поскольку помещение для коммутационного оборудования служит в качестве центральной точки перехода для коммутации и коммутационного оборудования, используемого для соединения устройств в сеть, логически оно находится в центре звездообразной топологии. Обычно оборудование, находящееся в помещении для коммутационного оборудования, включает коммутационные панели, концентраторы проводных соединений, мосты, коммутаторы и маршрутизаторы. Внешний вид помещения для коммутационного оборудования показан на рис. 8.9.

Помещение для коммутационного оборудования должно быть по возможности достаточно большим, чтобы в нем могло разместиться все оборудование и коммутационное кабельное хозяйство, которое там должно быть. Естественно, размеры этого помещения могут быть различными, что зависит от размера ЛВС и типов оборудования, требующегося для ее работы. Например, оборудование, необходимое для некоторых небольших ЛВС, может занимать объем, не превышающий объема большого картотечного шкафа, тогда как большая ЛВС может потребовать полноценного машинного зала. Наконец, помещение для коммутационного оборудования должно быть достаточно большим, чтобы удовлетворить потребности роста в будущем.

Стандарт EIA/TIA-569 определяет, что должно быть минимум одно такое помещение на этаж, и устанавливает необходимость наличия дополнительного помещения для коммутационного оборудования на каждые 1000 квадратных метров, если обслуживаемая площадь этажа превышает 1000 квадратных метров или если протяженность горизонтальной кабельной системы больше 90 метров.

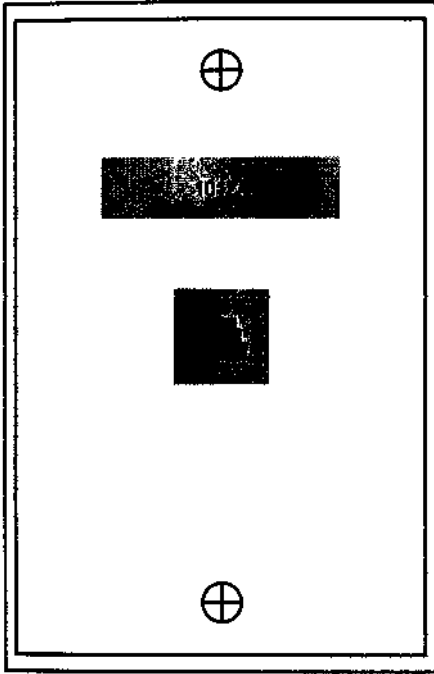


Рис 88 Лицевые панели точек соединения кабелей 1012A, 1012B, 1012C и 1012D со шнурами подключения рабочих станций должны снабжаться этикетками, соответствующими каждому кабелю. На этом рисунке показана лицевая панель с правильно установленной этикеткой 1012A

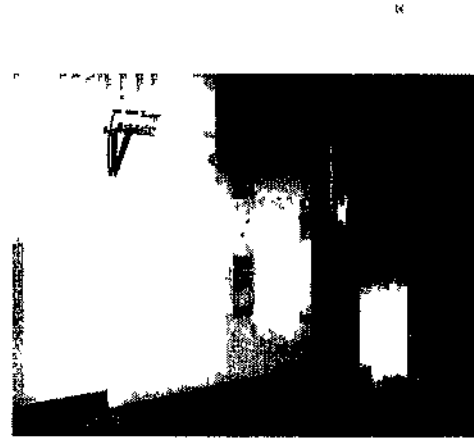


Рис 89 Основная разводка кабелей для голосовых сетей и сетей передачи данных выполняется в коммутационном шкафу

Примечание

Одна тысяча квадратных метров равна 10 000 квадратных футов. 90 метров равны приблизительно 300 футам.

Для больших сетей нет ничего необычного в наличии более одного помещения для коммутационного оборудования. Если это имеет место, тогда говорят, что сеть имеет расширенную звездообразную топологию. Обычно, когда требуется больше одного помещения для коммутационного оборудования, одно является главной распределительной станцией (ГРС) (main distribution facility), а все остальные, называемые промежуточными распределительными станциями (ПРС) (intermediate distribution facility), зависимы по отношению к ней.

Если помещение для коммутационного оборудования играет роль ГРС, то выходы всех кабелей, идущих от него в ПРС, комнаты, где размещаются компьютеры, и в помещения с коммуникационным оборудованием, находящиеся на других этажах здания, должны быть сделаны через 4-дюймовые (10 см) кабельные трубопроводы или муфтовые вставки. Аналогично, все входы кабелей в ПРС тоже должны быть сделаны через такие же 4-дюймовые кабельные трубопроводы или муфтовые вставки. Точное количество требующихся кабельных трубопроводов определяется исходя из количества оптоволоконных кабелей, кабелей STP и UTP, которые должны находиться в каждом помещении для коммутационного оборудования и в каждой комнате с компьютерами или коммуникационным оборудованием.

Любое место, выбранное для коммутационного оборудования, должно отвечать определенным требованиям по отношению к окружающей среде. Если говорить коротко, то эти требования включают электропитание, отопление, вентиляцию и кондиционирование воздуха в объемах, достаточных для поддержания в помещении температуры приблизительно 70°F (21°C), когда все оборудование ЛВС полностью функционирует. Кроме того, выбранное место должно быть защищено от несанкционированного доступа и удовлетворять всем строительным нормам и нормам техники безопасности.

Все внутренние стены или по крайней мере те, на которых будет монтироваться оборудование, должны быть облицованы клеевой фанерой толщиной 3/4 дюйма (1,9 см) с

расстоянием до основной стены минимум 1 3/4 дюйма (4,4 см) Если помещение для коммутационного оборудования является главной распределительной станцией здания, то точка входа в телефонную сеть (ТВТС) (telephone point of presence) тоже может находиться здесь В этом случае внутренние стены у точки входа в телефонную сеть и за внутренней АТС должны быть защищены от пола до потолка фанерой толщиной 3/4 дюйма, и минимум 15 футов (4,5 метра) стенового пространства должны быть выделены под заделку концов телефонных кабелей и соответствующее оборудование Кроме того, для окраски всех внутренних стен должна использоваться огнеупорная краска, удовлетворяющая всем соответствующим нормам противопожарной безопасности Настенный выключатель Для включения и выключения освещения должен размещаться непосредственно у входной двери Из-за внешних помех, генерируемых лампами дневного света, их применения следует избегать.

Использование нескольких помещений для коммутационного оборудования

Примером, когда с высокой долей вероятности будет использоваться несколько помещений для коммутационного оборудования, может служить случай объединения в сеть комплекса зданий (например, это может быть университетский городок). В сети Ethernet комплекса зданий будет присутствовать как горизонтальная кабельная система, так и система магистральных кабелей. Как показано на рис. 8.10, главная распределительная станция находится в центральном здании комплекса. В данном случае и точка входа в телефонную сеть тоже находится внутри этой станции. Кабель магистрального канала, показанный штриховой линией, идет от главной распределительной станции ко всем промежуточным распределительным станциям. Промежуточные распределительные станции имеются в каждом здании комплекса. Кроме главной распределительной станции в центральном здании находится еще и промежуточная распределительная станция, так что в зону охвата попадают все компьютеры. Горизонтальная кабельная система, обеспечивающая связь между главной и промежуточными распределительными станциями и рабочими областями, показана сплошными линиями, соединяющими компьютерные рабочие станции с промежуточными и главной распределительными станциями.

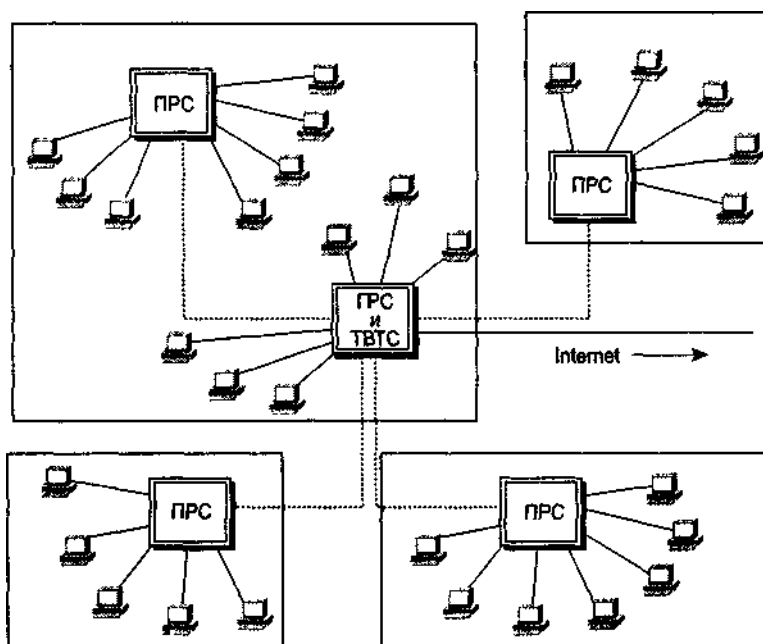


Рис. 8.10. Главная распределительная станция находится в центральном здании комплекса

Магистральная кабельная система

Точно так же, как имеется специальный термин (горизонтальная кабельная система), используемый в стандарте EIA/TIA-568 для обозначения кабелей, идущих от помещения для коммутационного оборудования к каждой рабочей области, есть специальный термин для кабельной системы, соединяющий в ЛВС Ethernet с расширенной звездообразной топологией между собой помещения для коммутационного оборудования. В стандарте EIA/TIA-568 кабельная система, соединяющая помещения для коммутационного оборудования друг с другом, называется *магистральной кабельной системой*.

Магистральная кабельная система включает отрезки магистрального кабеля, главное и промежуточные кросс-соединения, механическую арматуру для заделки концов кабелей и коммутационные шнуры, использующиеся для кроссирования кабелей магистрального канала передачи данных. Сюда также входят вертикальная сетевая среда передачи данных между помещениями для коммутационного оборудования, находящимися на разных этажах здания, сетевая среда между главной распределительной станцией и точкой входа телефонной кабельной системы и сетевая среда, используемая между зданиями, если сеть объединяет комплекс зданий.

Стандарт EIA/TIA-568 определяет четыре типа сетевых сред передачи данных, которые могут использоваться в магистральной кабельной системе: 100-омный кабель UTP, 150-омный кабель STP, оптоволоконный кабель 62,5/125 мкм и одномодовый оптоволоконный кабель. Хотя в стандарте EIA/TIA-568 упоминается еще и 50-омный коаксиальный кабель, вообще говоря, он не рекомендуется для новых проектов, и предполагается, что этот тип кабеля будет исключен при следующем пересмотре стандарта. В настоящее время в большинстве проектов для создания магистральной кабельной системы используется оптоволоконный кабель 62,5/125 мкм.

Коммутационные панели

В сетях Ethernet, использующих звездообразную топологию или расширенную звездообразную, отрезки кабелей горизонтальной кабельной системы, идущие от рабочих областей, обычно приходят на коммутационную панель. *Коммутационная панель* представляет собой устройство для межсоединений, посредством которого отрезки кабелей горизонтальной кабельной системы могут подключаться к другим сетевым устройствам, например к концентраторам или повторителям. Говоря более конкретно, коммутационная панель, как показано на рис. 8.6, представляет собой поле контактов, снабженное портами. По сути своей, как показано на рис. 8.9, коммутационная панель действует как распределительный щит, где горизонтальная кабельная система, приходящая от рабочих станций, может коммутироваться на другие рабочие станции ЛВС. В некоторых случаях коммутационная панель может быть тем местом, где устройства могут подсоединяться к глобальной сети или даже к Internet. В стандарте EIA/TIA-568A такое соединение называется *горизонтальным кросс-соединением*.

Коммутационные панели могут устанавливаться либо на стену с помощью установочных скоб, либо в стойки, либо в шкафы, оборудованные внутренними стойками и дверцами. Наиболее часто для установки коммутационных панелей используются распределительные стойки. Распределительная стойка представляет собой простой каркас для установки оборудования (коммутационных панелей, повторителей, концентраторов и маршрутизаторов), используемого в помещении для коммутационной аппаратуры. Высота стоек может составлять от 39 дюймов (99 см) до 74 дюймов (188 см). Преимуществом распределительной стойки является то, что она обеспечивает легкий доступ к оборудованию как спереди, так и сзади. Основание используется для крепления распределительной стойки к полу с целью обеспечения устойчивости. Хотя сегодня некоторые компании предлагают на рынке стойки шириной 23 дюйма (58,4 см), стандартной шириной еще с 1940-х годов остается 19 дюймов (48,2 см).

Порты коммутационной панели

Чтобы разобраться, как коммутационная панель обеспечивает межсоединения отрезков кабелей горизонтальной кабельной системы с другими сетевыми устройствами, рассмотрим ее структуру. На одной стенке коммутационной панели располагаются ряды контактов, в основном точно такие же, как в разъеме RJ45, о котором уже говорилось выше. И точно так же, как в разъеме RJ45, эти контакты имеют цветовую кодировку. Для получения электрического соединения с контактом провода запрессовываются с использованием такого же запрессовочного приспособления, которое применяется при работе с разъемами RJ45. Для получения оптимальной производительности сети здесь также критическим моментом является последовательность разводки. Поэтому, укладывая провода в коммутационной панели, необходимо, чтобы они точно соответствовали цветам у места расположения контактов. Следует помнить, что окрашенные в разные цвета проводники не являются взаимозаменяемыми.

Порты размещаются на противоположной стороне коммутационной панели. Как показано на рис. 8.11, по внешнему виду они напоминают порты, которые находятся на лицевых панелях телекоммуникационных выходов в рабочих областях. И как и в порты RJ45, в порты коммутационной панели вставляются вилки такого же размера. Подключаемые к портам коммутационные шнуры позволяют организовать межсоединения компьютеров с другими сетевыми устройствами, например с концентраторами, повторителями и маршрутизаторами, которые тоже подсоединяются к коммутационной панели.



Рис 8 11 Порты размещаются на передней стенке коммутационной панели

Структура разводки коммутационной панели

В любой ЛВС разъемы являются самым слабым звеном. Будучи неправильно установленными, разъемы могут создавать электрический шум. Плохие соединения могут также быть причиной прерывистого электрического контакта между проводами и контактами панели. Если такое происходит, то передача данных в сети прекращается или происходит со значительно меньшей скоростью. Поэтому стоит их делать правильно. Чтобы гарантировать правильность установки кабелей, необходимо следовать стандартам EIA/TIA.

Важно укладывать кабели в коммутационной панели в порядке возрастания их номеров, т.е. тех, которые были присвоены им при прокладке от рабочей области к помещению для коммутационного оборудования. Как уже говорилось выше, номера кабелей соответствуют номерам комнат, в которых размещаются подключаемые к кабелю рабочие станции. Укладка кабелей в коммутационной панели в порядке возрастания номеров позволит легко диагностировать и локализовать проблемы, если таковые возникнут в будущем.

При укладке проводов в коммутационной панели следует использовать подготовленную ранее схему нарезки. Позже можно будет снабдить коммутационную панель соответствующими этикетками. Как уже упоминалось, провода надо укладывать так, чтобы их цвета точно соответствовали цветам у места нахождения контакта. Работая, важно помнить, что конец кабеля должен располагаться по центру соответствующих ему контактов. Если проявить небрежность, то может произойти перекос проводов, что замедлит скорость передачи данных в уже полностью скоммутированной ЛВС.

Во избежание слишком длинных концов проводов край оболочки кабеля должен быть в 3/4 дюйма (0,64 см) от места расположения контактов. Хороший способ добиться этого — отмерить нужное расстояние до снятия оболочки кабеля. Для выполнения работы 1 1/2—2

дюйма (приблизительно 4-5 см) будет вполне достаточно. Надо помнить, что если концы проводов будут слишком длинными, то скорость передачи данных в сети замедлится. Опять же, не надо развивать провода в паре больше, чем это необходимо; расплетенные провода не только передают данные с меньшей скоростью, но и могут привести к возникновению перекрестных помех.

В зависимости от типа используемой коммутационной панели применяется либо запрессовочный инструмент под панель 110, либо инструмент фирмы Krone. Коммутационная панель, которая показана на рисунках, приведенных в данной главе, является панелью типа 110. Выяснить, какой инструмент понадобится, необходимо до начала работ. Запрессовочный инструмент представляет собой приспособление пружинного действия, которое одновременно делает две работы: запрессовывает проводник между двумя контактами, снимая с него изоляцию и обеспечивая тем самым электрическое соединение с контактами, и с помощью своего лезвия отрезает лишний кусок проводника.

Используя запрессовочный инструмент, следует позиционировать его так, чтобы лезвие находилось с противоположной стороны от той, с которой проводник подходит к контактам. Если пренебречь этой предосторожностью, провод будет отрезан слишком коротко, чтобы дотянуться до места формирования собственно электрического соединения.

Тестирование кабельной системы

Как объяснялось выше, фундаментом эталонной модели OSI является сетевая среда передачи данных; каждый последующий уровень модели зависит и поддерживается сетевой средой передачи данных. В данной книге уже говорилось о том, что надежность сети зависит от надежности ее кабельной системы. Многие специалисты считают ее самым важным элементом любой сети.

Поэтому после установки сетевой среды передачи данных важно определить, насколько надежна кабельная система. Даже при огромных вложениях в кабели, разъемы, коммутационные панели и другое оборудование лучшего качества, плохо выполненная установка может не позволить сети работать на оптимальном уровне. После монтажа все установленные элементы сети должны быть протестированы.

В ходе тестирования сети следует придерживаться следующих шагов.

1. Разбить систему на логически понятные функциональные элементы.
2. Записать все симптомы.
3. На основе наблюдаемых симптомов определить, какой из элементов с наибольшей долей вероятности не функционирует.
4. Используя замену или дополнительное тестирование, выяснить, действительно ли этот наиболее вероятный элемент является нефункционирующим.
5. Если подозреваемый в неправильном функционировании элемент не является источником проблемы, перейти к следующему наиболее подозрительному элементу.
6. Если нефункционирующий элемент найден, отремонтируйте его.
7. Если ремонт нефункционирующего элемента невозможен, замените его.

IEEE и EIA/TIA установили стандарты, которые позволяют после завершения установки оценить, работает ли сеть на приемлемом уровне. При условии, что сеть проходит этот тест и была сертифицирована как удовлетворяющая стандартам, данный начальный уровень качества функционирования сети может быть взят в качестве базового.

Знание базовых замеров важно, так как необходимость в тестировании не прекращается только потому, что сеть была сертифицирована как удовлетворяющая стандартам. Для гарантий оптимальности производительности сети потребность в ее тестировании будет возникать периодически. Сделать это можно путем сравнения записанных измерений, снятых в тот момент, когда было известно, что сеть работала соответствующим образом, с текущими измерениями.

Значительное ухудшение по сравнению с замерами базового уровня будет свидетельствовать о том, что с сетью что-то не в порядке.

Повторное тестирование сети и сравнение с базовым уровнем помогут выявить конкретные проблемы и позволят проследить деградацию, вызываемую старением, плохой установкой, погодными или другими факторами. Можно было бы считать, что тестирование кабелей сводится к простой замене одного кабеля другим. Однако такая замена ничего определенно не доказывает, поскольку одна общая проблема может оказывать влияние на все кабели ЛВС. По этой причине для измерений характеристик сети рекомендуется пользоваться кабельным тестером. Кабельные тестеры — это ручные приборы, которые используются для проверки кабелей на соответствие требованиям соответствующих стандартов IEEE и EIA/TIA. Кабельные тестеры разнятся по выполняемым типам тестирования. Некоторые из них могут выводить распечатки, другие — подключаться к ПК и создавать файл данных.

Кабельные тестеры

Кабельные тестеры обладают широким диапазоном функций и возможностей. Поэтому приводимый здесь перечень данных, которые могут измеряться кабельными тестерами, служит единственной цели: дать общее представление об имеющихся функциональных возможностях. Прежде всего следует определить те функции, которые наиболее полно удовлетворяют существующим потребностям, и затем сделать соответствующий выбор.

Вообще говоря, кабельные тестеры могут выполнять тесты, результаты которых характеризуют общие возможности отрезка кабеля. Сюда входит определение протяженности кабеля, обнаружение местоположения плохих соединений, получение карты соединений для обнаружения скрещенных пар, измерение аттенюации сигнала, выявление приконцевых перекрестных помех, обнаружение расщепленных пар, выполнение тестов по замеру шумов и нахождение места прохождения кабеля за стенами.

Измерение протяженности кабеля очень важно, так как величина общей длины кабельного отрезка может влиять на возможности устройств в сети по коллективному использованию сетевой среды передачи данных. Как уже говорилось, кабель, протяженность которого превышает максимальную длину, задаваемую стандартом EIA/TIA-568A, может стать причиной деградации сигнала.

Кабельные тестеры, называемые *измерителями отраженного сигнала*, измеряют протяженность разомкнутого или короткозамкнутого кабеля. Делают это они путем посылки по кабелю электрического импульса. Затем прибор измеряет время поступления сигнала, отраженного от конца кабеля. Как можно ожидать, точность измерений расстояний, обеспечиваемых этим методом, лежит в пределах 2 футов (0,61 м).

Если при установке ЛВС используется кабель UTP, то измерения расстояния могут быть использованы для определения качества соединений на коммутационной панели и в телекоммуникационных выходах. Чтобы понять, почему это так, необходимо немного больше знать о принципе работы измерителя отраженного сигнала.

Замеряя протяженность кабеля, измеритель отраженного сигнала посылает электрический сигнал, который отражается, натолкнувшись на самое удаленное разомкнутое соединение. Представим теперь, что этот прибор используется для определения отказавших соединений на отрезке кабеля. Начинают тестирование с подключения прибора к коммутационному шнуру на коммутационной панели. Если измеритель отраженного сигнала показывает расстояние, соответствующее расстоянию до коммутационной панели, а не до какой-либо более удаленной точки, то тогда понятно, что существует проблема с соединением. Аналогичная процедура может быть использована и на противоположном конце кабеля для выполнения измерений через разъем RJ45, находящийся в точке телекоммуникационного выхода.

Карты соединений

Чтобы показать, какие пары проводников кабеля соединены с какими контактами

наконечника или концевого разъема, кабельные тестеры используют функцию, которая называется *картированием соединений*. Такой тест применяется для того, чтобы определить, правильно ли монтажники подключили провода к вилке или гнезду, или это было сделано в обратном порядке. Проводники, подсоединенные в обратном порядке, называются *скрещенными парами* и являются общей проблемой, характерной для установки кабелей UTP. Как показано на рис. 8.12 и 8.13, если в кабельной системе ЛВС на основе кабелей UTP обнаруживаются скрещенные пары, то соединение считается плохим. В этом случае разводка проводников должна быть переделана.

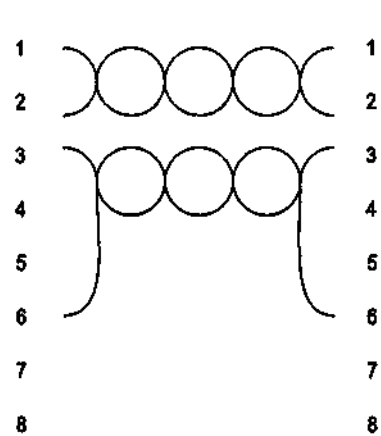


Рис. 8.12. Правильная разводка

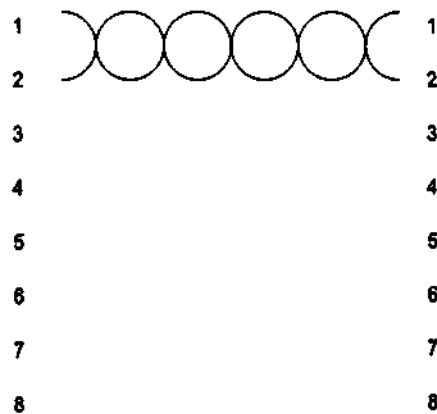


Рис. 8.13. Неправильная разводка; видно наличие скрещенных пар

Электропитание

Электричество, достигнув здания, дальше подводится к рабочим станциям, серверам и сетевым устройствам по проводам, упрятанным в стены, полы и потолки. Как следствие, в таких зданиях шум от линий электропитания переменного тока имеется повсюду. Если на это не обратить внимания, то шум от линий подачи электропитания может стать проблемой для работы сети.

Фактически, и это знает каждый, кто достаточно поработал с сетями, для возникновения ошибок в компьютерной системе может оказаться достаточно шума от линий переменного тока, идущего от расположенного поблизости видеомонитора или привода жесткого диска. Этот шум маскирует полезные сигналы и не позволяет логическим вентилям компьютера распознавать передние и задние фронты прямоугольных сигналов. Данная проблема может еще более усугубляться плохим заземлением компьютера.

Заземление

В электрооборудовании с защитным заземлением провод защитного заземления всегда подключается ко всем открытым металлическим частям оборудования. В компьютерном оборудовании материнские платы и цепи компьютера электрически соединены с шасси и, следовательно, с проводом защитного заземления. Это заземление используется для рассеивания статического электричества.

Целью соединения защитного заземления с открытыми металлическими частями компьютерного оборудования является предотвращение попадания на металлические части опасного для жизни высокого напряжения, вызванного нарушением проводки внутри устройства.

Примером нарушения проводки, которое может произойти в сетевом устройстве, является случайное соединение провода, находящегося под напряжением, с шасси. Если происходит такое нарушение, то провод защитного заземления, подсоединенный к устройству, будет играть роль низкоомного пути к земле. При правильной установке низкоомный путь,

обеспечиваемый проводом защитного заземления, имеет достаточно низкое сопротивление и позволяет пропускать достаточно большой ток, чтобы не допустить возникновения опасных для жизни напряжений. Более того, поскольку теперь существует прямая цепь, соединяющая точку под напряжением с землей, это приведет к активизации защитных устройств, например пакетных выключателей. Разрывая цепь к трансформатору, пакетные выключатели остановят поток электронов и предотвратят возможность опасного удара электрическим током.

Большие здания часто требуют наличия более одного заземления. Отдельные заземления для каждого здания также необходимы и для комплекса зданий. К сожалению, заземления различных зданий почти никогда не бывают одинаковыми. Да и разные земли одного здания также могут отличаться друг от друга. Ситуация, когда заземленные провода в разных местах имеют немного отличающийся потенциал (напряжение) по сравнению с общим проводом и активными проводами, может представлять серьезную проблему.

Чтобы разобраться в этом вопросе, предположим, что провод заземления в здании А имеет немного другой потенциал по сравнению с общим и активными проводами, чем провод заземления в здании В. Как следствие, внешние корпуса компьютерных устройств, находящихся в здании А, будут иметь потенциал (напряжение), отличающийся от потенциала внешних корпусов компьютерного оборудования, находящегося в здании В. Если теперь создается цепь, связывающая компьютерные устройства в здании А с компьютерными устройствами в здании В, то от отрицательного источника к положительному потечет электрический ток и каждый, кто коснется какого-либо устройства, стоящего этой цепи, может получить неприятный удар. Кроме того, этот плавающий потенциал способен серьезно повредить миниатюрные микросхемы памяти компьютера.

Если все работает правильно и в соответствии со стандартами IEEE, разницы в напряжении между сетевой средой передачи данных и шасси сетевого устройства быть не должно. Однако не всегда все происходит так, как думается. Например, при некачественном соединении провода заземления в точке выхода кабеля между кабельной системой ЛВС на основе кабеля UTP и шасси сетевого устройства могут возникнуть фатальные напряжения.

В настоящее время большинство фирм, занимающихся установкой сетей, рекомендуют применять в магистральной кабельной системе, соединяющей помещения для коммутационного оборудования на разных этажах здания, а также в разных зданиях, оптоволоконный кабель. Причина этого проста: вполне обычна ситуация, когда разные этажи здания питаются от различных силовых трансформаторов. Различные силовые трансформаторы могут иметь разные соединения с заземлением, а это приводит к тем проблемам, которые только что рассматривались. Непроводящие электрический ток оптические волокна исключают эту проблему.

Опорная земля сигналов

Когда компьютер, подсоединенный к сети, принимает данные в виде цифровых сигналов, он должен каким-то образом распознавать их. Он делает это путем измерения и сравнения принимаемых 3- или 5-вольтовых сигналов с опорной точкой, называемой *опорной землей сигналов*. Для правильной работы опорная земля сигналов должна находиться как можно ближе к цифровым цепям компьютера. Инженеры решают это, вводя в печатные платы земляную плоскость. Корпус компьютера используется в качестве общей точки соединения земляных плоскостей плат, создавая опорную землю сигналов. (В данной главе на рисунках с изображениями сигналов опорная земля устанавливает положение линии нулевого напряжения.)

В идеале опорная земля сигналов должна быть полностью изолирована от земли электропитания. Подобная изоляция не позволяла бы утечкам цепей переменного тока и всплескам напряжения воздействовать на опорную землю сигналов. Однако инженеры посчитали непрактичным изолировать опорную землю сигналов подобным образом. Вместо этого шасси вычислительного устройства служит как в качестве опорной земли сигналов, так и в качестве земли цепей питания переменного тока.

Из-за того что существует связь между опорной землей сигналов и землей питания, проблемы с

землей питания могут привести к помехам в работе систем обработки данных. Такие помехи могут быть трудно обнаруживаемыми и затрудняющими отслеживание источника. Обычно это является следствием того факта, что подрядчики, выполняющие работы по прокладке сетей электропитания и сетей данных, не обращают внимания на длину нейтральных проводов и проводов заземления, идущих к каждой розетке электропитания. К сожалению, если эти провода имеют большую длину, они могут служить для электрического шума антенной. И этот шум накладывается на цифровые сигналы, которые компьютер должен иметь возможность распознать.

Влияние электрического шума на цифровые сигналы

Чтобы понять, как электрический шум влияет на цифровые сигналы, представим, что необходимо послать по сети данные, выражаемые двоичным числом 1011001001101. Компьютер преобразовывает двоичное число в цифровой сигнал. На рис. 8.14 показано, как выглядит цифровой сигнал для числа 1011001001101.

Этот цифровой сигнал посылается по сети получателю. Случилось так, что получатель оказался рядом с розеткой электропитания с длинными нейтральным и земляным проводами. Для электрического шума эти провода работают как антенна. На рис. 8.15 показан внешний вид электрического шума. Вследствие того, что шасси компьютера получателя используется как в качестве земли электропитания, так и в качестве опорной земли сигналов, шум накладывается на цифровой сигнал, принимаемый компьютером. На рис. 8.16 показано, что происходит с сигналом, когда он складывается с электрическим шумом. И теперь, из-за того, что шум накладывается сверху на сигнал, компьютер читает его не как число 1011001001101, а как 1011000101101 (рис. 8.17).

Чтобы избежать проблем, связанных с электрическим шумом, важно работать в тесном сотрудничестве с подрядчиком, прокладывающим цепи электропитания, и электроэнергетической компанией. Это позволит иметь наилучшее и самое короткое заземление в сети питания. Один из способов достижения такой цели состоит в том, чтобы посмотреть стоимость получения возможности работы с одним силовым трансформатором, выделенным на всю область установки ЛВС. Если такой вариант допустим, тогда можно проконтролировать подключение к такой выделенной сети электропитания всех других устройств. Накладывая ограничения на то, как и где подключаются такие устройства, как моторы или сильноточные электрические нагреватели, можно в значительной степени исключить влияние от генерируемого ими электрического шума.

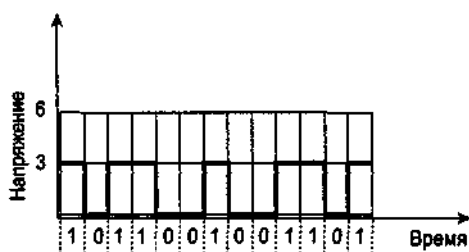


Рис. 8.14. Цифровой сигнал, соответствующий числу 1011001001101

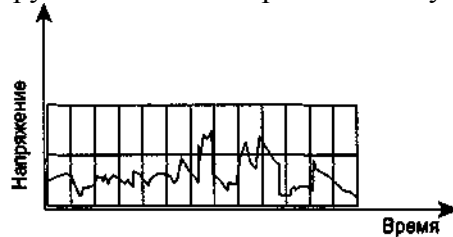


Рис. 8.15. На этой диаграмме показан сигнал электрического шума



Рис. 8.16. Шум накладывается на цифровой сигнал, принимаемый компьютером

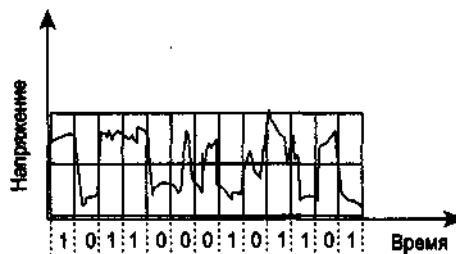


Рис. 8.17. Из-за того что электрический шум накладывается поверх сигнала, компьютер читает его как число 1011000101101

Работая с подрядчиком, выполняющим монтаж сети электропитания, необходимо потребовать установки отдельных силовых распределительных панелей, называемых *распределительными щитами*, для каждого офисного помещения. Поскольку провода нейтрали и земли от каждой силовой розетки собираются на распределительном щите, такой шаг увеличит шанс добиться уменьшения длины земли сигналов. Хотя установка отдельных силовых распределительных панелей и увеличит начальную стоимость сети электропитания, она уменьшит длину проводов заземления и ограничит возможность появления забивающих сигналы электрических шумов нескольких типов.

Подавители перенапряжения

Подавители перенапряжения являются эффективным средством в решении проблем, связанных с перепадами и всплесками напряжения. Кроме того, важно, чтобы все устройства в сети были защищены подавителями перенапряжения. Как правило, подавители перенапряжения устанавливаются на стенную розетку электропитания, к которой подключается сетевое устройство. Подавители перенапряжения такого типа имеют схемы, спроектированные для предотвращения повреждения сетевого устройства от перенапряжения или всплесков в сети питания. Защищают они сетевое устройство путем перенаправления избыточного напряжения, возникающего в результате перенапряжения или всплеска, на землю. Проще говоря, подавитель перенапряжения представляет собой устройство, которое способно без повреждения поглощать большие токи.

Когда подавители перенапряжения, расположенные в близости от сетевых устройств, каналируют высокое напряжение на общую землю, это может создать высокую разность напряжений между сетевыми устройствами. В результате эти устройства могут потерять данные или, в некоторых случаях, получить повреждение своих цепей.

Чтобы избежать этих проблем, вместо установки индивидуальных подавителей перенапряжения у каждой рабочей станции следует использовать подавители перенапряжения промышленного класса. Как показано на рис. 8.18, такие подавители должны устанавливаться у каждой силовой распределительной панели, а не в непосредственной близости от сетевых устройств. Размещение подавителей перенапряжения промышленного класса рядом с силовой панелью может уменьшить воздействие на сеть отводимых на землю перенапряжений и выбросов.

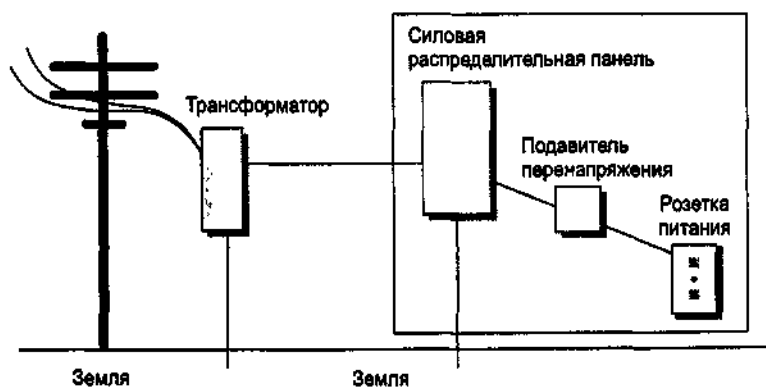


Рис. 8.18. Подавитель перенапряжений должен размещаться у каждой силовой распределительной панели

Перебои электропитания

Перебои электропитания происходят тогда, когда что-то, например удар молнии, создает перегрузку в сети и приводит к срабатыванию автоматического выключателя. Поскольку автоматические выключатели спроектированы таким образом, что обеспечивают автоматическое возвращение во включенное состояние, они могут работать от окружающей сети электропитания, в которой находится источник коротки, восстанавливая подачу электричества.

Однако могут иметь место и более длительные перебои в подаче электроэнергии. Обычно такое случается, когда какое-нибудь событие, например сильный шторм или наводнение, вызывает физическое повреждение в системе передачи электроэнергии. В отличие от краткосрочных перебоев электропитания, восстановление в случае подобных перерывов в обслуживании, как правило, зависит от ремонтных бригад.

Если говорить в общем, то источники бесперебойного питания (ИБП) спроектированы так, чтобы справляться только с краткосрочными перебоями в подаче электроэнергии. (Более подробно об ИБП рассказывается в следующем разделе.) Если ЛВС требует бесперебойной подачи электропитания даже при отсутствии электричества в течение нескольких часов, то в дополнение к резервному питанию, обеспечиваемому ИБП, необходима установка генератора.

Источники бесперебойного питания

Перебои в электропитании, вызываемые провисанием проводов или являющиеся следствием отключений, имеют относительно небольшую продолжительность. Проблема таких перебоев решается наилучшим образом с помощью источников бесперебойного питания (ИБП). Уровень обеспечения ЛВС источниками бесперебойного питания зависит от таких факторов, как величина бюджета, тип услуг, которые ЛВС должна предоставлять пользователям, периодичность возникновения подобных перебоев в регионе, а также от типичной продолжительности перебоев, если они случаются.

Резервным питанием должен быть обеспечен каждый стоящий в сети файл-сервер. Если требуются мощные концентраторы проводных соединений, то они тоже должны поддерживаться резервными источниками питания. Наконец, в сетях с расширенной звездообразной топологией, где используются такие устройства межсетевого взаимодействия, как мосты и маршрутизаторы, они также должны быть снабжены резервным питанием, чтобы избежать отказов в системе. Где возможно, резервное питание должно быть обеспечено для всех рабочих областей. Как известно каждому сетевому администратору, мало толку иметь в рабочем состоянии серверы и систему коммутации, если нельзя гарантировать, что компьютеры не отключатся до тех пор, пока пользователи смогут сохранить свои редактируемые текстовые файлы и файлы электронных таблиц.

В общем случае ИБП состоит из аккумуляторных батарей, зарядного устройства инвертора. Функция инвертора заключается в преобразовании низковольтного напряжения постоянного тока от аккумуляторных батарей в напряжение переменного тока, обычно подаваемого из сети электропитания на сетевые устройства. Зарядное устройство спроектировано так, чтобы поддерживать аккумуляторные батареи в состоянии полного заряда в те периоды, когда силовая сеть функционирует нормально. В соответствии с общим эмпирическим правилом, чем больше батареи в ИБП, тем больше времени он будет способен поддерживать сетевые устройства во время перебоя электропитания.

ИБП разработаны и поставляются рядом производителей и отличаются по следующим характеристикам: емкостью батарей, мощностью, которую можно отбирать от инвертора, и работает ли инвертор все время или только тогда, когда напряжение на входе достигает конкретного уровня. В общем случае, чем больше функций имеет ИБП, тем он дороже.

Обычно ИБП, которые имеют небольшое количество функций и стоят не дорого, используются только в качестве резервных систем электропитания. Это означает, что они работают в режиме мониторинга электросети. Только если возникает проблема, ИБП включает инвертор, питаемый от аккумуляторных батарей. Время, необходимое для такого переключения, называется *временем перехода* и имеет продолжительность всего несколько миллисекунд. Поскольку время перехода настолько мало, это, как правило, не составляет проблемы для большинства современных компьютеров, которые спроектированы так, что способны работать по инерции на собственных источниках питания по крайней мере сотню миллисекунд.

ИБП, которые имеют больше функций и стоят дороже, обычно работают в интерактивном режиме. Это означает, что они постоянно подают электроэнергию от инверторов, подпитываемых от аккумуляторных батарей. При этом батареи продолжают заряжаться от

сети электропитания. Поскольку инверторы поставляют "свежевыработанное" напряжение переменного тока, такие ИБП дают дополнительную выгоду, гарантируя непопадание на обслуживаемые ими устройства выбросов напряжения из электросети. Но как только напряжение в сети падает, аккумуляторные батареи ИБП плавно переключаются из режима заряда в режим подачи напряжения на инвертор. Как следствие, ИБП этого типа эффективно уменьшают необходимое время перехода до нуля.

Другие ИБП попадают в гибридную категорию. Хотя они считаются интерактивными системами, свои инверторы они не держат все время включенными. Вследствие существования таких различий надо обязательно ознакомиться с функциями ИБП, которые планируется ввести в качестве элемента ЛВС.

В любом случае хороший ИБП должен уметь обмениваться информацией с файл-сервером. Это важно, поскольку файл-сервер тогда будет предупрежден о необходимости закрытия файлов при снижении мощности батарей ИБП до нижнего предела. Дополнительно после возникновения перебоя в электропитании хороший ИБП сообщает серверу о том, что тот начинает питаться от аккумуляторных батарей, и передает эту информацию всем рабочим станциям в сети.

Резюме

- Типы сетевых сред передачи данных, которые могут использоваться в горизонтальной кабельной системе ЛВС, определяются стандартами EIA/TIA.
- Каждый раз после установки кабеля очень важно документировать сделанное.
- Помещение для коммутационного оборудования представляет собой специально спроектированную комнату, используемую для коммутирования сети передачи данных и телефонной сети.
- Магистральная кабельная система включает отрезки магистрального кабеля, главное и промежуточные кросс-соединения, механические кабельные наконечники и коммутационные шнуры, используемые для кросс-соединений магистральных кабелей.
- IEEE и EIA/TIA установили стандарты, которые позволяют после завершения установки сети оценить, работает ли она на приемлемом уровне.
- Кабельные тестеры могут определить общие характеристики отрезка кабеля. Чтобы показать, какие пары проводников кабеля соединены с какими контактами наконечника или концевого разъема, кабельные тестеры используют так называемое картирование соединений.
- Если не уделить соответствующего внимания шуму от силовых линий переменного тока, то он может стать источником проблем в сети.
- Целью соединения защитной земли с открытыми металлическими частями компьютерного оборудования является предотвращение попадания на такие металлические части опасного для жизни высокого напряжения, вызванного нарушением проводки внутри устройства.
- Подавители перенапряжения являются эффективным средством в решении проблем, связанных с перепадами и всплесками напряжения.
- Проблемы, связанные с провисанием проводов и отключениями электричества, наилучшим образом решаются с помощью источников бесперебойного питания.

Контрольные вопросы

1. Какой класс кабелей UTP из описываемых в стандарте EIA/TIA-568B является наиболее часто рекомендуемым и используемым при установке ЛВС?
 - A. Категории 2.
 - B. Категории 3.
 - C. Категории 4.
 - D. Категории 5.
2. Какой тип оптоволоконного кабеля требуется в соответствии со стандартом EIA/TIA-568B для горизонтальной кабельной системы?
 - A. 100-омный кабель с двумя витыми парами.
 - B. 150-омный кабель с двумя витыми парами.
 - C. Двухволоконный многомодовый кабель 62,5/125 мкм.
 - D. Четырехволоконный многомодовый кабель 62,5/125 мкм.
3. Какой тип гнездового разъема должен использоваться для создания соединений с кабелем UTP категории 5 в горизонтальной кабельной системе?
 - A. RJ45.
 - B. TIA74.
 - C. UTP 55.
 - D. EIA45.
4. Для чего используется запрессовочное приспособление?
 - A. Для проверки сетевого соединения.
 - B. Для надежного крепления кабеля к монтажной арматуре потолка.
 - C. Для крепления этикеток к кабелям.
 - D. Для создания электрического соединения между кабелем и гнездовым разъемом.
5. Для чего используется схема нарезки?
 - A. Для содержания кабелей в порядке и без захлестов.
 - B. Для размещения соответствующих номеров на телекоммуникационных вы ходах и коммутационной панели.
 - C. Для решения проблем, связанных с перекрестными помехами, путем сверки с записями в таблице.
 - D. Для преобразования кодов IEEE в коды EIA и наоборот.
6. В чем разница между главной распределительной станцией и промежуточной распределительной станцией?
 - A. На главной распределительной станции стоят главный сетевой сервер и основные сетевые устройства, а на промежуточной — только необходимые дополнительные маршрутизаторы и повторители.
 - B. Главная распределительная станция располагается в сети на нижнем этаже многоэтажного здания, а промежуточные распределительные станции — на верхних этажах.
 - C. На главной распределительной станции находятся все необходимые сети мосты, концентраторы, маршрутизаторы и порты, а на промежуточной распределительной станции — только необходимые повторители.
 - D. Главная распределительная станция является основной коммуникационной комнатой и центральной точкой сети, тогда как промежуточная распределительная станция является вторичной коммуникационной комнатой, зависимой от главной распределительной станции.
7. Какое из определений наилучшим образом описывает функцию коммутационной панели?
 - A. Служит для временного решения проблем в сети.
 - B. Служит в качестве концентратора для создаваемых на короткий срок сетей, часто встречающихся на съездах и шоу.
 - C. Служит в качестве коммутатора, где кабели горизонтальной кабельной системы от рабочих станций могут соединяться с другими рабочими станциями, образуя сеть.
 - D. Служит в качестве центра сети Token Ring и управляет прохождением и освобождением маркера.
8. Какова роль коммутационных шнуров?

- A. Кроссируют компьютеры, выведенные на коммутационную панель, позволяя функционировать ЛВС.
 - B. Служат в качестве средства временного решения проблем в кабельной системе сети.
 - C. Соединяют кабели вместе при изменении конфигурации сети.
 - D. Позволяют сетевому администратору реконфигурировать ЛВС с минимальным количеством новых отрезков кабелей.
9. Какова цель заземления компьютерного оборудования?
- A. Предотвращение попадания на металлические части опасного для жизни напряжения, вызванного нарушением проводки внутри устройства.
 - B. Соединение защитной земли с незаизолированными металлическими частями компьютерного оборудования, с тем чтобы на нее могли быть отведены незначительные перенапряжения в сети электропитания.
 - C. Для предупреждения возможности повреждения материнской платы или ОЗУ от воздействия перенапряжения в электросети.
 - D. Для предотвращения попадания в компьютер повышенного напряжения, которое могло бы нанести вред конечному пользователю.
10. Какое определение наилучшим образом описывает ИБП?
- A. Устройство, которое гасит избыточное напряжение в сети электропитания, возникающее из-за удара молнии
 - B. Резервное устройство, которое обеспечивает электропитание во время его отсутствия в электросети.
 - C. Устройство, которое позволяет избежать перекоммутации сети в случае продолжительных флуктуации питания.
 - D. Устройство, которое обеспечивает электропитанием многопутевое соединение между компьютерами.

Глава 9

Уровни приложений, представлений, сеансовый и транспортный

В этой главе...

- Уровень приложений, представлений, сеансовый и транспортный уровни
- Процесс установления соединения с одноранговой системой
- Применение управления потоком
- Работа с окнами соответствующих процессов
- Процесс подтверждений, методы идентификации сигналов подтверждения и их цели.

Введение

В главе 8, "Структурированная кабельная система и электропитание в сетях", рассказывалось о структурированной кабельной системе и электрических спецификациях, используемых в локальных вычислительных сетях (ЛВС). Кроме того, в ней рассматривались методики подключения кабелей и сети электропитания, применяемые при создании сетей передачи данных.

В данной главе речь пойдет о четырех верхних уровнях эталонной модели взаимодействия открытых систем (модели OSI): уровне приложений, представлений, сеансовом и транспортном уровнях. Будут также кратко объяснены функции каждого из этих уровней и тех конкретных приложений, за которые они отвечают. Транспортный уровень рассматривается более подробно; здесь будет описан весь процесс передачи данных от отправителя получателю. Наконец, в данной главе будут описаны функции и процессы, используемые на транспортном уровне для обеспечения надежной доставки данных, а также для обеспечения эффективного управления трафиком.

Уровень приложений

В контексте эталонной модели OSI уровень приложений (уровень 7) поддерживает коммуникационную составляющую приложения. Как изображено на рис. 9.1, компьютерные приложения могут запрашивать только информацию, находящуюся в машине, на которой исполняется приложение. На рис. 9.1 показано несколько типов компьютерных прикладных программ. Броузеры Netscape Navigator и Internet Explorer являются, вероятно, наиболее знакомыми из них.

Текстовый процессор может включать составляющую, решающую задачу пересылки файлов, которая позволяет пересылать документ по сети в электронном виде. Данная составляющая пересылки файлов квалифицирует текстовый процессор как приложение в контексте модели OSI и принадлежит уровню 7 этой модели. Web-броузеры, например Netscape Navigator и Internet Explorer, тоже имеют свои составляющие пересылки файлов. Примером их работы может быть случай, когда вы заходите на Web-сервер: Web-страницы пересылаются на ваш компьютер.

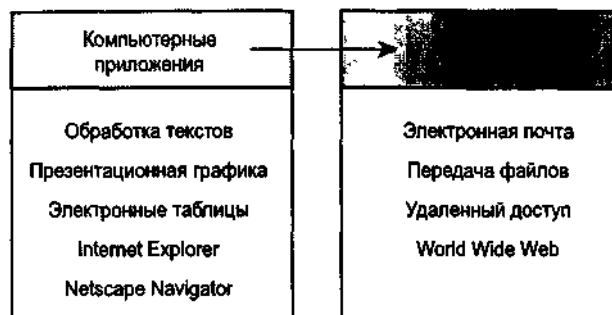


Рис. 9.1. Коммуникационная составляющая прикладной программы поддерживается уровнем приложений

Уровень приложений модели OSI включает собственно приложения и элементы сервиса приложений, облегчающие взаимодействие приложений с более низкими уровнями. Тремя наиболее важными элементами сервиса приложений являются элемент службы управления ассоциированием ACSE (association control service element), элемент службы удаленных операций ROSE (remote operation service element) и элемент службы надежной пересылки RTSE (reliable transfer service element). ACSE связывает имена приложений друг с другом в процессе подготовки обмена данными между приложениями. Элемент ROSE реализует общий механизм запросов-ответов, позволяющий выполнять операции удаленным образом подобно тому, как это делает механизм вызова удаленных процедур (RPC). Элемент RTSE помогает в надежной доставке, облегчая использование конструкций сеансового уровня.

К пяти общим приложениям OSI относятся следующие.

- *Протокол обмена общей управляющей информацией (Common Management Information Protocol, CMIP)* — обеспечивает возможности по управлению сетью. Подобно протоколам SNMP и NetView, позволяет осуществлять обмен управляющей информацией между оконечными системами и управляющими рабочими станциями (которые тоже являются оконечными системами).
- *Служба каталогов (Directory Service, DS)* — обязана своим происхождением спецификации X.500, разработанной Консультативным комитетом по международной телеграфной и телефонной связи (ССИТТ); теперь он называется Сектор стандартизации телекоммуникаций международного союза по электросвязи (ITU-T); эта служба обеспечивает реализацию функций распределенной базы данных, полезных для идентификации и адресации узлов на верхних уровнях.
- *Служба управления, доступа и пересылки файлов (File Transfer, Access, and Management, FTAM)* — предоставляет сервис по пересылке файлов. В дополнение к классической пересылке файлов, для которой она обеспечивает многочисленные опции, FTAM также предоставляет средства по распределенному доступу к файлам в духе ОС NetWare компании Novell, Inc. или файловой системы Network File System (NFS) компании Sun Microsystems, Inc.
- *Системы работы с сообщениями (message handling systems, MHS)* — обеспечивают базовый транспортный механизм для приложений по обработке электронных сообщений и других приложений, которым нужен сервис типа "запомнил и переслал". Хотя они служат подобным целям, MHS здесь — это не то же самое, что MHS в ОС NetWare компании Novell.
- *Протокол виртуального терминала (Virtual Terminal Protocol, VTP)* — обеспечивает эмуляцию терминала. Другими словами, он позволяет компьютерной системе выглядеть для удаленной оконечной системы так, словно первая является непосредственно подключенным терминалом. С помощью VTP можно, например, выполнять задания на мэйнфреймах.

Уровень представлений

Уровень 6 (представлений) эталонной модели OSI обычно представляет собой проходной протокол для информации из соседних уровней. Это позволяет осуществлять обмен между приложениями на разнородных компьютерных системах прозрачным для приложений образом.

Уровень представлений обеспечивает форматирование и преобразование кода. Форматирование кода используется для того, чтобы гарантировать приложению поступление информации для обработки, которая имела бы для него смысл. При необходимости этот уровень может выполнять перевод из одного формата данных в другой.

Уровень представлений имеет дело не только с форматами и представлением данных, он также занимается структурами данных, которые используются программами. Таким образом, уровень 6 обеспечивает организацию данных при их пересылке.

Чтобы понять, как это работает, представим, что имеются две системы. Одна использует для представления данных расширенный двоичный код обмена информацией EBCDIC, например, это может быть мэйнфрейм компании IBM, а другая — американский стандартный код обмена информацией ASCII (его используют большинство других производителей компьютеров). Если этим двум системам необходимо обменяться информацией, то нужен уровень представлений, который выполнит преобразование и осуществит перевод между двумя различными форматами.

Другой функцией, выполняемой на уровне представлений, является шифрование данных, которое применяется в тех случаях, когда необходимо защитить передаваемую информацию от приема несанкционированными получателями. Чтобы решить эту задачу, процессы и коды, находящиеся на уровне представлений, должны выполнить преобразование данных. На этом уровне существуют и другие подпрограммы, которые сжимают тексты и преобразовывают графические изображения в битовые потоки, так что они могут передаваться по сети.

Стандарты уровня представлений также определяют способы представления графических изображений. Как показано на рис. 9.2, для этих целей может использоваться формат PICT — формат изображений, применяемый для передачи графики QuickDraw между программами для компьютеров Macintosh и PowerPC. Другим форматом представлений является тэгированный формат файлов изображений TIFF, который обычно используется для растровых изображений с высоким разрешением. Следующим стандартом уровня представлений, который может использоваться для графических изображений, является стандарт, разработанный Объединенной экспертной группой по фотографии (Joint Photographic Expert Group); в повседневном пользовании этот стандарт называют просто JPEG.

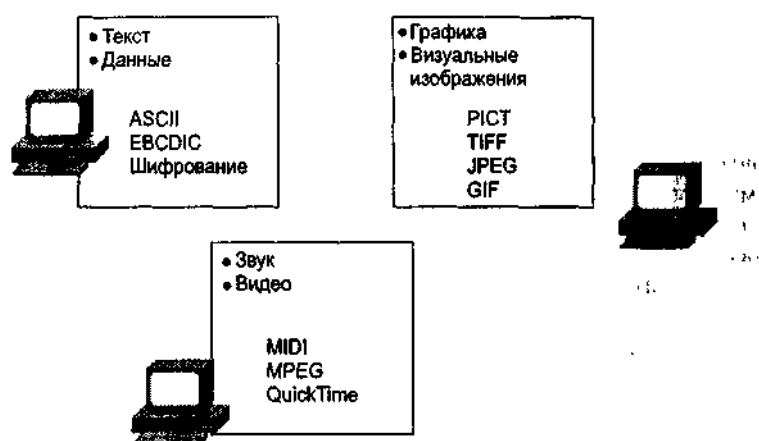


Рис. 9.2. Уровень представлений преобразует и форматирует текстовые, графические, видео- и аудиоэлементы

Существует другая группа стандартов уровня представлений, которая определяет представление звука и кинофрагментов. Сюда входят интерфейс электронных музыкальных инструментов MIDI (Musical Instrument Digital Interface) для цифрового представления музыки, разработанный. Экспертной группой по кинематографии стандарт MPEG, используемый для сжатия и кодирования видеороликов на компакт-дисках, хранения в оцифрованном виде и передачи со скоростями до 1,5 Мбит/с, и QuickTime — стандарт, описывающий звуковые и видеоэлементы для программ, выполняемых на компьютерах Macintosh и PowerPC.

Сеансовый уровень

Протокол сеансового уровня (уровня 5) модели OSI, реализуя различные механизмы управления, преобразовывает потоки данных, формируемые четырьмя нижними уровнями, в сеансы. Эти механизмы включают учет, управление разговорным процессом (т.е. определяется, кто и когда может говорить) и переговоры относительно параметров сеанса.

Сеансовый уровень устанавливает, управляет и завершает сеансы между приложениями. По сути, как показано на рис.9.3, сеансовый уровень координирует запросы на обслуживание и ответы, которые имеют место в процессе обмена данными между приложениями на различных хост-машинах. Управление разговором во время сеанса осуществляется с помощью маркера, наличие которого обеспечивает право на выполнение обмена. Маркер может запрашиваться, и окончательные системы могут наделяться приоритетами, которые обеспечивают неравноправное использование маркера.

Транспортный уровень

Транспортный уровень определяет сквозное взаимодействие приложений на хост-машинах. Транспортные службы предоставляют четыре основных сервиса:

- сегментируют приложения верхнего уровня;
- устанавливают сквозную работу;
- посылают сегменты от одной хост-машины, стоящей в одном конце цепочки взаимодействия, к другой хост-машине, стоящей в другом конце цепочки взаимодействия;
- они гарантируют надежность данных.

Как показано на рис. 9.4, транспортный уровень, или уровень 4, предполагает, что он, посылая пакеты данных от отправителя (источника) получателю (в пункт назначения), может использовать сеть в качестве некоего "облака". "Облако" отвечает за такие вопросы, как, например, "Какой из нескольких путей является лучшим для данного маршрута?" Здесь уже видно, какую роль в этом процессе играют маршрутизаторы.



Рис. 9.3. В процессе общения приложений, находящихся на различных хост-машинах, сеансовый уровень координирует запросы на обслуживание и ответы на них

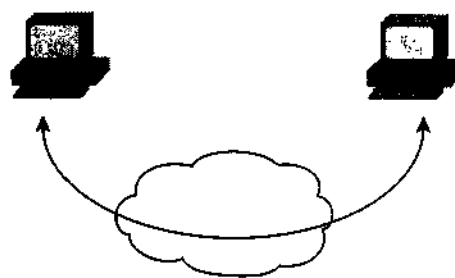


Рис. 9.4. При посылке пакетов данных сеть используется в качестве "облака"

Поток данных транспортного уровня обеспечивается транспортными сервисами на всем пути от хост-машины до пункта назначения. Иногда подобные сервисы называются *сквозными*. Поток данных транспортного уровня представляет собой логическое соединение между фиксированными точками сети.

Управление потоком

Когда транспортный уровень посылает свои сегменты данных, он также может гарантировать целостность данных. Одним из методов для этого является так называемое *управление потоком*, которое позволяет избежать проблемы, связанной с ситуацией, когда хост-машина на одном конце соединения переполняет буферы хост-машины на другом конце соединения. Переполнения могут быть серьезными проблемами, поскольку они могут приводить к потере данных.

Службы транспортного уровня также позволяют пользователям требовать надежный транспорт данных между хост-машинами и пунктами назначения. Для получения надежного транспорта данных между коммуницирующими конечными системами используются отношения с установлением соединения. Надежная транспортировка может:

- гарантировать, что отправитель будет получать подтверждение о доставке каждого сегмента;
- обеспечивать повторную отсылку любых сегментов, подтверждение о доставке которых не было получено;
- расставлять сегменты в пункте назначения в правильном порядке;
- не допускать перегрузку сети и обеспечивать управление в случае ее возникновения.

Установление соединения с одноранговой системой

В эталонной модели OSI несколько приложений может коллективно использовать одно транспортное соединение. Как показано на рис. 9.5, функции транспорта реализуются посегментно. Это означает, что различные приложения могут посылать данные по принципу "первый пришел, первый получил обслуживание". Такие сегменты могут предназначаться для одного получателя или для многих.

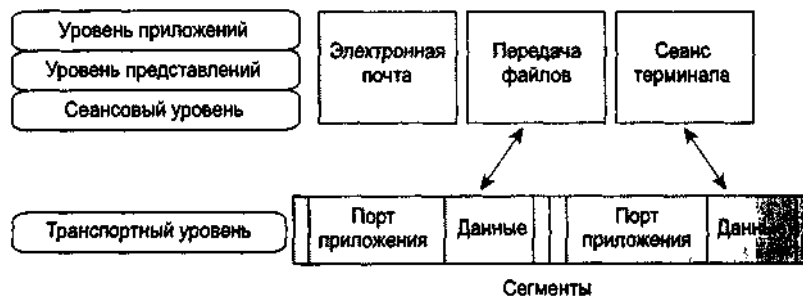


Рис. 9.5. Одно транспортное соединение может коллективно использоваться несколькими приложениями

Для того чтобы увидеть, как это работает, предположим, что по сети отправляется сообщение электронной почты с присоединенными к нему файлами. Одним из присоединенных файлов является файл, созданный текстовым редактором Microsoft Word, а второй файл — электронная таблица Excel.

При отсылке электронного почтового сообщения еще до начала передачи программное обеспечение устройства устанавливает номер порта для каждой использованной прикладной программы. Он включает дополнительные биты, с помощью которых кодируются тип сообщения, порождающая программа и используемый протокол. Когда каждое приложение, использованное в электронном почтовом сообщении, посылает сегмент потока данных, оно использует этот ранее заданный номер порта. Устройство в пункте назначения, принимая поток данных, разделяет и сортирует сегменты таким образом, что транспортный уровень может передавать данные правильному приложению на машине-получателе. В результате данные Excel-файла принимаются и читаются на устройстве в пункте назначения программой Excel, а Word-файл принимается и читается на устройстве в пункте назначения программой Word.

Пользователь транспортного уровня должен открыть сеанс с установлением соединения с одноранговой системой. Для того чтобы передача данных началась, как посылающее, так и принимающее приложение информируют свои операционные системы о том, что будет инициироваться соединение. Одна из машин посылает соответствующий вызов, который должен быть принят другой стороной. Протокольные программные модули двух операционных систем начинают общаться друг с другом, посылая по сети сообщения, чтобы проверить авторизацию передачи и подтвердить готовность обеих сторон.

После осуществления полной синхронизации говорят, что соединение установлено, и начинается передача данных. Во время передачи обе машины продолжают обмениваться информацией со своим протокольным программным обеспечением, удостоверяясь, что данные принимаются правильно.

На рис. 9.6 показано типичное соединение между посылающей и принимающей системами. Первая квитанция представляет собой запрос на синхронизацию, вторая и третья подтверждают начальный запрос на синхронизацию и синхронизируют параметры соединения в обратном направлении. Наконец, сегмент с последней квитанцией представляет собой подтверждение, используемое для того, чтобы информировать пункт назначения о согласии обеих сторон с тем, что соединение установлено. После того как соединение установлено, начинается передача данных.

В процессе передачи данных может возникнуть перегрузка, и причин для этого две. Первая состоит в том, что быстродействующий компьютер способен генерировать трафик быстрее, чем сеть может его передавать. Вторая возникает в ситуации, когда многим компьютерам одновременно необходимо послать данные в один пункт назначения. Тогда пункт назначения может испытывать перегрузку, хотя каждый источник в отдельности проблемы не вызывает.

В тех случаях, когда дейтаграммы поступают слишком быстро и хост-машина или шлюз не успевают их обрабатывать, они временно сохраняются в памяти. Если трафик продолжается,

то хост-машина или шлюз, исчерпав в конце концов свои ресурсы памяти, вынуждены отбрасывать дополнительные поступающие дейтаграммы.

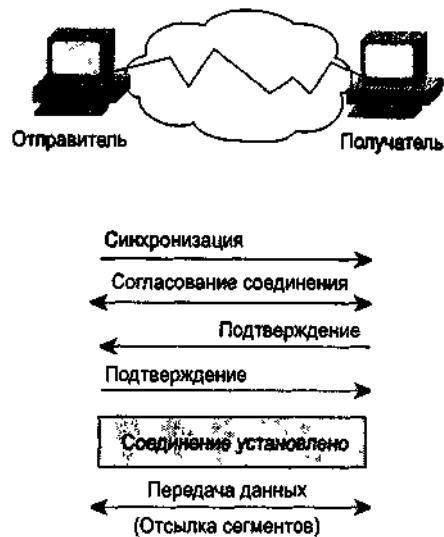


Рис.9.6. Типичное соединение между посылающей и принимающей системами

Чтобы не дать данным пропасть, транспортная функция может посылать отправителю индикатор "не готов". Действуя как красный сигнал светофора, этот индикатор сигнализирует отправителю о необходимости прекратить посылку данных. После того как получатель снова сможет обрабатывать дополнительные данные, он посылает транспортный индикатор "готов", который подобен зеленому сигналу светофора. Как показано на рис. 9.7, получая такой индикатор, отправитель может возобновить передачу сегментов.

Работа с окнами

В наиболее общей форме надежной пересылки данных с установлением соединения пакеты данных должны доставляться принимающей стороне в том же порядке, в котором они передавались. Протокол сигнализирует о сбое, если какие-либо пакеты данных теряются, повреждаются, дублируются или принимаются в другом порядке. Базовым решением является наличие подтверждения получателя о приеме каждого сегмента данных.

Однако если отправитель вынужден ждать подтверждения после посылки каждого сегмента, то пропускная способность становится низкой. Поскольку есть определенное время с того момента, как отправитель заканчивает отсылку пакета данных, до момента завершения обработки какого-либо принятого подтверждения, этот интервал используется для передачи дополнительных данных. Количество пакетов данных, которое разрешается иметь отправителю без получения подтверждения, известно под названием *окна*.

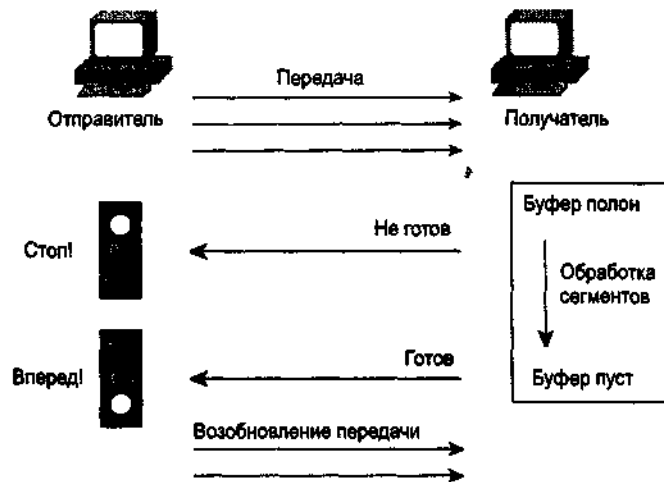


Рис. 9.7. Отправитель может возобновить передачу сегментов после получения от получателя транспортного индикатора "готов"

Работа с окнами — это метод управления количеством информации, пересылаемой между конечными точками соединения. Некоторые протоколы измеряют информацию в терминах количества пакетов, другие, например протокол TCP/IP, измеряют информацию в количестве байтов.

На рис. 9.8 отправителем и получателем являются рабочие станции. При размере окна 1 отправитель ждет подтверждения каждому переданному пакету данных. При размере окна 3 отправитель может послать три пакета данных прежде, чем начнет ожидать подтверждения.

Подтверждение

Надежный механизм доставки гарантирует, что поток данных, посланный от одной машины, будет доставлен по каналу передачи данных другой машине без дублирования или потери данных. Положительное подтверждение с повторной передачей является одной из методик, гарантирующих надежную доставку потоков данных. Положительное подтверждение требует, чтобы получатель общался с источником, посылая ему назад сообщение с подтверждением после приема данных. Отправитель регистрирует каждый отосланный им пакет и перед посылкой следующего пакета данных ждет подтверждения. В момент отсылки сегмента отправитель также запускает таймер и повторно передает сегмент, если установленное таймером время истекает до поступления подтверждения.

На рис. 9.9 показан отправитель, который передает пакеты 1, 2 и 3. Получатель подтверждает прием пакетов, запрашивая пакет 4. Отправитель, получив подтверждение, посылает пакеты 4, 5 и 6. Если пакет 5 не прибывает в пункт назначения, получатель посылает соответствующее подтверждение с запросом о повторной отсылке пакета 5. Отправитель повторно отсылает пакет 5 и должен получить соответствующее подтверждение, чтобы продолжить передачу пакета 7.

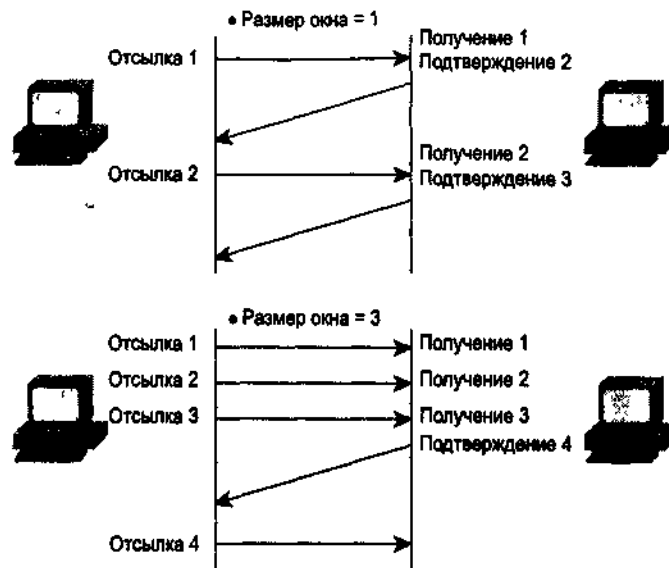


Рис. 9.8. Большой размер окна увеличивает эффективность связи

Резюме

- Каждый из верхних уровней выполняет свои функции и зависит от сервисов, предоставляемых уровнем ниже.
- Все четыре верхних уровня — транспортный (уровень 4), сеансовый (уровень 5), представлений (уровень 6) и приложений (уровень 7) — могут инкапсулировать данные в сегментах, передаваемых из одного конца соединения на другой.
 Уровень приложений поддерживает коммуникационную составляющую приложения.
 Уровень представлений форматирует и преобразовывает данные сетевого приложения, придавая соответствующее представление текстам, графике, изображениям, видео и звуку.
 Функции сеансового уровня координируют коммуникационное взаимодействие приложений.
 Транспортный уровень работает в предположении, что для отсылки пакетов данных от источника-отправителя в пункт назначения получателю он может использовать сеть в качестве "облака".
- Функции надежного транспортного уровня включают:
 управление потоком;
 установление соединения с одноранговой системой;
 работу с окнами;
 подтверждения.

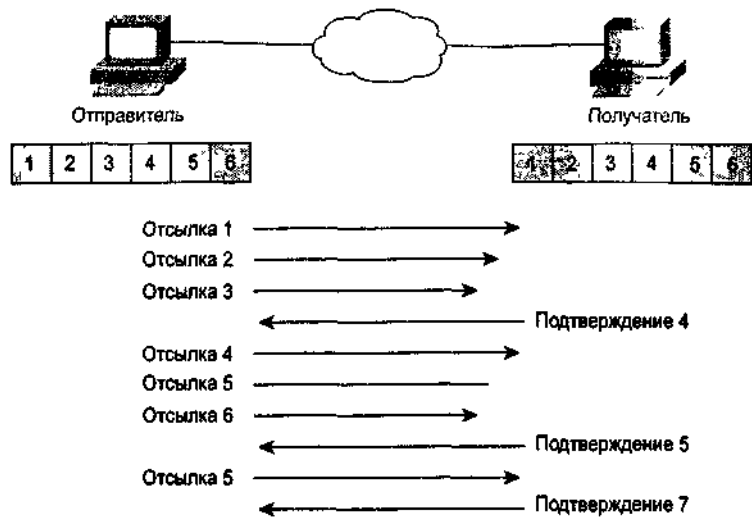


Рис. 9.9. Отправитель регистрирует каждый отосланный им пакет и перед посылкой следующего пакета данных ждет подтверждения

Контрольные вопросы

1. Какие уровни в эталонной модели OSI являются четырьмя верхними?
 - A. Приложений, представлений сеансовый и транспортный.
 - B. Приложений, сеансовый, сетевой и физический.
 - C. Физический, канальный, сетевой и транспортный.
 - D. Физический, сетевой, транспортный и приложений.
2. Какой уровень эталонной модели OSI поддерживает взаимодействие между такими программами, как электронная почта, передача файлов и Web-браузеры?
 - A. Уровень приложений.
 - B. Уровень представлений.
 - C. Сеансовый уровень.
 - D. Транспортный уровень.
3. Какое из определений наилучшим образом описывает понятие "управление потоком"?
 - A. Метод управления ограниченной полосой пропускания.
 - B. Метод синхронного соединения двух хост-машин.
 - C. Метод обеспечения целостности данных.
 - D. Метод проверки данных перед отсылкой на наличие вирусов.
4. Какой из уровней эталонной модели OSI осуществляет управление потоком и восстановление после ошибки?
 - A. Уровень приложений.
 - B. Уровень представлений.
 - C. Транспортный уровень.
 - D. Сетевой уровень.
5. Какое из приведенных ниже определений наилучшим образом описывает процесс сегментации?
 - A. Осуществляет разбивку данных на более мелкие пакеты для более быстрой передачи.
 - B. В моменты пикового трафика непрерывно осуществляет переключение хост-машин из режима отсылки в режим приема.
 - C. Позволяет нескольким приложениям коллективно использовать транспортное соединение.
 - D. Передает данные с уровня представлений на сетевой для кодирования и инкапсуляции.
6. Какой из приведенных ниже механизмов управляет объемом пересылаемой из конца в конец информации и помогает в обеспечении надежности протокола TCP?
 - A. Широковещание.
 - B. Работа с окнами.
 - C. Восстановление после ошибки.
 - D. Управление потоком.
7. Какой уровень эталонной модели OSI может выполнять трансляцию между различными форматами данных, например между форматами ASCII и EBCDIC?
 - A. Уровень приложений.
 - B. Уровень представлений.
 - C. Сеансовый уровень.
 - D. Транспортный уровень.
8. Что из приведенного ниже наилучшим образом описывает функцию уровня представлений?
 - A. Устанавливает приложения, управляет ими и завершает их.
 - B. Поддерживает взаимодействие таких программ, как электронная почта, передача файлов и Web-браузеры.
 - C. Обеспечивает транспортный сервис на всем пути от хост-машины до пункта назначения.
 - D. Выполняет трансляцию между различными форматами данных, например между форматами ASCII и EBCDIC.

9. ASCII, шифрование, QuickTime и JPEG: для какого из уровней все они типичны?
- A. Для уровня представлений.
 - B. Для транспортного уровня.
 - C. Для уровня приложений.
 - D. Для сеансового уровня.
10. Какой из уровней эталонной модели OSI устанавливает связь между приложениями, управляет ею и завершает ее?
- A. Уровень приложений.
 - B. Уровень представлений.
 - C. Сеансовый уровень.
 - D. Транспортный уровень.

Глава 10

Протокол TCP/IP

В этой главе...

- Функции уровня приложений протокола TCP/IP
- Функции транспортного уровня протокола TCP/IP
- Функции сетевого уровня протокола TCP/IP
- Протокол ICMP
- Протокол ARP
- Протокол RARP
- Почему протокол TCP является надежным
- Почему протокол UDP является ненадежным

Введение

В главе 9, "Уровни приложений, представлений, сеансовый и транспортный", рассказывалось о четырех верхних уровнях эталонной модели OSI. Кроме того, в ней описывались функции и процессы, используемые на транспортном уровне для обеспечения надежной доставки данных, а также для эффективного управления трафиком. В данной главе речь пойдет о протоколе управления передачей/межсетевом протоколе (Transmission Control Protocol/Internet Protocol, TCP/IP) и его работе по обеспечению обмена данными через произвольное количество взаимосвязанных сетей

Краткое описание протокола TCP/IP

Группа протоколов под общим названием TCP/IP была разработана в ходе исследовательской работы, выполненной Управлением перспективных исследований и разработок министерства обороны США (DARPA). Первоначально она разрабатывалась для обеспечения связи между компьютерами внутри самого управления. В настоящее время протокол TCP/IP де-факто является стандартом для межсетевого обмена данными и играет роль транспортного протокола в сети Internet, позволяя связываться миллионам компьютеров по всему миру.

В данной книге протоколу TCP/IP уделяется основное внимание по нескольким причинам.

- Протокол TCP/IP является универсально доступным, и с большой долей вероятности он будет использоваться в работе любой вновь организуемой сети.
- Протокол TCP/IP представляет собой полезный пример для понимания работы других протоколов, так как он включает элементы, которые типичны и для других протоколов
- Протокол TCP/IP важен, поскольку он используется маршрутизаторами в качестве средства конфигурирования.

Группа протоколов TCP/IP

Межсетевые протоколы могут использоваться для обеспечения взаимодействия в среде произвольного количества взаимосвязанных сетей. Они одинаково хорошо подходят для обмена информацией как в локальных, так и в глобальных вычислительных сетях. Группа протоколов Internet Protocol включает спецификации не только уровней 3 и 4 (например, IP и TCP), но также и спецификации таких общеупотребительных приложений, как электронная почта, удаленный вход в систему, эмуляция терминала и передача файлов.

Как видно из рис. 10.1, структура протокола TCP/IP подобна нижним уровням эталонной модели взаимодействия открытых систем (модели OSI). Протокол TCP/IP поддерживает все стандартные протоколы физического и канального уровней.

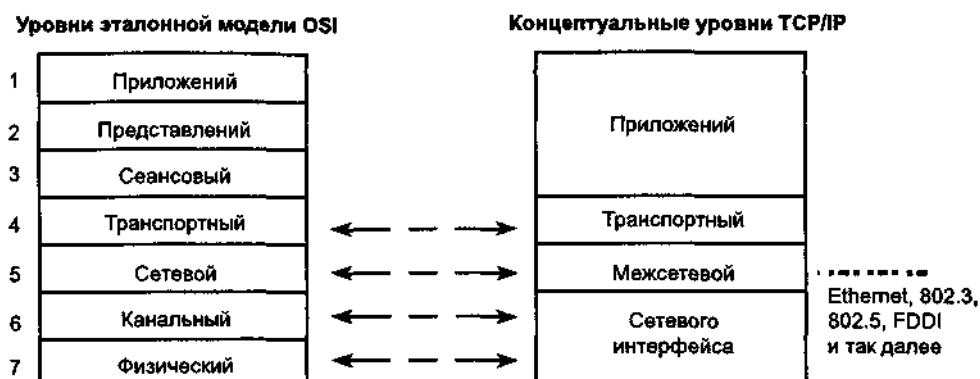


Рис. 10.1 С точки зрения заданных функциональностей четырехуровневая модель протокола TCP/IP подобна модели OSI

В протоколе TCP/IP информация передается в виде последовательности дейтаграмм. Одно сообщение может передаваться как ряд дейтаграмм, которые собираются в сообщение в месте приема.

TCP/IP и уровень приложений

Как показано на рис. 10.2, протоколы уровня приложений существуют для передачи файлов, электронной почты и удаленного входа в систему. На уровне приложений также поддерживается задача управления сетью.

TCP/IP и транспортный уровень

Транспортный уровень выполняет две функции:

- управляет потоком, что обеспечивается механизмом скользящих окон;
- гарантирует надежность благодаря наличию порядковых номеров сегментов и подтверждений.

Как показано на рис. 10.3, на транспортном уровне существуют два протокола.

- TCP — надежный протокол с установлением соединения. Он отвечает за разбиение сообщений на сегменты, их сборку на станции в пункте назначения, повторную отсылку всего, что оказалось не полученным, и сборку сообщений из сегментов. Протокол TCP обеспечивает виртуальный канал между приложениями конечных пользователей.

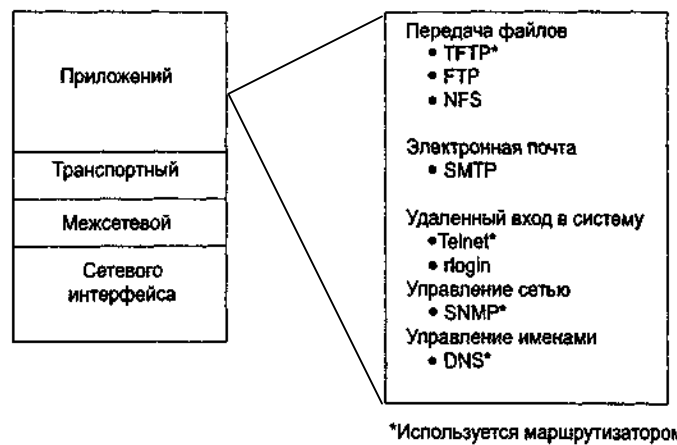


Рис. 10.2. Некоторые приложения, например тривиальный протокол передачи файлов (TFTP) и простой протокол управления сетью (SNMP), могут выполняться на маршрутизаторах

- Протокол дейтаграмм пользователя (User Datagram Protocol, UDP) — "ненадежный", не ориентированный на установление соединения. Хотя протокол UDP и отвечает за передачу сообщений, на этом уровне отсутствует программное обеспечение для проверки доставки сегментов; отсюда и определение "ненадежный".

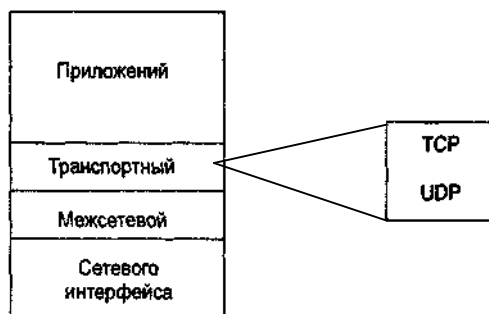


Рис 10.3. Разработчики приложений могут выбрать транспортный механизм с установленным соединением (TCP) или без такового (UDP)

Формат сегмента протокола TCP

На рис. 10.4 показаны поля TCP-сегмента, которые определяются следующим образом.

- *Порт источника* — номер вызывающего порта.
- *Порт назначения* — номер вызываемого порта.
- *Порядковый номер* — номер, используемый для расположения поступающих данных в правильной последовательности.
- *Номер подтверждения* — следующий ожидаемый TCP-октет.
- *HLLEN* — количество 32-разрядных слов в заголовке.
- *Зарезервированное* (поле) — все биты установлены в значение 0.
- *Биты кода* — служебные функции (например, установка и завершение сеанса).
- *Окно* — количество октетов, с которым отправитель готов согласиться.
- *Контрольная сумма* — расчетная контрольная сумма заголовка и полей данных.
- *Указатель срочных данных* — указывает конец срочных данных.
- *Опция* — в настоящее время определена одна: максимальный размер TCP-сегмента.
- *Данные* — данные протокола более высокого уровня.

Количество битов

16	16	32	32	4	6	6
Порт источника	Порт назначения	Порядковый номер	Номер подтверждения	HLLEN	Зарезервированное	Биты кода
16	16	16	0 или 32	Данные		
Окно	Контрольная сумма	Указатель срочных данных	Опция			

Рис. 10.4 Формат TCP-сегмента включает 12 полей

Номера портов

Для передачи информации на более высокие уровни как протокол TCP, так и протокол UDP используют номер порта, или так называемого сокета (рис. 10.5). Номера портов используются для отслеживания различных разговоров, одновременно ведущихся в сети.

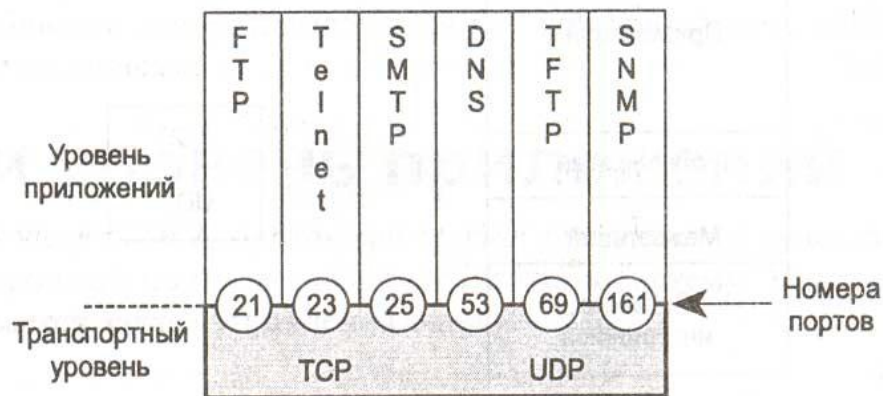


Рис. 10.5. Номера портов указывают протокол более высокого уровня, который в данный момент пользуется транспортом

Разработчики прикладного программного обеспечения договорились пользоваться широко известными номерами портов, определенными в документе RFC 1700. Например, любой обмен, связанный с пересылкой файлов по протоколу FTP, использует стандартный номер порта 21 (см. рис. 10.5).

Переговорам, не связанным с приложениями, имеющими общеизвестный номер порта, эти номера присваиваются произвольным образом, но при этом они выбираются из конкретного диапазона значений. Как показано в табл. 10.1, эти номера портов используются в TCP-сегменте в качестве адресов источника и пункта назначения.

Таблица 10.1 Зарезервированные номера портов в протоколах NCP и UDP

Десятичный номер	Ключевое слово	Описание
0	—	Зарезервирован
1-4	—	Не назначен
5	pe	Удаленный ввод заданий
7	echo	Эхо
9	discard	Отбросить
11	users	Активные пользователи
13	daytime	Днем
15	netstat	Кто активен, или сетевая статистика
17	quote	Кавычки дня
19	chargen	Генератор символов
20	ftp-data	Протокол FTP (данные)
21	ftp	Протокол FTP
23	telnet	Терминальное соединение
25	smtp	Простой протокол передачи почтовых сообщений (SMTP)
37	time	Время суток
39	rip	Протокол указания местонахождения ресурсов (RLP)
42	nameserver	Сервер имен хост-машин
43	nickname	Кто?
53	domain	Сервер имен домена (DNS)
67	bootps	Сервер задачи начальной загрузки
68	bootpc	Клиент задачи начальной загрузки
69	tftp	Протокол TFTP
75	—	Любая частная служба подключения к внешним сервисам по телефонной линии
77	—	Любая частная служба удаленного ввода задания

79	finger	Служба определения активных клиентов в сети
123	ntp	Протокол сетевого времени (NTP)
133-159	—	Не назначены
160-223	—	Зарезервированы
224-241	—	Не назначены
242-255	—	Не назначены

В протоколах TCP и UDP некоторые номера портов зарезервированы, но приложения могут быть написаны так, что не поддерживают их. Номера портов имеют следующие выделенные диапазоны значений.

- Номера меньше 255 предназначаются для приложений общего пользования.
- Номера от 255 до 1023 отданы компаниям для продаваемых приложений.
- Использование номеров более 1023 не регламентируется.

Конечная система использует номер порта для выбора соответствующего приложения. Как показано на рис. 10.6, номер порта источника происхождения — обычно это какой-нибудь номер больше 1023 — присваивается динамически хост-машиной отправителя.

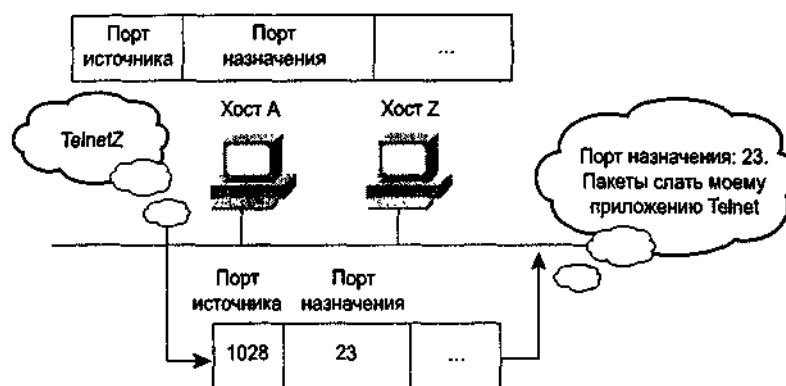


Рис. 10.6. Порт отправителя и порт пункта назначения не обязательно должны совпадать

Открытое TCP-соединение с трехсторонним квитированием

Для установления или инициализации соединения как бы два протокола TCP используют не сам TCP, а процессы или конечные станции, и должны синхронизировать начальные порядковые номера (ISN) сегментов друг друга для данного соединения. Порядковые номера используются для того, чтобы отслеживать последовательность обмена и гарантировать отсутствие потерянных фрагментов данных, которые требуют для пересылки нескольких пакетов. Начальный порядковый номер представляет собой стартовый номер, используемый при установлении TCP-соединения. Обмен начальными порядковыми номерами в процессе выполнения последовательности установления соединения гарантирует возможность восстановления потерянных данных, если в будущем возникнут проблемы.

Синхронизация выполняется путем обмена сегментами, несущими номера ISN и управляющий бит, называемый SYN (от английского *synchronize* — синхронизировать). (Сегменты, содержащие бит SYN, тоже называются SYN.) Для успешного соединения требуется наличие подходящего механизма выбора начального порядкового номера и слегка запуганный процесс квитирования, который обеспечивает обмен значениями ISN.

Процесс синхронизации требует, чтобы каждая сторона послала свой номер ISN и получила подтверждение и ISN от другой стороны соединения. Каждая сторона должна принимать ISN от другой стороны и посылать положительное подтверждение (ACK) в определенном порядке, который

описан в следующей последовательности шагов.

1. $A > B$ SYN — мой порядковый номер X .
2. $A < B$ ACK — твой порядковый номер X .
3. $A < B$ SYN — мой порядковый номер Y .
4. $A > B$ ACK — твой порядковый номер Y .

Так как второй и третий шаги могут объединяться в одном сообщении, то такой обмен называется *открытым с трехсторонним квитированием* (three-way handshake/open). Как показано на рис. 10.7, обе стороны соединения синхронизируются, выполняя последовательность открытого соединения с трехсторонним квитированием.

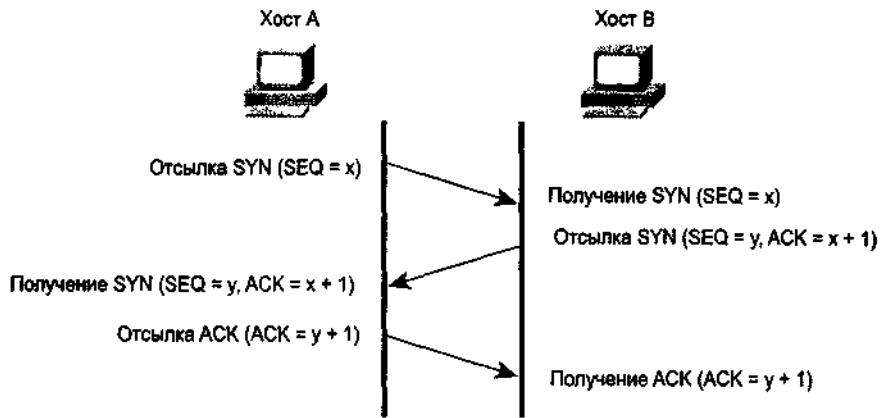


Рис. 10.7. Обмен данными невозможен до тех пор, пока не будет успешно завершено трехстороннее квитирование

Эта последовательность похожа на разговор двух людей. Первый хочет поговорить со вторым и говорит: "Я бы хотел с вами поговорить" (SYN). Второй отвечает: "Хорошо, я хочу с вами говорить" (SYN, ACK). Тогда первый говорит: "Прекрасно, давайте поговорим" (ACK).

Трехстороннее квитирование необходимо, поскольку порядковые номера не привязываются к глобальным часам сети и протоколы TCP могут использовать различные механизмы для выбора номера ISN. У приемника первого сегмента SYN нет способа узнать, не был ли этот сегмент старым задержавшимся, если он не помнит последний порядковый номер, использованный в соединении, что не всегда возможно, и поэтому он должен попросить отправителя верифицировать этот сегмент SYN.

В этот момент времени любая из сторон либо может начать обмен данными, либо разорвать связь, поскольку протокол TCP является методом одноранговой (равноправной) связи.

Простое подтверждение и работа с окнами в протоколе TCP

Размером окна называют количество сегментов, которое может быть передано в процессе ожидания подтверждения. После того как хост-машина передаст определяемое размером окна количество сегментов, она должна будет получить подтверждение и только потом сможет послать какие-либо другие сообщения.

Размер окна определяет объем данных, который может принять принимающая станция за один раз. Если размер окна равен 1, подтверждаться должен каждый сегмент, и только после этого передается следующий. Это приводит к неэффективному использованию хост-машиной полосы пропускания.

Целью введения механизма окон является улучшение управления потоком и надежности. К сожалению, и это видно из рис. 10.8, при размере окна, равном 1, наблюдается неэффективное использование полосы пропускания.

Скольльзящие окна в протоколе TCP

Для регулирования потока данных между устройствами в протоколе TCP используется механизм управления потоком. Принимающий протокол TCP сообщает посылающему протоколу TCP размер окна. Этот размер задает количество байтов, начиная с номера подтверждения, которое принимающий TCP готов принять на текущий момент (рис. 10.9).

В протоколе TCP используются ожидаемые подтверждения, означающие, что номер подтверждения соответствует октету, ожидаемому следующим. Слово "скользящее" в термине *скользящее окно* отражает тот факт, что размер окна согласуется динамически во время TCP-сеанса. Использование скользящего окна приводит к более эффективному использованию хост-машиной полосы пропускания, поскольку больший размер окна позволяет передавать больший объем данных, откладывая момент получения подтверждения.

Порядковые номера и номера подтверждений в протоколе TCP

Протокол TCP обеспечивает организацию последовательности сегментов, которую предваряет подтверждение с номером, определяющим точку отсчета. Перед передачей каждая дейтаграмма нумеруется. На принимающей станции протокол TCP собирает сегменты в полное сообщение. Если какой-либо порядковый номер в последовательности теряется, то сегмент с этим номером передается повторно. Кроме того, если через заданный период времени сегмент не получает свое подтверждение, то он тоже передается повторно.

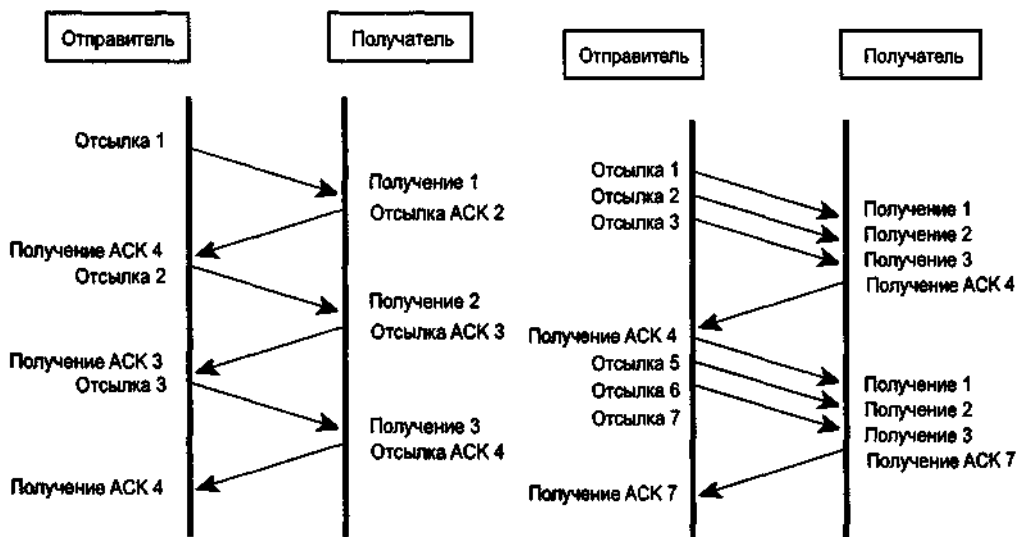


Рис. 10.8. Если размер окна равен 1, отправитель перед отправкой следующих данных должен ждать соответствующее подтверждение

Рис. 10.9. Большой размер окна увеличивает эффективность потока

Порядковые номера и номера подтверждений являются направленными. Это означает, что связь осуществляется в обоих направлениях. На рис. 10.10 показан обмен, происходящий в одном направлении. Номер в последовательности и номер подтверждения определяются отправителем, показанным слева. Кроме того, протокол TCP предоставляет возможность полной дуплексной связи. Как следствие, подтверждения гарантируют надежность.

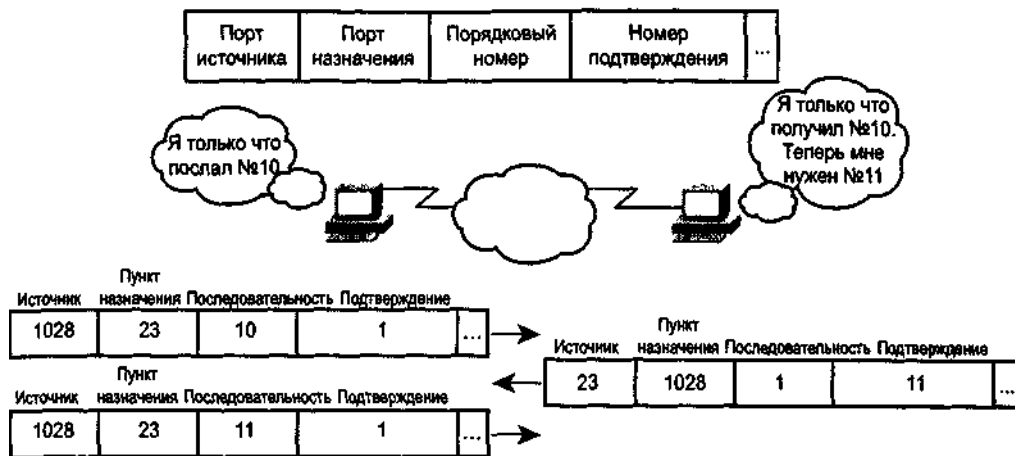


Рис. 10.10. Получатель запрашивает следующую дейтаграмму в последовательности

Формат сегмента в протоколе UDP

Протокол UDP не использует окна или подтверждения. Надежность могут обеспечить протоколы уровня приложений. Протокол UDP был спроектирован для приложений, которые не нуждаются в сборке последовательностей сегментов.

К протоколам, которые используют UDP, относятся TFTP, SNMP, сетевая файловая система (NFS) и система имен домена (DNS). Как видно из рис. 10.11, размер заголовка в протоколе UDP относительно небольшой.

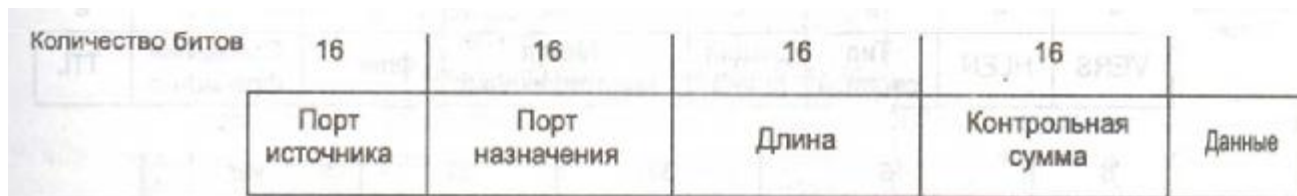


Рис. 10.11. Протокол UDP не предусматривает наличия полей порядкового номера и номера подтверждения

TCP/IP и межсетевой уровень

Межсетевой уровень в иерархической структуре протокола TCP/IP соответствует сетевому уровню модели OSI. Каждый из этих уровней несет ответственность за прохождение пакетов по взаимосвязанным сетям, используя при этом программную адресацию.

Как показано на рис. 10.12, на межсетевом уровне протокола TCP/IP (который соответствует сетевому уровню модели OSI) функционирует несколько протоколов.

- Протокол IP, который обеспечивает маршрутизацию дейтаграмм с минимальными затратами на доставку и без установления соединения. Его не интересует содержание дейтаграмм, вместо этого он занимается поиском способа перемещения дейтаграмм в пункт назначения.
- Межсетевой протокол управляющих сообщений (Internet Control Message Protocol, ICMP), который обеспечивает возможности по управлению и передаче сообщений.
- Протокол преобразования адреса (Address Resolution Protocol, ARP), определяющий канальный адрес по известному IP-адресу.
- Протокол обратного преобразования адреса (Reverse Address Resolution Protocol, RARP), определяющий сетевые адреса по известным канальным адресам.

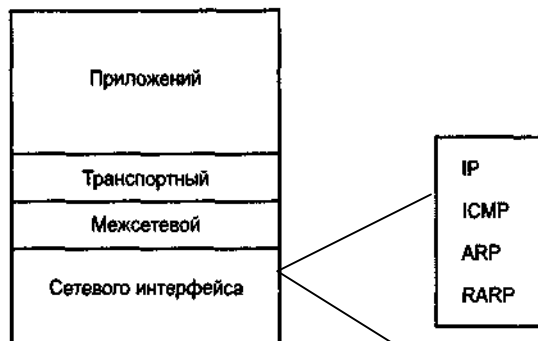


Рис. 10.12. Сетевой уровень модели OSI соответствует межсетевому уровню протокола TCP/IP

IP-дейтаграмма

На рис. 10.13 изображен формат IP-дейтаграммы, которая содержит IP-заголовок и данные, окруженные с одной стороны заголовком уровня управления доступом к среде (MAC), а с другой — концевым завершителем MAC-уровня.

Количество битов

4	4	8	16	16	3	13	8
VERS	HLEN	Тип сервиса	Общая длина	Метка идентификации	Флаги	Смещение фрагмента	TTL
8	16	32	32	var			
Протокол	Контрольная сумма заголовка	IP-адрес отправителя	IP-адрес получателя	IP опции	Данные		

Рис. 10.13 Из-за поля IP-опций заголовок протокола IP имеет переменную длину

Определения полей внутри этой IP-дейтаграммы выглядят следующим образом.

- *VERS* — номер версии.
- *HLEN* — длина заголовка в 32-разрядных словах.
- *Тип сервиса* — как дейтаграмма должна обрабатываться.
- *Общая длина* — общая длина (заголовок плюс данные).
- *Метка идентификации, флаги и смещение фрагмента* — обеспечивают фрагментацию дейтаграмм с целью обеспечения возможности подстройки под различные размеры максимального блока передачи (MTU) в сети Internet.
- *TTL* — поле времени жизни (Time To Live) пакета с обратным отсчетом. Каждая станция должна уменьшать значение этого поля на единицу или на то количество секунд, которое было ею потрачено на пакет. При достижении счетчиком нулевого значения время жизни пакета истекает, и он уничтожается. Этот параметр времени жизни не дает пакетам бесконечно путешествовать по сети Internet в поисках несуществующих пунктов назначения.
- *Протокол* — протокол более высокого уровня (уровня 4), который посылает дейтаграмму. Поле протокола определяет протокол уровня 4, который переносится внутри IP-дейтаграммы. Хотя большинство IP-трафика пользуется протоколом TCP, протокол IP могут использовать и другие протоколы. Каждый IP-заголовок должен идентифицировать для дейтаграммы протокол уровня

4 в пункте назначения. Как показано на рис. 10.14, протоколы транспортного уровня представляются заданными номерами, подобно тому, как это используется в случае номеров портов. Номер протокола и указывается в поле IP-дейтаграммы *Протокол*.

- *Контрольная сумма заголовка* — контроль целостности заголовка.
- *IP-адрес отправителя и IP-адрес получателя* — 32-разрядные IP-адреса, идентифицирующие конечные устройства, участвующие в обмене.
- *IP опции* — защита, тестирование и отладка в сети и другие функции.

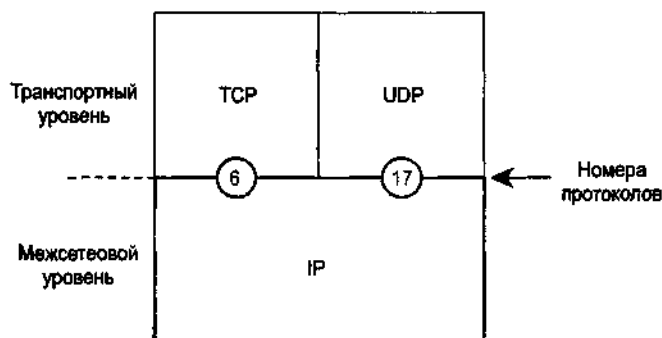


Рис. 10.14. Поле типа протокола в заголовке IP-дейтаграммы используется для идентификации протокола следующего по возрастанию уровня

Протокол ICMP

Протокол ICMP работает на всех хост-машинах, использующих протокол TCP/IP. Сообщения этого протокола переносятся внутри IP-дейтаграмм и используются для отправки управляющих сообщений и сообщений об ошибках.

В протоколе ICMP используются следующие фиксированные типы сообщений (некоторые из которых приведены на рис. 10.15).

- Пункт назначения недостижим.
- Время истекло.
- Проблемы с параметром.
- Гашение отправителя.
- Перенаправление.
- Эхо-запрос.
- Эхо-ответ.
- Запрос временной метки.
- Ответ на запрос временной метки.
- Информационный запрос.
- Информационный ответ.
- Запрос адреса.
- Ответ на запрос адреса.

Существуют и другие типы сообщений, которые не включены в данный перечень.

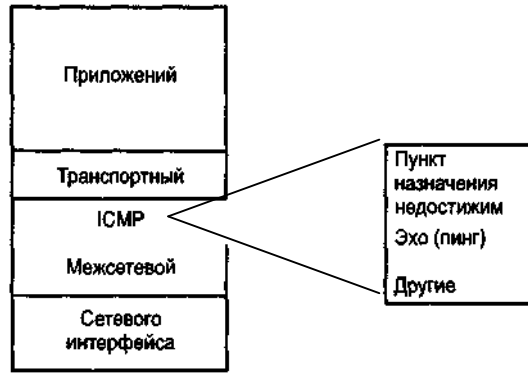


Рис. 10.15. Протокол ICMP обеспечивает механизмы для осуществления управления и обработки ошибок

Проверка пункта назначения с помощью протокола ICMP

Если маршрутизатор получает пакет, который не может быть доставлен в конечный пункт назначения, то он посылает отправителю ICMP-сообщение "Пункт назначения недоступим". Но сначала он пошлет маршрутизатору-получателю эхо-запрос. Как показано на рис. 10.16 и 10.17, сообщение может быть не доставлено из-за того, что маршрут к пункту назначения неизвестен, а эхо-ответ представляет собой успешный ответ на выдачу команды ping. Однако результатом выполнения этой команды могут быть и другие сообщения, например сообщение о недоступности или сообщение об окончании времени ожидания.

Протокол ARP

Протокол ARP используется для преобразования или отображения известного IP-адреса на подуровневый MAC-адрес, чтобы обеспечить взаимодействие в среде передачи данных с множественным доступом, например Ethernet. Чтобы определить адрес пункта назначения дейтаграммы, сначала проверяется ARP-таблица, находящаяся в кэш-памяти. Если адрес в таблице отсутствует, то тогда протокол ARP, пытаясь найти станцию-получатель, генерирует широковещательный запрос. Широковещательный запрос принимает каждая станция, находящаяся в сети.

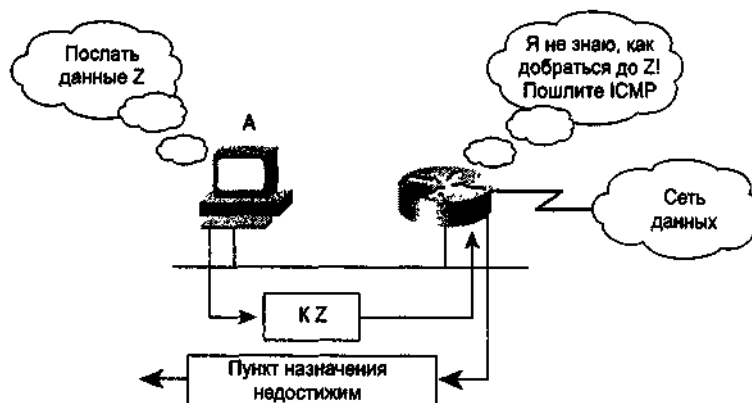


Рис. 10.16. Протокол ICMP сообщает, что требуемый пункт назначения недоступим

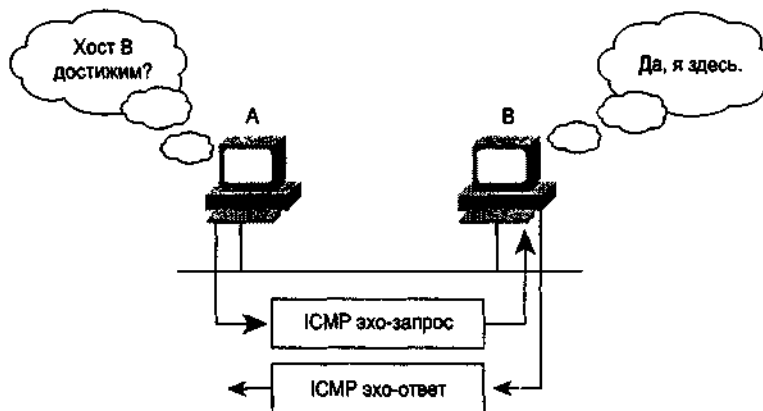


Рис. 10.17. Эхо-запрос генерируется командой `ping`

Термин *локальное преобразование адреса* используется для описания процедуры преобразования адреса, когда запрашивающая хост-машина и хост-машина в пункте назначения вместе используют одну и ту же среду передачи данных или провод. Как показано на рис. 10.18, перед выдачей ARP-запроса выполняется сверка с подсетевой маской. В случае, показанном на рис. 10.18, маска свидетельствует о том, что узлы находятся в одной подсети.

Протокол RARP

Работа протокола RARP основана на наличии RARP-сервера с заполненной таблицей или других средств, отвечающих на RARP-запросы (рис. 10.19). В локальном сегменте протокол RARP может использоваться для инициации последовательности удаленной загрузки операционной системы.

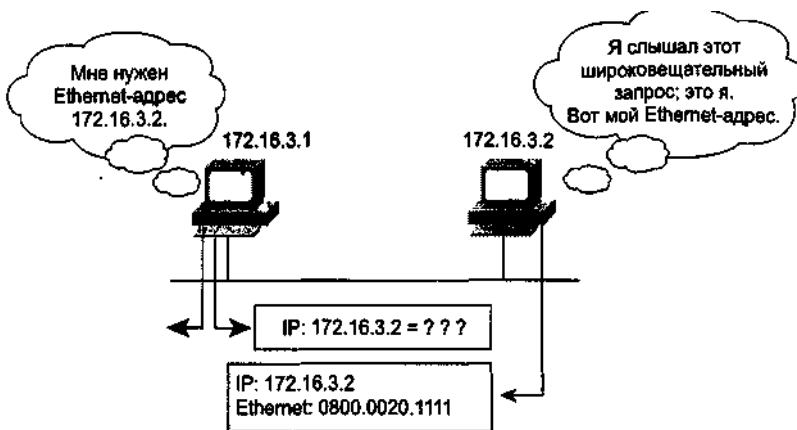


Рис. 10.18. Протокол ARP используется для получения MAC-адреса

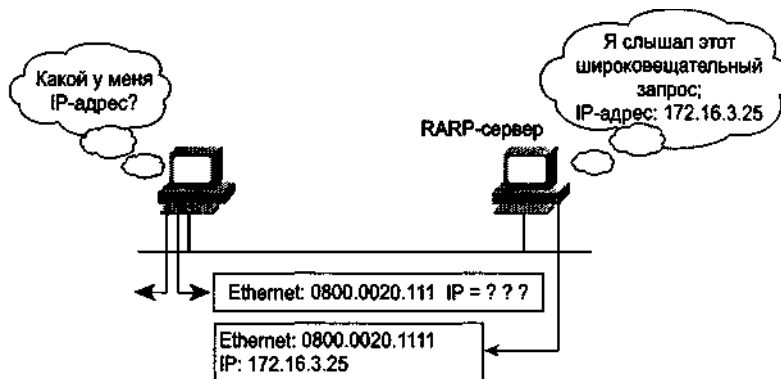


Рис. 10.19. Протокол RARP используется для получения IP-адреса с помощью RARP-запроса

Резюме

- Структура группы протоколов TCP/IP соответствует нижним уровням эталонной модели OSI и имеет следующие компоненты.
 - Протоколы, поддерживающие передачу файлов, электронную почту, удаленный вход в систему и другие приложения.
 - Надежный и ненадежный транспорт.
 - Доставка дейтаграмм без установления соединения на сетевом уровне.
- Протоколы уровня приложений существуют для передачи файлов, электронной почты и удаленного доступа к системе. На уровне приложений также поддерживается управление сетью.
- Транспортный уровень выполняет две функции.
 - Управление потоком, которое обеспечивается за счет использования механизма скользящих окон.
 - Обеспечение надежности, которая достигается благодаря наличию порядковых номеров и подтверждений.
- Межсетевой уровень протокола TCP/IP соответствует сетевому уровню модели OSI.
- Протокол ICMP обеспечивает реализацию функций управления и передачи сообщений на сетевом уровне. Этот протокол работает на всех хост-машинах, использующих протокол TCP/IP.
- Протокол ARP используется для преобразования или отображения известного IP-адреса на подуровневый MAC-адрес. Это необходимо, чтобы обеспечить взаимодействие в среде передачи данных с множественным доступом, например Ethernet.
- Работа протокола RARP основана на наличии RARP-сервера с заполненной таблицей или других средств, отвечающих на RARP-запросы.

Контрольные вопросы

1. Какое из приведенных ниже определений наилучшим образом описывает протокол TCP/IP?
 - A. Группа протоколов, которая может использоваться для организации взаимодействия произвольного количества взаимосвязанных сетей.
 - B. Группа протоколов, которая позволяет подключать локальные сети к глобальным.
 - C. Группа протоколов, которая позволяет передавать данные через большое количество сетей.
 - D. Группа протоколов, которая позволяет взаимосвязанным сетям коллективно использовать различные устройства.
2. Какое из приведенных ниже определений лучше всего описывает цель этажерочных структур протоколов группы TCP/IP?
 - A. Точно соответствуют верхним уровням модели OSI.
 - B. Поддерживают все стандартные протоколы физического и канального уровней.
 - C. Передают информацию в виде последовательности дейтаграмм.
 - D. В месте приема выполняют сборку дейтаграмм в полные сообщения.
3. Какой из следующих протоколов относится к транспортному уровню?
 - A. UDP.
 - B. UDP.
 - C. TCP.
 - D. TCP.
4. Для чего нужны номера портов?
 - A. Они отслеживают различные переговоры, одновременно ведущиеся в сети.
 - B. Системы-отправители используют их для сохранения организации сеанса и для выбора нужного приложения.
 - C. Конечные системы используют их для динамического приписывания конечных пользователей к конкретному сеансу в зависимости от используемого ими приложения.
 - D. Системы-отправители генерируют их для прогнозирования адресов пунктов назначения.
5. Зачем в протоколе TCP используются открытые соединения с трехсторонним квитированием?
 - A. Для восстановления данных, если потом возникнут проблемы.
 - B. Для определения объема информации, который принимающая станция может принять за один раз.
 - C. Для эффективного использования пользователями полосы пропускания.
 - D. Для преобразования двоичных ответов на команду ring в информацию для более высоких уровней модели OSI.
6. Какова роль скользящего окна в протоколе TCP?
 - A. Оно делает окно большим, поэтому за один раз может проходить больший объем данных, что приводит к более эффективному использованию полосы пропускания.
 - B. При приеме данных размер окна регулируется для каждого раздела дейтаграммы, что приводит к более эффективному использованию полосы пропускания.
 - C. Оно позволяет во время TCP-сеанса динамически согласовывать размер окна, что приводит к более эффективному использованию полосы пропускания.
 - D. Оно ограничивает объем поступающих данных, так что каждый сегмент должен посылаться по одному, что приводит к неэффективному использованию полосы пропускания.
7. Какие протоколы использует протокол UDP для обеспечения надежности?
 - A. Протоколы сетевого уровня.
 - B. Протоколы уровня приложений.
 - C. Межсетевые протоколы.
 - D. Протоколы управления передачей.
8. Зачем нужна проверка, выполняемая протоколом ICMP?

- A. Чтобы выяснить, достигают ли сообщения пункта назначения, и если нет — для определения возможных причин этого.
 - B. Для проверки полноты мониторинга всех действий в сети.
 - C. Для определения соответствия настройки сети модели.
 - D. Чтобы определить, находится сеть в режиме управления или в пользовательском режиме.
9. Если предположить, что MAC-адреса нет в ARP-таблице, то как отправитель находит MAC-адрес пункта назначения?
- A. Сверяется с таблицей маршрутизации.
 - B. В поисках адреса посылает сообщение по всем адресам.
 - C. Посылает широковещательное сообщение по всей локальной сети.
 - D. Посылает широковещательное сообщение по всей сети.
10. Какое из приведенных ниже определений лучше всего описывает смысл параметра "размер окна"?
- A. Максимальный размер окна, с которым может работать программное обеспечение, сохраняя достаточно высокую скорость обработки.
 - B. Количество сообщений, которое может передаваться в процессе ожидания подтверждения.
 - C. Размер окна в пиках (1 пика равна 1/12 пункта, или 1/6 дюйма. — *Прим персе*), который должен быть установлен заранее, чтобы данные могли быть отосланы.
 - D. Размер окна, открытого на экране монитора, которое не всегда совпадает с размером экрана.

Глава 11

Сетевой уровень и маршрутизация

В этой главе

- Идентификация составных частей сетевого адреса
- Маршрутизация с использованием метода вектора расстояния
- Маршрутизация с учетом состояния канала связи
- Гибридная маршрутизация
- Сравнение процессов, используемых маршрутизаторами для актуализации таблиц маршрутизации, и проблем и их решений при обновлении информации в маршрутизаторах после изменений в топологии сети.

Введение

В главе 10, "Протокол TCP/IP", рассказывалось о протоколе управления передачей/межсетевом протоколе (TCP/IP) и его работе при обеспечении обмена информацией во взаимосвязанных сетях.

В данной главе будут описываться применение маршрутизаторов и их работа при выполнении ключевых функций сетевого уровня (уровня 3) эталонной модели взаимодействия открытых систем (модели OSI). Кроме того, здесь будет объяснена разница между протоколами маршрутизации и маршрутизируемыми протоколами, а также показан способ, которым пользуются маршрутизаторы для прослеживания расстояния между узлами. Наконец, будут описаны подходы на основе вектора расстояния, учета состояния канала связи и гибридный, и как каждый из них решает общие проблемы маршрутизации.

Маршрутизаторы Cisco

Маршрутизаторы представляют собой устройства, которые реализуют сетевой сервис. Они обеспечивают интерфейсы для широкого диапазона каналов связи и подсетей и с самым широким диапазоном скоростей. Поскольку маршрутизаторы являются активными и интеллектуальными узлами сети, то они могут принимать участие в управлении сетью. Управление сетями достигается за счет обеспечения динамического контроля ресурсов и поддержки целей и задач сети, которые включают возможность установления связи, надежность в работе, управленческий контроль и гибкость.

В дополнение к базовым функциям коммутирования и маршрутизации маршрутизаторы также обеспечивают реализацию и других самоценных характеристик, которые помогают улучшить стоимостную эффективность сети. К таким характеристикам относятся выстраивание последовательности прохождения трафика на основе приоритетов и его фильтрация.

Обычно маршрутизаторы требуются для поддержки множества протокольных групп, каждая из которых имеет свой собственный протокол маршрутизации, и для обеспечения параллельной работы таких различных сред. На практике маршрутизаторы также имеют функции, которые позволяют создавать мостовые соединения, и, кроме того, могут играть роль усеченной формы концентратора. В данной главе будет рассказано об операциях и методиках конфигурирования маршрутизаторов Cisco на работу с протоколами и многими средами передачи данных (рис. 11.1).

Понимает разные
протоколы

Соединяет разные
среды передачи данных

TCP/IP AppleTalk
IPX/SPX
DECnet PPP
Banyan VINES
IPX/SPX
X 25 Frame Relay
ISDN

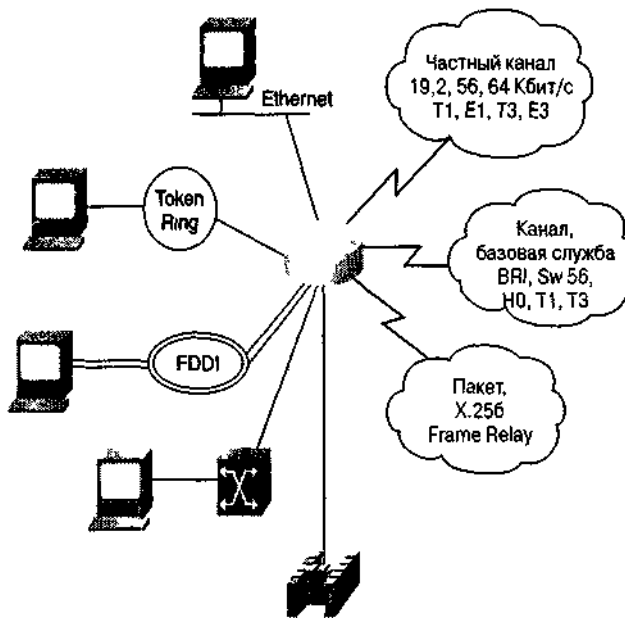


Рис 111. Для соединения множества различных сред используются маршрутизаторы Cisco, сконфигурированные на одновременную работу с несколькими протоколами

Основные характеристики сетевого уровня

Сетевой уровень для сетей играет роль интерфейсов и обеспечивает своему пользователю, транспортному уровню, сервис по наилучшей сквозной доставке пакетов. Сетевой уровень пересылает пакеты из сети источника в сеть пункта назначения.

В данном разделе объясняется общая работа сетевого уровня, включая то, как он определяет выбранный путь до пункта назначения и сообщает о нем, как работают и чем отличаются схемы адресации протоколов и как функционируют протоколы маршрутизации.

Определение пути сетевым уровнем

Каким путем должен пойти трафик через сети Этот выбор пути происходит на сетевом уровне. Функция выбора пути позволяет маршрутизатору оценивать имеющиеся пути до пункта назначения и устанавливать наилучший в этом плане метод обработки пакетов.

Оценивая возможные пути, протоколы маршрутизации используют информацию о топологии сетей. Эта информация может конфигурироваться сетевым администратором или собираться посредством динамических процессов, исполняемых в сети.

Сетевой уровень для сетей играет роль интерфейсов и обеспечивает своему пользователю, транспортному уровню, сервис по наилучшей сквозной доставке пакетов. Сетевой уровень пересылает пакеты из сети-источника в сеть пункта назначения на основе таблицы IP-маршрутизации.

После того как маршрутизатор определит, какой путь использовать, он может переходить к коммутированию пакета: принимая пакет, полученный через один интерфейс, и перенаправляя его на другой интерфейс или порт, который соответствует наилучшему пути к пункту назначения пакета.

Путь коммуникации

Чтобы иметь практическую ценность, сеть должна непротиворечивым образом показывать пути, имеющиеся между маршрутизаторами. Как показано на рис. 112, каждая связь между

маршрутизаторами имеет номер, который маршрутизаторы используют в качестве адреса. Эти адреса должны нести в себе информацию, которая может быть использована в процессе маршрутизации. Это означает, что адрес должен содержать информацию о пути соединений сред передачи данных, которую процесс маршрутизации будет использовать для пересылки пакетов от отправителя в конечный пункт назначения.

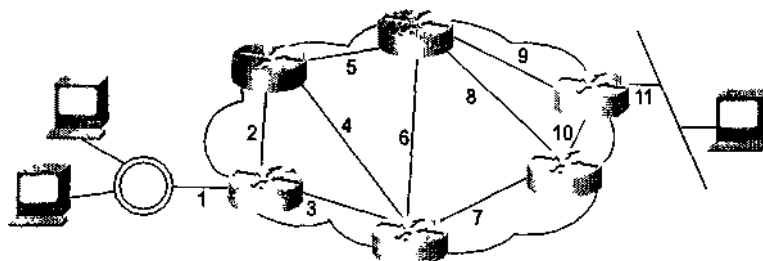


Рис. 11.2 Адреса отражают путь соединений сред передачи данных

Используя эти адреса, сетевой уровень может обеспечить организацию релейного соединения, которое будет связывать независимые сети. Непротиворечивость адресов уровня 3 во всем многосетевом комплексе также улучшает использование полосы пропускания, исключая необходимость в ширококвещательных рассылках. Широковещательные рассылки приводят к накладным расходам в виде ненужных процессов и напрасно расходуют мощности устройств или каналов связи, которым вовсе не надо принимать эти ширококвещательные рассылки.

Благодаря использованию непротиворечивой сквозной адресации для представления пути соединений сред передачи данных сетевой уровень может находить путь до пункта назначения без ненужной загрузки устройств или каналов связи многосетевого комплекса ширококвещательными рассылками.

Адресация: сеть и хост-машина

Сетевой адрес состоит из сетевой части и части хост-машины, которые используются маршрутизатором в "облаке" сети. Обе они нужны для доставки пакетов от отправителя получателю.

Сетевой адрес используется маршрутизатором для идентификации сети отправителя или получателя пакета внутри сетевого комплекса. На рис. 11.3 показаны три номера сетей: 1,1 2.1 и 3.1, исходящих из маршрутизатора.

Для некоторых протоколов сетевого уровня эти отношения задаются администратором сети, который назначает сетевые адреса в соответствии с планом адресации сетевого комплекса. Для других же протоколов сетевого уровня назначение адресов является частично или полностью динамическим.

Большинство схем адресации в сетевых протоколах использует некоторую форму адреса хост-машины или узла. На рис. 11.3 показаны три хост-машины, использующие номер сети 1.

Маршрутизация с использованием сетевых адресов

В общем случае маршрутизаторы передают пакет по эстафете из одного канала связи : другой. Чтобы осуществить такую эстафетную передачу, маршрутизаторы используют , основные функции: функцию определения пути и функцию коммутации.

На рис. 11.4 показано, как маршрутизаторы используют адресацию для реализации своих функций маршрутизации и коммутации. Сетевая часть адреса используется для осуществления выбора пути, а узловая часть адреса говорит о порте маршрутизатора" по пути следования.

Маршрутизатор отвечает за передачу пакета в следующую сеть по пути следования. Сетевая часть адреса используется маршрутизатором для выбора пути.

Функция коммутирования позволяет маршрутизатору принимать пакет на один

интерфейс и переправлять его на другой. Функция определения пути позволяет маршрутизатору выбрать наиболее подходящий интерфейс для переадресации пакета. Узловая часть адреса говорит о конкретном порте маршрутизатора, который имеет выход на соседний маршрутизатор в выбранном направлении.

Сеть назначения	Направление и порт маршрутизатора
1.0	← 1.1
2.0	→ 2.1
3.0	→ 3.1

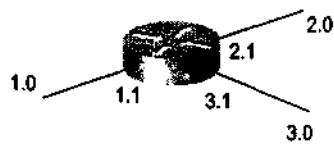


Рис. 11.4. Сетевая часть адреса используется для выбора пути

Сеть	Хост-машина
1	1 2 3
2	1
3	1

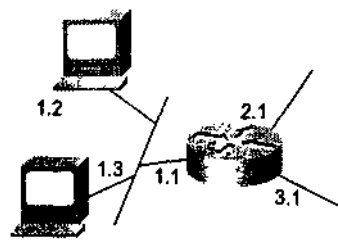


Рис. 11.3. Сетевой адрес состоит из сетевой части и части хост-машины

Протоколы маршрутизации и маршрутизируемые протоколы

Очень часто путают похожие термины *протокол маршрутизации (routing protocol)* и *маршрутизируемый протокол (routed protocol)* (рис. 11.5). Некоторые разъяснения по этому поводу приведены ниже.

- *Маршрутизируемый протокол* — любой сетевой протокол, который обеспечивает в адресе сетевого уровня достаточно информации, чтобы позволить передать пакет от одной хост-машины к другой на основе принятой схемы адресации. Маршрутизируемый протокол определяет формат и назначение полей внутри пакета. В общем случае пакеты переносятся от одной конечной системы к другой. Примером маршрутизируемого протокола является межсетевой протокол IP.
- *Протокол маршрутизации* — поддерживает маршрутизируемый протокол за счет предоставления механизмов коллективного использования маршрутной информации. Сообщения протокола маршрутизации циркулируют между маршрутизаторами. Протокол маршрутизации позволяет маршрутизаторам обмениваться информацией с другими маршрутизаторами с целью актуализации и ведения таблиц. Примерами протоколов маршрутизации являются протокол маршрутной информации (RIP), протокол внутренней маршрутизации между шлюзами (IGRP), усовершенствованный протокол внутренней маршрутизации между шлюзами (EIGRP) и протокол маршрутизации с выбором кратчайшего пути (OSPF).

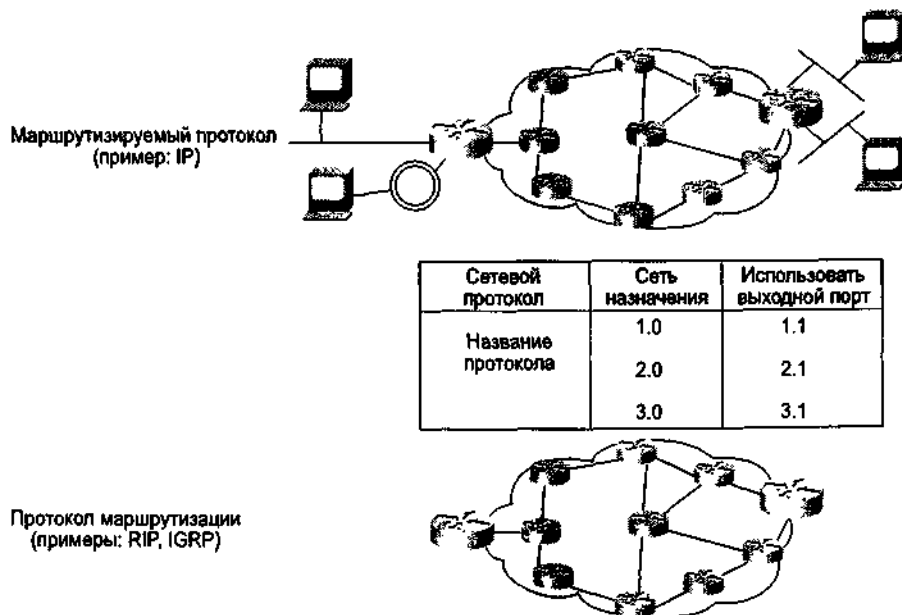


Рис. 11.5. Маршрутизируемый протокол используется для направления трафика, а протокол маршрутизации используется между маршрутизаторами для ведения таблиц

Операции, выполняемые протоколом сетевого уровня

Когда приложению, исполняемому на хост-машине, необходимо послать пакет в пункт назначения, находящийся в другой сети, на один из интерфейсов маршрутизатора принимается кадр канального уровня. Сетевой уровень проверяет заголовок и определяет сеть пункта назначения, а затем сверяется с таблицей маршрутизации, которая связывает сети с работающими на выход интерфейсами (рис. 11.6).

Пакет снова инкапсулируется в кадр канального уровня для выбранного интерфейса и ставится в очередь для доставки на следующий переход по пути следования.

Такой процесс повторяется каждый раз, когда пакет коммутируется следующим маршрутизатором. На маршрутизаторе, соединенном с сетью, в которой находится хост-машина получателя, пакет инкапсулируется в кадр канального уровня ЛВС пункта назначения и доставляется хост-машине получателя.

Многопротокольная маршрутизация

Маршрутизаторы способны поддерживать несколько независимых протоколов маршрутизации и вести таблицы маршрутизации для нескольких маршрутизируемых протоколов одновременно. Эта их способность позволяет маршрутизатору доставлять пакеты нескольких маршрутизируемых протоколов по одним и тем же каналам передачи данных (рис. 11.7).

Статические и динамические маршруты

Статическая информация администрируется вручную. Сетевой администратор вводит ее в конфигурацию маршрутизатора. Если изменение в топологии сети требует актуализации статической информации, то администратор сети должен вручную обновить соответствующую запись о статическом маршруте.

Динамическая информация работает по-другому. После ввода администратором сети команд, запускающих функцию динамической маршрутизации, сведения о маршрутах обновляются процессом маршрутизации автоматически сразу после поступления из сети новой информации. Изменения в динамически получаемой информации распространяются между

маршрутизаторами как часть процесса актуализации данных.

Пример статического маршрута

Статическая маршрутизация имеет несколько полезных применений, которые связаны с привлечением специальных знаний администратора сети о сетевой топологии. Одним из таких применений является защита в сети. Динамическая маршрутизация раскрывает все, что известно о сети. Однако по причинам безопасности может понадобиться скрыть некоторые части сети. Статическая маршрутизация позволяет администратору сетевого комплекса задавать те сведения, которые могут сообщаться о закрытых частях сети.

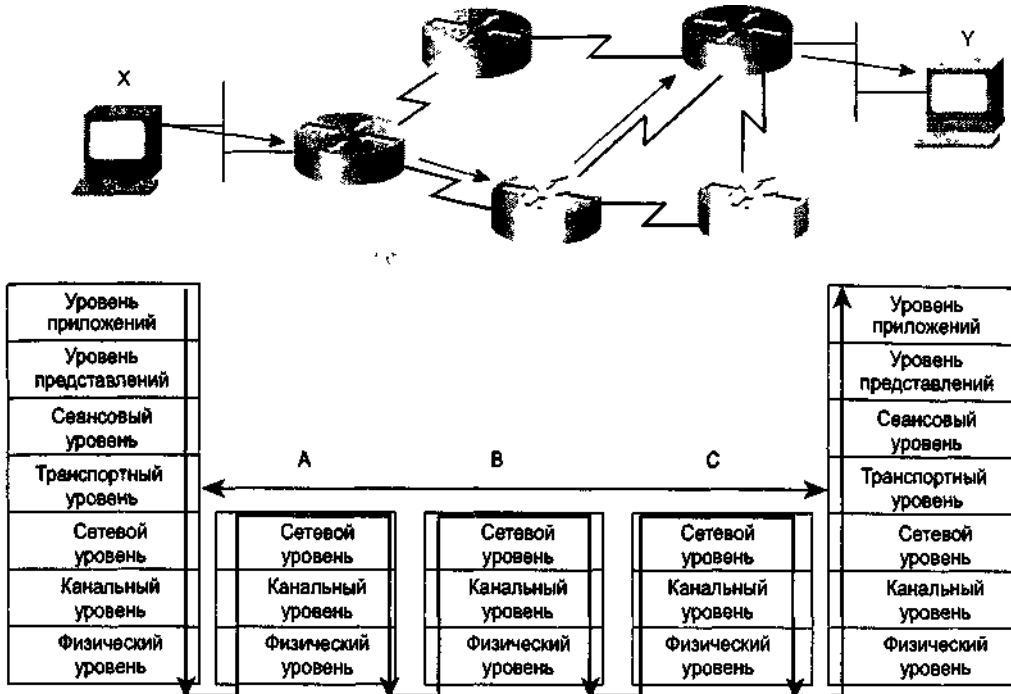


Рис. 11.6 Каждый маршрутизатор обеспечивает сервис для поддержки функций более высокого уровня модели OSI

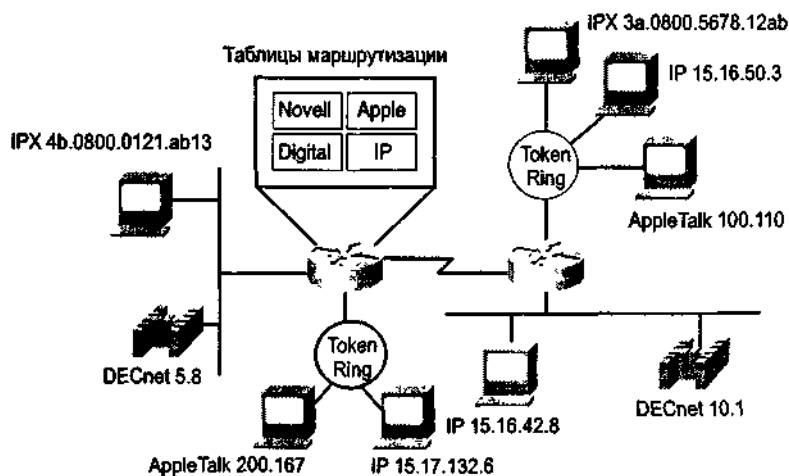


Рис. 11.7. Маршрутизаторы пропускают трафик всех маршрутизируемых протоколов, существующих в сети

Статический маршрут к сети также достаточен в том случае, если сеть доступна только по одному пути. Такой тип участка сетевого комплекса называется *тупиковой сетью*. Конфигурирование статического маршрута к тупиковой сети исключает накладные расходы,

связанные с динамической маршрутизацией (рис. 11.8).

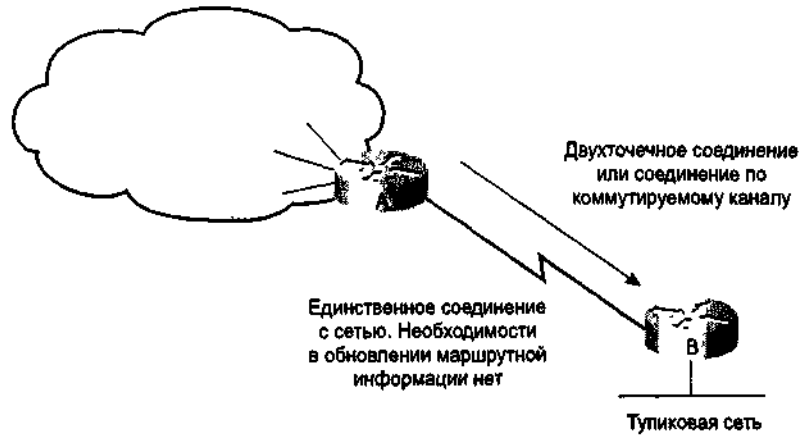


Рис. 11.8 Записи о статических маршрутах могут исключить необходимость в обновлении маршрутной информации по каналу глобальной сети

Пример маршрута по умолчанию

На рис. 11.9 показано применение *маршрута по умолчанию*— записи в таблице маршрутизации, которая используется для направления кадров, которые не имеют в таблице маршрутизации явно указанного следующего перехода. Маршруты по умолчанию могут устанавливаться как результат статического конфигурирования, выполняемого администратором.

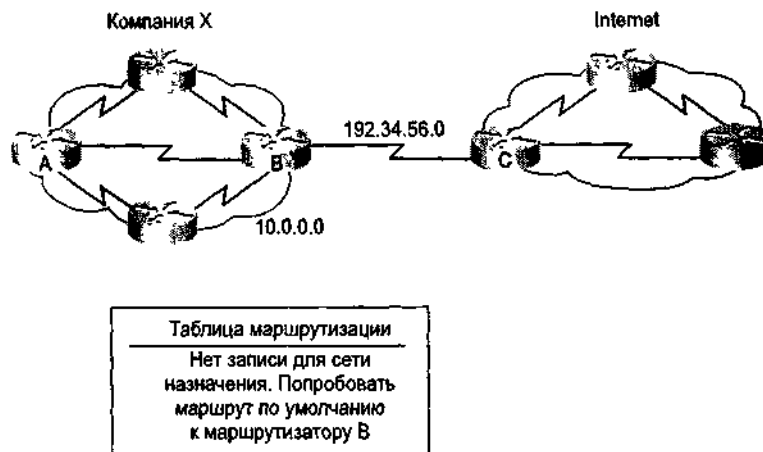


Рис. 11.9 Маршрут по умолчанию используется в тех случаях, когда следующий переход отсутствует в таблице маршрутизации в явном виде

В этом примере маршрутизаторы компании X знают только о топологии сети этой компании, но ничего не знают о других сетях. Вообще говоря, содержание сведений обо всех других сетевых комплексах, доступных через сеть Internet, излишне и неразумно, если не невозможно.

Вместо сведений о каждой конкретной сети каждому маршрутизатору компании X сообщается маршрут по умолчанию, с помощью которого он может добраться до любого неизвестного пункта назначения, направляя пакет в сеть Internet.

Адаптация к изменениям топологии

Показанная на рис. 11.10 сеть по-разному адаптируется к изменениям в топологии, в зависимости от того, используется статическая или динамическая информация.

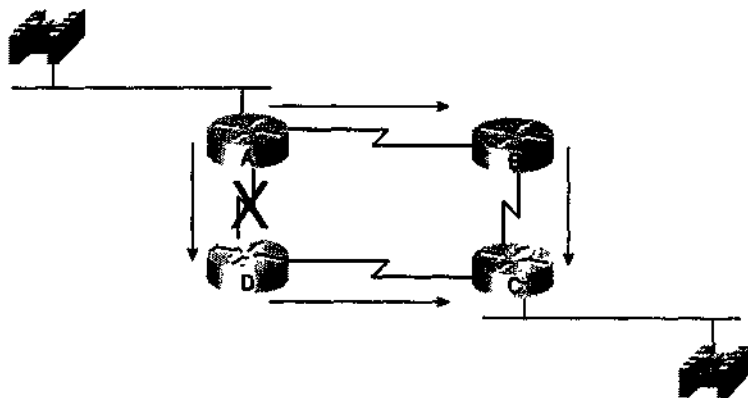


Рис. 11.10. Динамическая маршрутизация позволяет маршрутизаторам при необходимости автоматически использовать резервные маршруты

Статическая маршрутизация позволяет маршрутизаторам правильно направлять пакет от сети к сети. Маршрутизатор просматривает свою таблицу маршрутизации и, следуя содержащимся там статическим данным, ретранслирует пакет маршрутизатору D. Маршрутизатор D делает то же самое и ретранслирует пакет маршрутизатору C. Маршрутизатор C доставляет пакет хост-машине получателя.

Но что произойдет, если путь между маршрутизаторами A и D становится непроходимым? Ясно, что маршрутизатор A не сможет ретранслировать пакет маршрутизатору D по статическому маршруту. Связь с сетью пункта назначения будет невозможна до тех пор, пока маршрутизатор A не будет реконфигурирован на ретрансляцию пакетов маршрутизатору B.

Динамическая маршрутизация обеспечивает более гибкое и автоматическое поведение. В соответствии с таблицей маршрутизации, генерируемой маршрутизатором A, пакет может достичь своего пункта назначения по предпочтительному маршруту через маршрутизатор D. Однако к пункту назначения возможен и другой путь через маршрутизатор B. Когда маршрутизатор A узнает, что канал на маршрутизатор D нарушен, он перестраивает свою таблицу маршрутизации, делая предпочтительным путь к пункту назначения через маршрутизатор B, а маршрутизаторы продолжают слать пакеты по этому каналу связи.

Когда путь между маршрутизаторами A и D восстанавливается, маршрутизатор A может снова изменить свою таблицу маршрутизации и указать предпочтительным путь к сети пункта назначения против часовой стрелки через маршрутизаторы D и C.

Протоколы динамической маршрутизации могут также перенаправлять трафик между различными путями в сети.

Операции динамической маршрутизации

Успех динамической маршрутизации зависит от двух основных функций маршрутизатора.

- Ведение таблицы маршрутизации.
- Своевременное распространение информации — в виде пакетов актуализации — среди других маршрутизаторов (рис. 11.11).

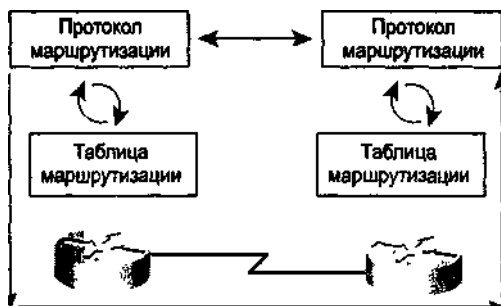


Рис. 11.11. Протоколы маршрутизации собирают и распространяют маршрутную информацию

В обеспечении коллективного пользования информацией о маршрутах динамическая маршрутизация полагается на протокол маршрутизации. Протокол маршрутизации определяет набор правил, используемых маршрутизатором при его общении с соседними маршрутизаторами. Например, протокол маршрутизации описывает следующее:

- как посылаются пакеты актуализации;
- какие сведения содержатся в таких пакетах актуализации;
- когда следует посылать эту информацию;
- как определять получателей этих пакетов актуализации.

Представление расстояния с помощью метрики

Когда алгоритм маршрутизации обновляет таблицу маршрутизации, его главной целью является определение наилучшей информации для включения в таблицу. Каждый алгоритм маршрутизации интерпретирует понятие *наилучшая* по-своему. Для каждого пути в сети алгоритм генерирует число, называемое *метрикой*. Как правило, чем меньше величина этого числа, тем лучше путь (рис 11.12).

Метрики могут рассчитываться на основе одной характеристики пути. Объединяя несколько характеристик, можно рассчитывать и более сложные метрики. Как показано на рис. 11.13, при вычислении значения метрики используется несколько характеристик пути.

Наиболее общеупотребительными метриками, используемыми маршрутизаторами, являются следующие.

- *Количество переходов* — количество маршрутизаторов, которые должен пройти пакет, чтобы дойти до получателя. Чем меньше количество переходов, тем лучше путь. Для обозначения суммы переходов до пункта назначения используется термин *длина пути*.

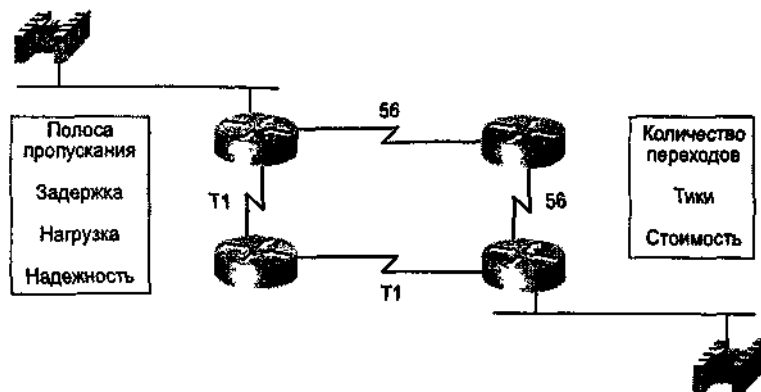


Рис. 11.12. Для нахождения наилучшего пути могут использоваться различные метрики

- *Полоса пропускания* — пропускная способность канала передачи данных. Например, для арендуемой линии 64 Кбит/с обычно предпочтительным является канал типа T1 с полосой пропускания 1,544 Мбит/с.
- *Задержка* — продолжительность времени, требующегося для перемещения пакета от отправителя получателю.
- *Нагрузка* — объем действий, выполняемый сетевым ресурсом, например маршрутизатором или каналом.
- *Надежность* — темп возникновения ошибок в каждом сетевом канале.
- *Тики* — задержка в канале передачи данных, определяемая в машинных тактах IBM-подобного ПК (приблизительно 55 миллисекунд).
- *Стоимость* — произвольное значение, обычно основанное на величине полосы пропускания, денежной стоимости или результате других измерений, которое назначается сетевым

администратором.

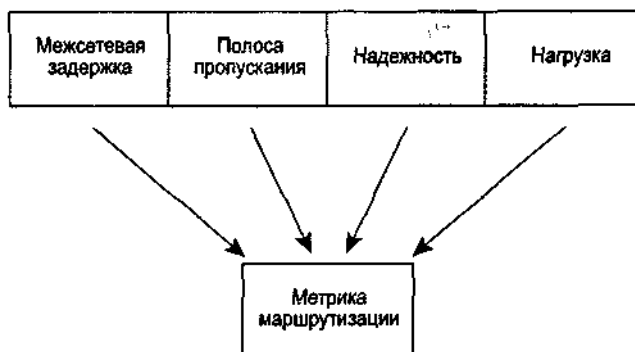


Рис. 11.13. Для вычисления метрик используется несколько характеристик пути

Протоколы маршрутизации

Большинство алгоритмов маршрутизации можно свести к трем основным алгоритмам.

- Подход на основе маршрутизации по вектору расстояния, в соответствии с которым определяются направление (вектор) и расстояние до каждого канала в сети.
- Подход на основе оценки состояния канала (также называемый выбором наикратчайшего пути), при котором воссоздается точная топология всей сети (или по крайней мере той части, где размещается маршрутизатор).
- Гибридный подход, объединяющий аспекты алгоритмов с определением вектора расстояния и оценки состояния канала.

В последующих разделах рассматриваются процедуры этих алгоритмов маршрутизации и проблемы, связанные с каждым из них, а также описаны методики минимизации этих проблем.

Алгоритм маршрутизации является основой динамической маршрутизации. Как только вследствие роста, реконфигурирования или отказа изменяется топология сети, база знаний о сети должна изменяться тоже; это прерывает маршрутизацию.

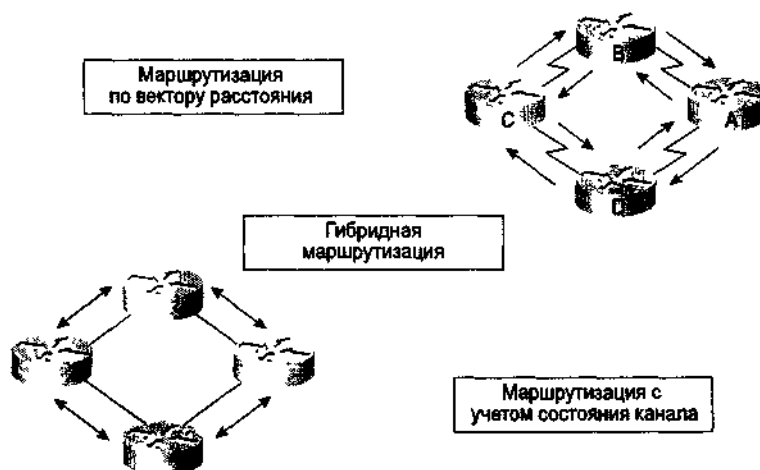


Рис. 11.14 Маршрутизация по вектору расстояния, с учетом состояния канала связи и гибридная — три основных типа алгоритмов маршрутизации

Необходимо, чтобы знания отражали точное и непротиворечивое представление о новой топологии. В том случае, когда все маршрутизаторы используют непротиворечивое представление

топологии сети, имеет место *сходимость*. Говорят, что сетевой комплекс *сошелся*, когда все имеющиеся в нем маршрутизаторы работают с одной и той же информацией. Процесс и время, требующиеся для возобновления сходимости маршрутизаторов, меняются в зависимости от протокола маршрутизации. Для сети желательно обладать свойством быстрой сходимости, поскольку это уменьшает время, когда маршрутизаторы используют для принятия решений о выборе маршрута устаревшие знания, и эти решения могут быть неправильными, расточительными по времени или и теми и другими одновременно.

Алгоритмы маршрутизации по вектору расстояния

Алгоритмы маршрутизации на основе вектора расстояния (также известные под названием *алгоритмы Беллмана—Форда* (Bellman-Ford algorithms)) предусматривают периодическую передачу копий таблицы маршрутизации от одного маршрутизатора другому. Регулярно посылаемые между маршрутизаторами пакеты актуализации сообщают обо всех изменениях топологии.

Каждый маршрутизатор получает таблицу маршрутизации от своего соседа. Например, на рис. 11.15 маршрутизатор В получает информацию от маршрутизатора А. Маршрутизатор В добавляет величину, отражающую вектор расстояния (скажем, количество переходов), которая увеличивает вектор расстояния, и затем передает таблицу маршрутизации своему соседу — маршрутизатору С. Такой же процесс пошагово выполняется между соседними маршрутизаторами во всех направлениях.

Подобным образом алгоритм аккумулирует сетевые расстояния и поэтому способен поддерживать базу данных информации о топологии сети. Однако алгоритмы на основе вектора расстояния не позволяют маршрутизатору знать точную топологию всего сетевого комплекса.

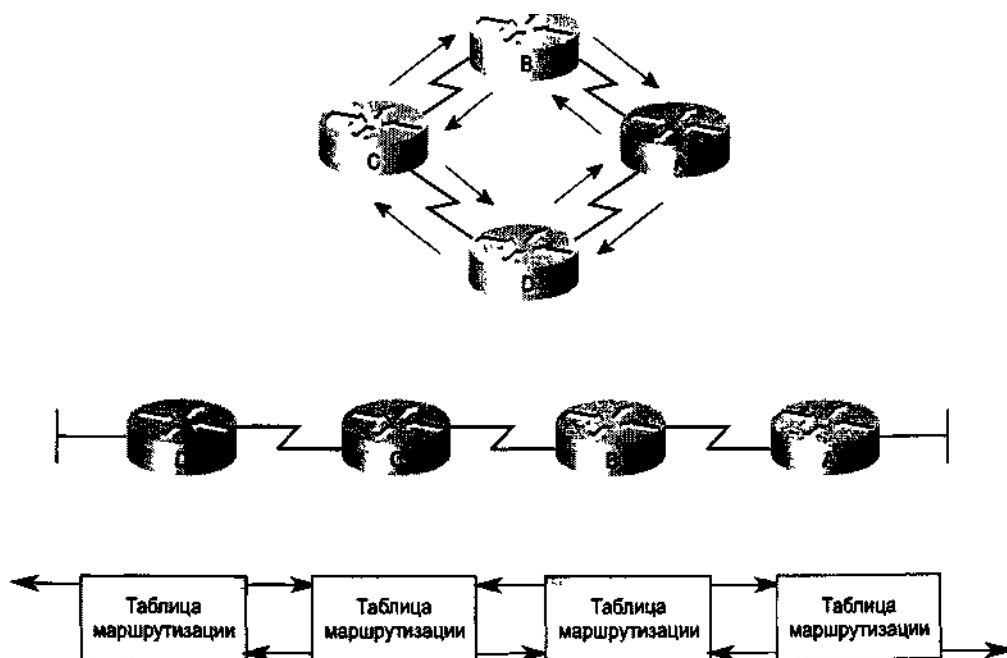


Рис. 11.15 Маршрутизаторы, использующие метод вектора расстояния, периодически посылают соседям свою таблицу маршрутизации и аккумулируют значения векторов расстояния

Алгоритм маршрутизации по вектору расстояния и исследование сети

Каждый маршрутизатор, использующий алгоритм маршрутизации по вектору расстояния, начинает с идентификации или *исследования* своих соседей. Как показано на рис. 11.16, порт к

каждой непосредственно подключенной сети имеет расстояние 0.

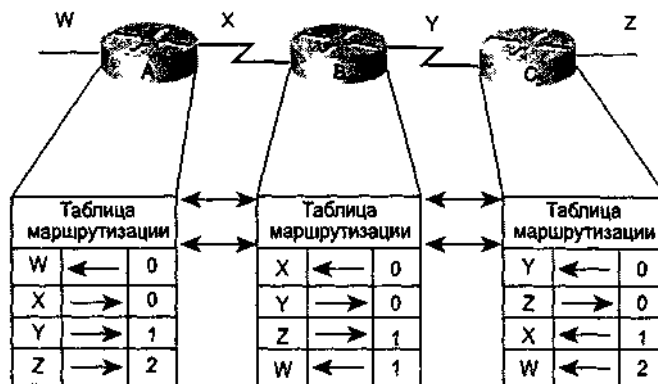


Рис. 11.16. Маршрутизаторы, использующие метод вектора расстояния, исследуют лучший путь к пункту назначения от каждого из своих соседей

Продолжая процесс исследования векторов расстояния в сети, маршрутизаторы как бы открывают наилучший путь до сети пункта назначения на основе информации от каждого соседа.

Например, маршрутизатор А узнает о других сетях, основываясь на информации, которую он получает от маршрутизатора В. Каждая запись в таблице маршрутизации об этих других сетях имеет кумулятивное значение вектора расстояния, показывающее, насколько далеко эта сеть находится в данном направлении.

Алгоритм маршрутизации по вектору расстояния и изменения топологии

При изменении топологии сети, использующей протокол на основе вектора расстояния, таблицы маршрутизации должны быть обновлены. Аналогично процессу исследования сети, обновление содержания таблиц маршрутизации из-за изменения топологии происходит шаг за шагом от одного маршрутизатора к другому (рис. 11.17).

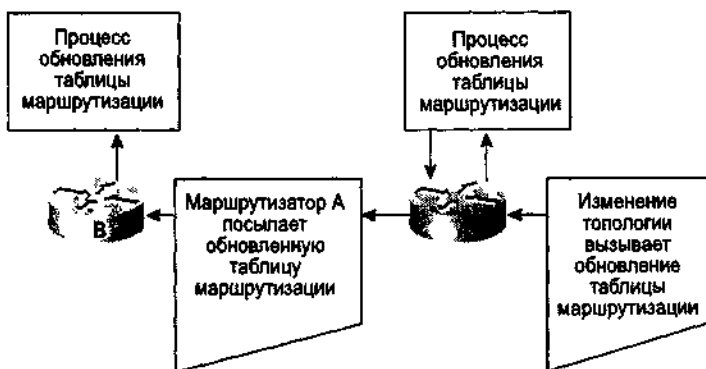


Рис. 11.17. Обновления таблиц маршрутизации происходят шаг за шагом от одного маршрутизатора к другому

Алгоритмы с вектором расстояния заставляют каждый маршрутизатор отсылать всю таблицу маршрутизации каждому своему непосредственному соседу. Таблицы маршрутизации, генерируемые в рамках метода вектора расстояния, содержат информацию об общей стоимости пути (определяемой его метрикой) и логический адрес первого маршрутизатора, стоящего на пути к каждой известной ему сети.

Проблема: маршрутизация по замкнутому кругу

Явление маршрутизации по замкнутому кругу может возникать в тех случаях, когда плохая сходимость сети на новой конфигурации вызывает наличие противоречивых записей о маршрутах. Эта ситуация проиллюстрирована на рис. 11.18.

1. Непосредственно перед отказом сети 1 все маршрутизаторы имеют непротиворечивую информацию и правильные таблицы маршрутизации. Как говорят, сеть сошлась. Предположим для целей данного примера, что предпочтительным путем к сети 1 в маршрутизаторе С является путь через маршрутизатор В и что в своей таблице маршрутизации маршрутизатор С имеет запись о расстоянии до сети 1, равном 3.
2. Когда в сети 1 происходит отказ, маршрутизатор Е посылает маршрутизатору А обновление, содержащее эту информацию. Маршрутизатор А прекращает направлять пакеты в сеть 1, но маршрутизаторы В, С и D продолжают это делать, так как они еще не проинформированы об отказе. После того как маршрутизатор А посылает свою обновленную таблицу маршрутизации, прекращают направлять пакеты в сеть 1 маршрутизаторы В и D, однако, маршрутизатор С по прежнему все еще не имеет обновленной информации. Для маршрутизатора С сеть 1 все так же доступна через маршрутизатор В. Это будет как бы новый предпочтительный маршрут с метрикой, равной трем переходам.
3. Теперь маршрутизатор С посылает периодическое обновление маршрутизатору D, указывающее на наличие пути к сети 1 через маршрутизатор В. Маршрутизатор D изменяет свою таблицу маршрутизации, отражая эту хорошую, но не правильную информацию, и передает эти сведения дальше маршрутизатору А. Маршрутизатор А распространяет их маршрутизаторам В и Е и т.д. Теперь любой пакет, имеющий назначением сеть 1, начинает ходить по кругу от маршрутизатора С — к В, далее — к А, затем — к D и назад к С.

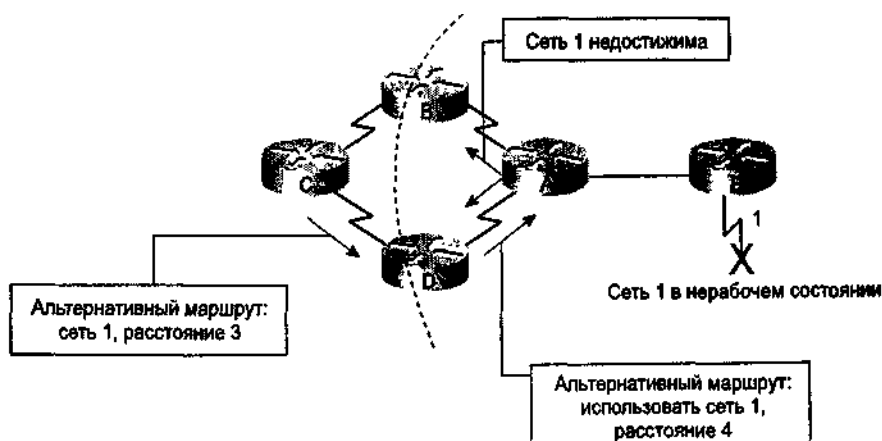


Рис. 11.18 Маршрутизатор А обновляет свою таблицу, отражая новое, но ошибочное значение количества переходов

Проблема: счет до бесконечности

Продолжим рассмотрение примера, описанного в предыдущем разделе. Некорректные пакеты обновления с информацией о сети 1 будут продолжать ходить по кругу до тех пор, пока какой-нибудь другой процесс не сможет остановить это заикливание. Подобное состояние, называемое *счетом до бесконечности*, продолжает заикливание перемещения пакетов по сети, несмотря на тот непреложный факт, что сеть 1 не работает. Пока маршрутизаторы имеют возможность считать до бесконечности, некорректная информация позволяет существовать маршрутизации по кругу.

В отсутствие контрмер, которые могли бы остановить процесс, вектор расстояния, исчисляемый количеством переходов, увеличивается на единицу каждый раз, когда пакет проходит следующий маршрутизатор (рис. 11.19). Эти пакеты ходят в сети по кругу из-за неправильной информации в таблицах маршрутизации.

Решение: задание максимального значения

Алгоритмы маршрутизации по вектору расстояния являются самокорректирующимися, но проблема маршрутизации по кругу прежде всего требует разрешения ситуации со счетом до бесконечности. Чтобы исключить эту длительную по времени проблему, в протоколах, использующих вектор расстояния, *бесконечность* определяется как некоторое максимальное число. Это число выражается в единицах метрики маршрутизации (например, в виде простого количества переходов).

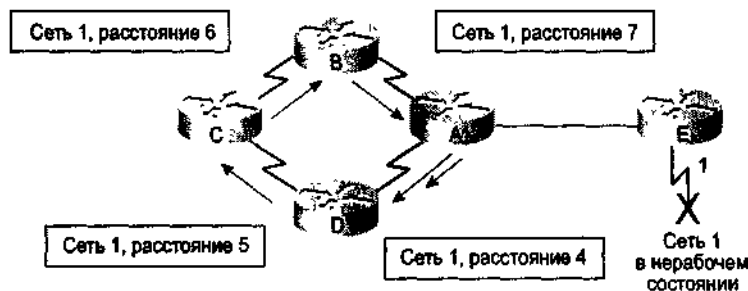


Рис. 11.19. Маршрутизация по кругу приводит к инкрементному увеличению вектора расстояния

При таком подходе протокол маршрутизации позволит существовать маршрутизации по кругу до тех пор, пока метрика не превысит максимально допустимое значение. На рис. 11.20 показан случай, когда это максимальное значение равно 16; обычно для векторов расстояния, измеряемых в количестве переходов, максимальное значение устанавливается равным 15 переходам. В любом случае, если значение метрики превысит максимум, то сеть 1 будет считаться недостижимой.

Решение: расщепление горизонта

Одним из способов устранения маршрутизации по кругу и ускорения сходимости сети является метод так называемого *расщепления горизонта*. Логика, стоящая за этим методом, заключается в том, что никогда нет ничего хорошего в посылке информации о маршруте назад в направлении, из которого она первоначально пришла.

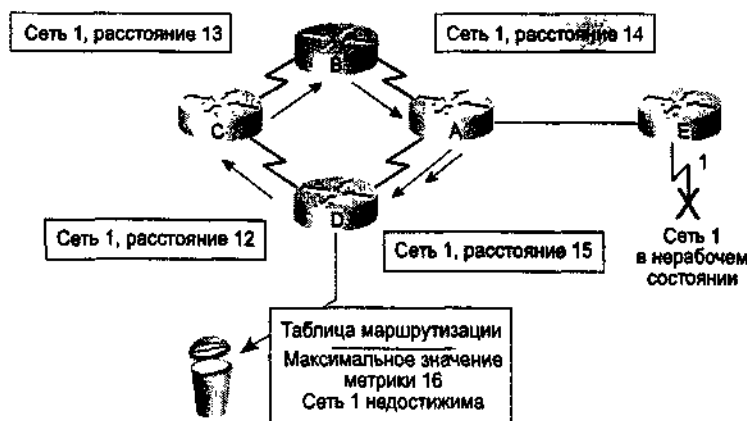


Рис. 11.20. Бесконечность можно определить в виде максимального допустимого расстояния

Другим возможным источником маршрутизации по кругу является ситуация, когда неправильная информация, посылаемая назад маршрутизатору, противоречит информации, посылаемой им самим. Вот как возникает эта проблема.

1. Маршрутизатор А передает маршрутизаторам В и D пакет актуализации, говорящий о том,

актуализации игнорируется. Игнорирование пакетов актуализации с худшей метрикой в период закрытия маршрута обеспечивает большее время на распространение сведений о разрушительном изменении по всей сети.

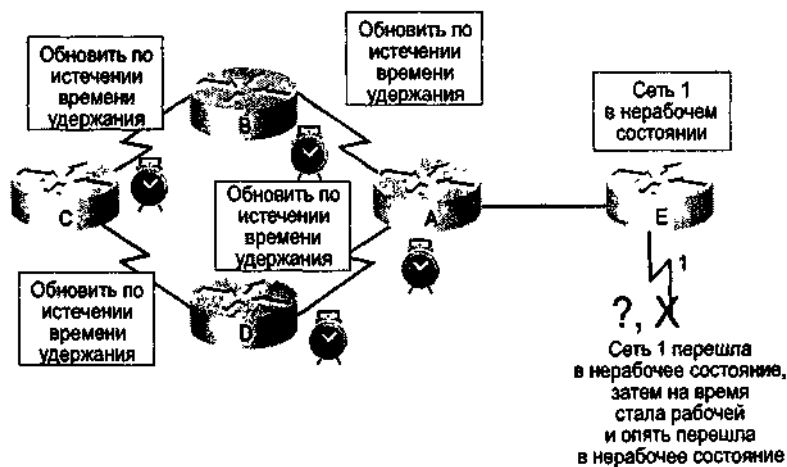


Рис. 11.22. Маршрутизатор удерживает запись о нерабочем состоянии сети, предоставляя время на то, чтобы другие маршрутизаторы выполнили соответствующий пересчет этого изменения в топологии

Алгоритмы маршрутизации с учетом состояния канала связи

Вторым основным алгоритмом, используемым для маршрутизации, является алгоритм с учетом состояния канала связи. Алгоритмы маршрутизации с учетом состояния канала связи, также известные под названием *алгоритмов выбора первого кратчайшего пути* (shortest path first (SPF) algorithms), поддерживают сложную базу данных топологической информации. И если алгоритмы с маршрутизацией по вектору расстояния работают с неконкретной информацией о дальних сетях, то алгоритмы маршрутизации с учетом состояния канала собирают полные данные о дальних маршрутизаторах и о том, как они соединены друг с другом.

Для выполнения маршрутизации с учетом состояния канала связи используются сообщения объявлений о состоянии канала (link-state advertisements, LSA), база данных топологии, SPF-алгоритм, результирующее SPS-дерево и таблица маршрутизации, содержащая пути и порты к каждой сети (рис. 11.23). В последующих разделах приводится более подробное описание этих процессов и баз данных.

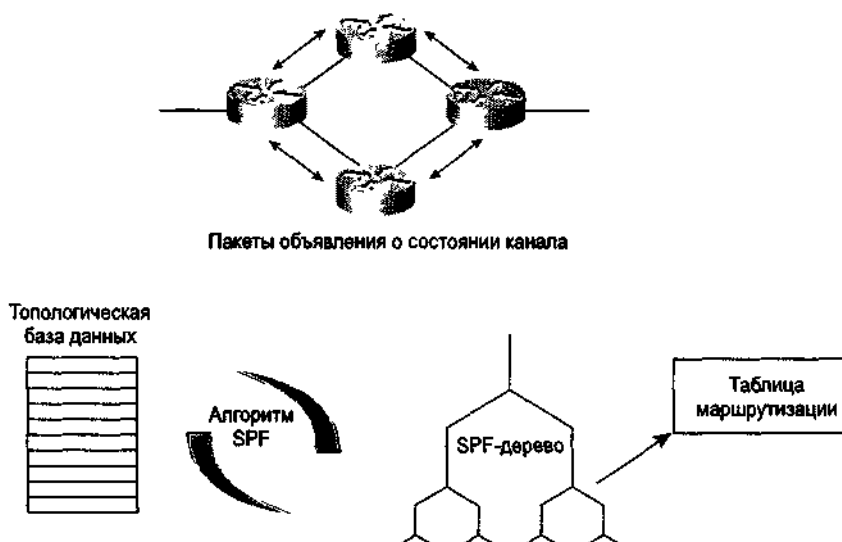


Рис. 11.23. Алгоритм, учитывающий состояние канала связи, обновляет информацию о топологии на всех других маршрутизаторах

Инженерами концепция учета состояния канала была реализована в виде OSPF-маршрутизации. Описание концепций, заложенных в протокол OSPF, а также описание работы этого протокола содержится в документе RFC 1583.

Режим исследования сети в алгоритмах с учетом состояния канала

Для создания общей картины всей сети используются механизмы исследования сети с учетом состояния канала связи. После этого все маршрутизаторы, которые работают с алгоритмом учета состояния канала, коллективно используют это представление сети. Все это подобно существованию нескольких идентичных карт города. На рис. 11.24 четыре сети (W, X, Y и Z) соединены тремя маршрутизаторами, выполняющими маршрутизацию с учетом состояния канала связи.

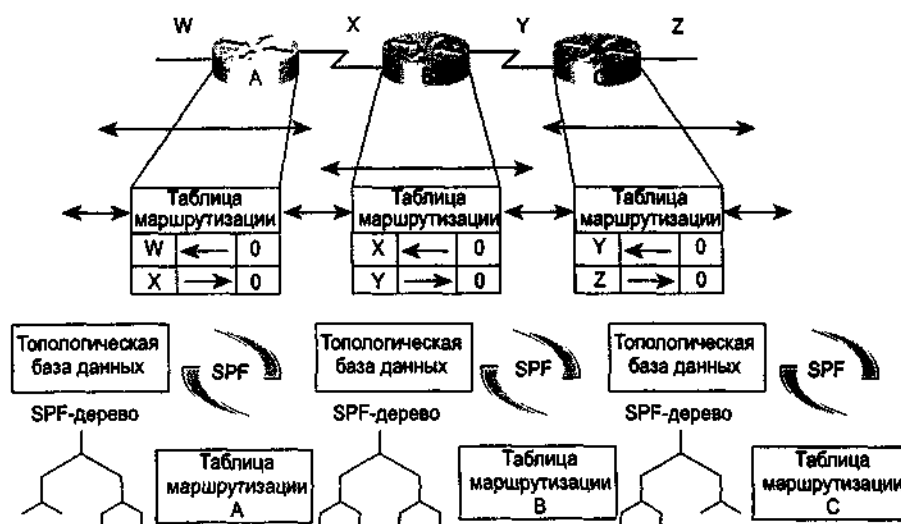


Рис. 11.24. При выполнении маршрутизации с учетом состояния канала связи маршрутизаторы вычисляют кратчайший путь к получателям параллельно

В режиме исследования сети при маршрутизации с учетом состояния канала связи выполняются следующие процессы.

1. Маршрутизаторы обмениваются друг с другом LSA-сообщениями. Каждый маршрутизатор начинает с непосредственно подключенных сетей, о которых у него есть прямая информация.
2. Маршрутизаторы параллельно друг с другом создают топологическую базу данных, содержащую все LSA-сообщения, сгенерированные в сетевом комплексе.
3. SPF-алгоритм вычисляет достижимость сетей, определяя кратчайший путь до каждой сети сетевого комплекса, где применяется протокол маршрутизации с учетом состояния канала связи. Маршрутизатор создает эту логическую топологию кратчайших путей в виде SPF-дерева, помещая себя в корень. Это дерево отображает пути от маршрутизатора до всех пунктов назначения.
4. Наилучшие пути и порты, имеющие выход на эти сети назначения, сводятся маршрутизатором в таблице маршрутизации. Он также формирует и другие базы данных с топологическими элементами и подробностями о статусе.

Обработка изменений топологии в протоколах маршрутизации с учетом состояния канала связи

Алгоритмы учета состояния канала связи полагаются на маршрутизаторы, имеющие общее представление о сети. Как показано на рис. 11.25, при изменении топологии в сетевом комплексе, использующем маршрутизацию с учетом состояния канала связи, маршрутизаторы, которые первыми узнают об изменении, посылают информацию другим маршрутизаторам или специально назначенному маршрутизатору, который затем может использовать все другие маршрутизаторы для обновления своей топологической информации. Это влечет за собой отсылку общей маршрутной информации всем маршрутизаторам, стоящим в сети. Для достижения сходимости каждый маршрутизатор выполняет следующие действия.

- Отслеживает своих соседей: его имя, его рабочее состояние и стоимость линии связи с ним.
- Создает LSA-пакет, в котором приводится перечень имен соседних маршрутизаторов и стоимость линий связи. Сюда же включаются данные о новых соседях, об изменениях в стоимости линий связи и о связях с соседями, которые стали нерабочими.
- Посылает LSA-пакет, так что все другие маршрутизаторы получают его.
- Получая LSA-пакет, записывает его в свою базу данных, так что он может хранить самые последние LSA-пакеты, сгенерированные каждым другим маршрутизатором.
- Используя накопленные данные LSA-пакетов для создания полной карты топологии сети, маршрутизатор, стартуя с этой общей точки, запускает на исполнение SPF-алгоритм и рассчитывает маршруты до каждой сети назначения.

Каждый раз, когда LSA-пакет вызывает изменение в базе данных состояний каналов, алгоритм учета состояния каналов связи пересчитывает лучшие пути и обновляет таблицу маршрутизации. Затем каждый маршрутизатор принимает к сведению изменение топологии и определяет кратчайшие пути для использования при коммутировании пакетов.

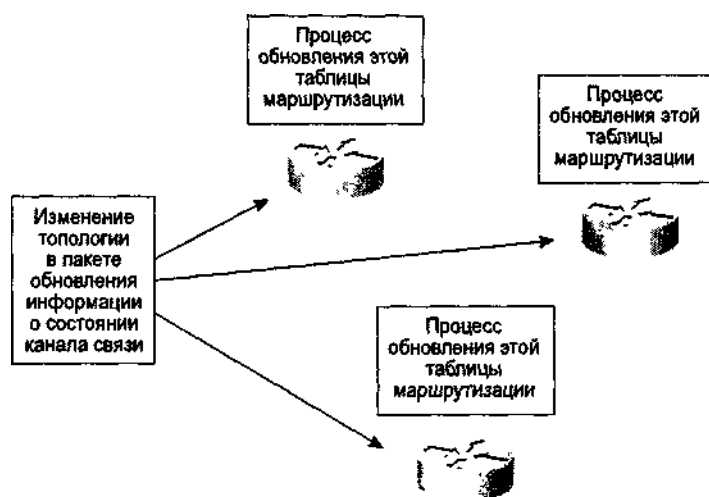


Рис. 11.25. Процессы обновления данных идут с использованием одних и тех же пакетов обновления информации о состоянии каналов связи

Моменты, которые требуют внимания

Как показано на рис. 11.26, при использовании протоколов с учетом состояния Канала связи существуют два основных момента, требующих повышенного внимания.

- *Требования по объему памяти и вычислительной мощности.* В большинстве ситуаций исполнение протоколов маршрутизации с учетом состояния канала связи требует, чтобы маршрутизаторы имели большой объем памяти и большие возможности по обработке. Сетевые администраторы должны гарантировать, что выбранные маршрутизаторы способны предоставлять такие ресурсы для выполнения маршрутизации.

Маршрутизаторы отслеживают своих соседей и сети, с которыми они могут связываться через

другие узлы маршрутизации. При использовании маршрутизации с учетом состояния канала в памяти должна сохраняться информация различных баз данных, дерево топологии и таблица маршрутизации.

В свою очередь, вычисление кратчайшего пути требует решение задачи, объем которой пропорционален количеству связей в сетевом комплексе, умноженному на количество маршрутизаторов в сети.

- *Требования по ширине полосы пропускания.* Во время начального процесса исследования все маршрутизаторы, использующие протоколы маршрутизации с учетом состояния канала связи, посылают всем другим маршрутизаторам LSA-пакеты. Это действие перегружает сетевой комплекс на период, когда маршрутизаторы нуждаются в максимально широкой полосе пропускания, и временно уменьшает полосу, доступную для маршрутизируемого трафика, несущего информацию пользователей.

После этой начальной перегрузки протоколы маршрутизации с учетом состояния канала связи обычно довольствуются шириной полосы пропускания сетевого комплекса, которая используется только для посылки нечастых или вообще запускаемых по событию LSA-пакетов, отражающих изменения топологии.

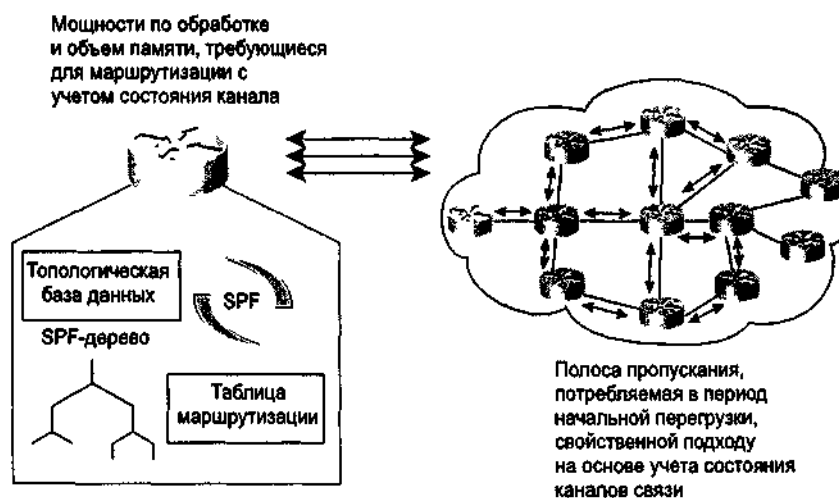


Рис. 11.26. Двама основными моментами, требующими внимания при применении алгоритмов маршрутизации с учетом состояния канала связи, являются объем памяти и вычислительная мощность, необходимые для осуществления такой маршрутизации, и величина полосы пропускания, потребляемая в момент начальной перегрузки, свойственной подходу на основе учета состояния канала связи

Проблема: обновление информации о состоянии каналов связи

Наиболее сложным и важным аспектом маршрутизации с учетом состояния канала связи является обеспечение получения всеми маршрутизаторами всех необходимых LSA-пакетов. Маршрутизаторы с различными наборами LSA-пакетов вычисляют маршруты на основе разных топологических данных. Как показано на рис. 11.27, в результате несогласия маршрутизаторов относительно состояния канала связи маршруты могут становиться недостижимыми. Ниже приведен пример несовместимой информации о пути.

- Предположим, что сеть 1, находящаяся между маршрутизаторами С и D, переходит в нерабочее состояние. Как обсуждалось ранее, оба маршрутизатора создают LSA-пакет, отражающий этот статус недостижимости.
- Вскоре после этого сеть 1 снова становится работоспособной. Поэтому необходим другой LSA-пакет, который бы отражал следующее изменение топологии.
- Если первоначальное сообщение маршрутизатора С "Сеть 1 недостижима" передается в

пакете актуализации по медленному пути, то этот пакет поступит позже. Таким образом, этот LSA-пакет может прийти на маршрутизатор А после LSA-пакета маршрутизатора D "Сеть 1 снова работоспособна".

- При такой рассинхронизации LSA-пакетов маршрутизатор А может столкнуться с дилеммой выбора, какое SPF-дерево строить: использовать пути, включающие сеть 1, или не учитывать сеть 1, последняя информация о которой подтверждает, что она недостижима?

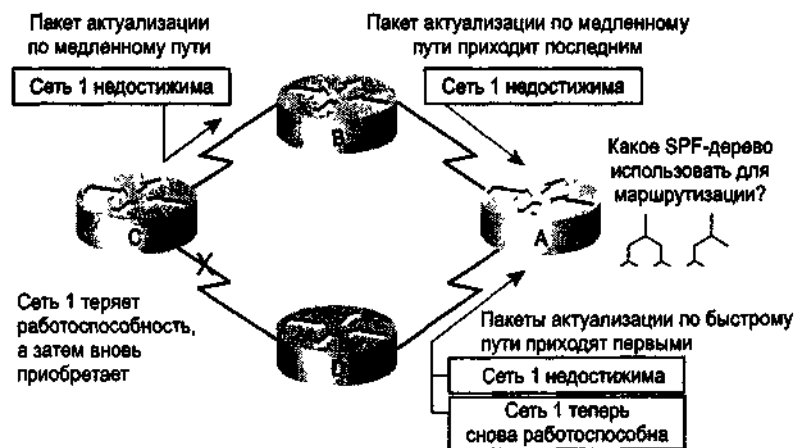


Рис. 11 27 Несинхронизированное поступление пакетов актуализации и противоречивые решения относительно путей делают маршрутизаторы недостижимыми

Если LSA-пакеты распространяются всем маршрутизаторам неправильно, то маршрутизация с учетом состояния канала связи может привести к возникновению некорректных маршрутов.

Переход на использование протоколов на основе учета состояния канала связи в очень больших сетевых комплексах может усугубить проблему неправильного распространения LSA-пакетов.

Если одна часть сети возвращается в рабочее состояние быстрее, чем другая, то порядок отсылки и получения LSA-пакетов будет меняться, что может изменить и ухудшить сходимость. Маршрутизаторы могут узнавать о различных версиях топологии до момента построения своих SPF-деревьев и таблиц маршрутизации. В больших сетях части, в которых обновление информации происходит быстрее, могут составлять проблемы для тех частей, где обновление происходит медленнее.

Решение: механизмы учета состояния канала связи

Маршрутизация с учетом состояния канала связи имеет несколько методик для предотвращения возникновения потенциальных проблем, возникающих из-за нехватки ресурсов и плохого распространения пакетов с информацией о состоянии каналов (link-state packets, LSP).

- Администратор сети может увеличить периодичность распространения LSP-I пакетов таким образом, чтобы обновления происходили только после некоторого конфигурируемого продолжительного периода времени. Снижение скорости периодических обновлений не мешает LSP-обновлениям, генерируемым изменениями в топологии.
- LSP-пакеты обновлений могут включаться в группу многоадресной рассылки, не нагружать все маршрутизаторы. Для нескольких соединенных между собой ЛВС можно использовать в качестве назначенного депозитария, ответственного за передачу LSP-пакетов, один или несколько маршрутизаторов. Другие маршрутизаторы могут использовать эти назначенные маршрутизаторы в качестве специализированного источника непротиворечивых данных о топологии.

- В больших сетях можно построить иерархию различных областей. Маршрутизатор из одной области иерархического домена не обязательно должен хранить и обрабатывать LSP-пакеты других маршрутизаторов, не принадлежащих этой области.
- Что касается проблем координации LSP-пакетов, то конкретная реализация метода учета состояния канала связи позволяет иметь LSP-пакетам временные метки, порядковые номера, а также применять различные схемы учета их возраста и другие связанные механизмы, которые помогают избежать неправильного распространения LSP-пакетов или нескоординированных обновлений логической информации.

Сравнение маршрутизации по вектору расстояния и маршрутизации с учетом состояния канала связи.

Сравнивать маршрутизацию по вектору расстояния и маршрутизацию с учетом состояния канала связи можно в нескольких ключевых областях (табл. 11.1).

- Процесс маршрутизации по вектору расстояния получает все топологические данные из информации, содержащейся в таблицах маршрутизации соседей. Процесс маршрутизации с учетом состояния канала связи получает широко представление обо всей топологии сетевого комплекса, собирая данные из всех необходимых LSA-пакетов.
- Процесс маршрутизации по вектору расстояния определяет лучший путь с помощью сложения получаемых метрик по мере того, как таблица движется от одного маршрутизатора к другому. При использовании маршрутизации с учетом состояния канала каждый маршрутизатор работает отдельно, вычисляя свой собственный кратчайший путь к пункту назначения.
- В большинстве протоколов маршрутизации по вектору расстояния пакеты актуализации, содержащие сведения об изменениях топологии, являются периодически посылаемыми пакетами актуализации таблиц маршрутизации. Эти таблицы передаются от одного маршрутизатора к другому, что обычно приводит к более медленной сходимости.
- В протоколах маршрутизации с учетом состояния канала связи пакеты актуализации обычно генерируются и рассылаются по факту возникновения изменения топологии. Относительно небольшие LSA-пакеты передаются всем другим маршрутизаторам, что, как правило, приводит к более быстрой сходимости при любом изменении топологии сетевого комплекса.

Таблица 11.1. Рабочие качества маршрутизации по вектору расстояния и маршрутизации с учетом состояния канала связи

Маршрутизация по вектору расстояния	Маршрутизация с учетом состояния канала связи
Видит топологию сети глазами соседних маршрутизаторов	Получает общий вид топологии всей сети
Суммирует вектор расстояния от одного маршрутизатора к другому	Вычисляет кратчайший путь до других маршрутизаторов
Частые периодические обновления топологической информации, медленная сходимость	Обновления инициируются фактом изменения топологии; быстрая сходимость
Передаёт копии таблицы маршрутизации только соседним маршрутизаторам	Передаёт пакеты с информацией об актуальном состоянии канала связи всем другим маршрутизаторам

Сбалансированная гибридная маршрутизация

Возникающий третий тип протоколов маршрутизации объединяет аспекты маршрутизации по вектору расстояния и маршрутизации с учетом состояния канала связи (рис. 11.28) и называется *сбалансированной гибридной маршрутизацией*.

Для определения наилучших путей до сетей назначения протокол сбалансированной гибридной маршрутизации предусматривает использование векторов расстояния с более точной метрикой. Однако он отличается от большинства протоколов маршрутизации по вектору расстояния тем, что обновления базы данных маршрутной информации инициируются фактом изменения топологии.

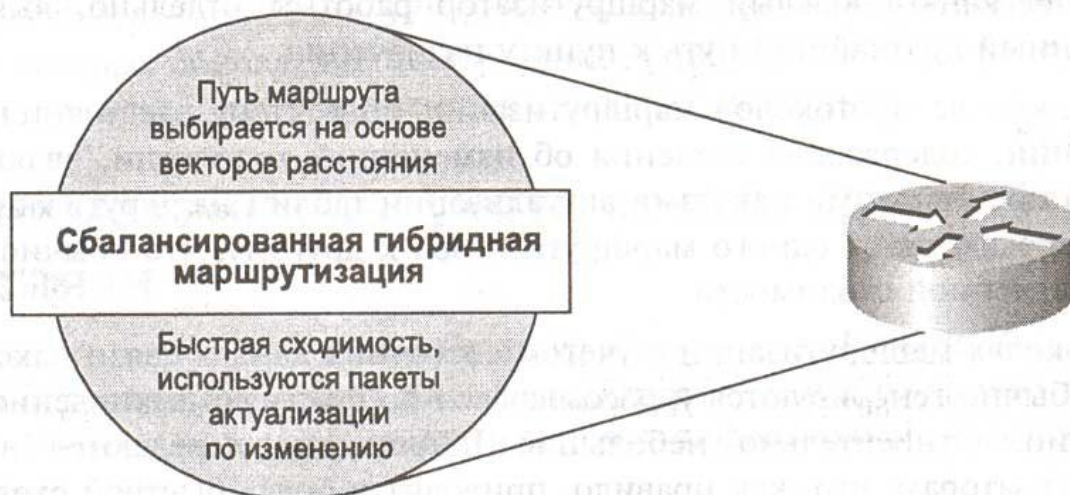


Рис. 11.28. Гибридная маршрутизация содержит признаки маршрутизации по вектору расстояния и маршрутизации с учетом состояния канала связи

Протоколы, относящиеся к типу сбалансированной гибридной маршрутизации, сходятся быстрее, приближаясь по этому показателю к протоколам маршрутизации с учетом состояния канала связи. Однако они отличаются от них меньшим потреблением таких ресурсов, как ширина полосы пропускания, объем памяти, и меньшими накладными расходами процессора. Примерами протоколов со сбалансированной гибридной маршрутизацией являются протокол взаимодействия открытых систем промежуточная система — промежуточная система (OSI Intermediate System — Intermediate System, IS-IS) и усовершенствованный протокол IGRP (EIGRP) компании Cisco.

Базовые процессы маршрутизации

Вне зависимости от того, использует ли сеть механизмы маршрутизации по вектору расстояния или маршрутизации с учетом состояния канала связи, ее маршрутизаторы должны выполнять одинаковые базовые функции маршрутизации. Сетевой уровень должен устанавливать связь и играть роль интерфейса с различными более низкими уровнями. Маршрутизаторы должны уметь без проблем работать с пакетами, инкапсулированными в различные кадры более низкого уровня, не меняя при этом адресацию пакета уровня 3.

Маршрутизация из одной локальной сети в другую

На рис. 11.29 показан пример выполнения сетевым уровнем роли интерфейса в процессе маршрутизации из одной локальной сети в другую. В этом примере трафику пакетов из источника "хост 4", находящегося в сети 1 Ethernet, нужен путь к пункту назначения "хост 5" в сети 2. Определение наилучшего пути для находящихся в локальных сетях хост-машин зависит от

маршрутизатора и его непротиворечивой адресации сетей.

Проверяя свои записи в таблице маршрутизации, маршрутизатор находит, что наилучший путь к сети 2 пункта назначения лежит через выходной порт ToO — интерфейс с ЛВС Token Ring.

Хотя формат кадра более низкого уровня должен измениться при коммутировании трафика маршрутизатором из сети 1 Ethernet в сеть 2 Token Ring, адресация источника и пункта назначения уровня 3 остается такой же. Как показано на рис. 11.29, адрес пункта назначения остается "Сеть 2, Хост 5", несмотря на другую инкапсуляцию более низкого уровня.

Маршрутизация из локальной сети в глобальную

Для перенаправления трафика из локальной сети в глобальную сетевой уровень должен устанавливать связь и играть роль интерфейса с различными более низкими уровнями. По мере роста сетевого комплекса путь пакета может проходить через несколько точек ретрансляции и иметь дело с различными типами канального уровня, стоящими за различными локальными сетями. Например, на рис. 11.30 пакет от показанной сверху рабочей станции с адресом 1.3 должен пройти три типа канальных уровней, чтобы попасть на файл-сервер с адресом 2.4, показанный внизу рисунка.

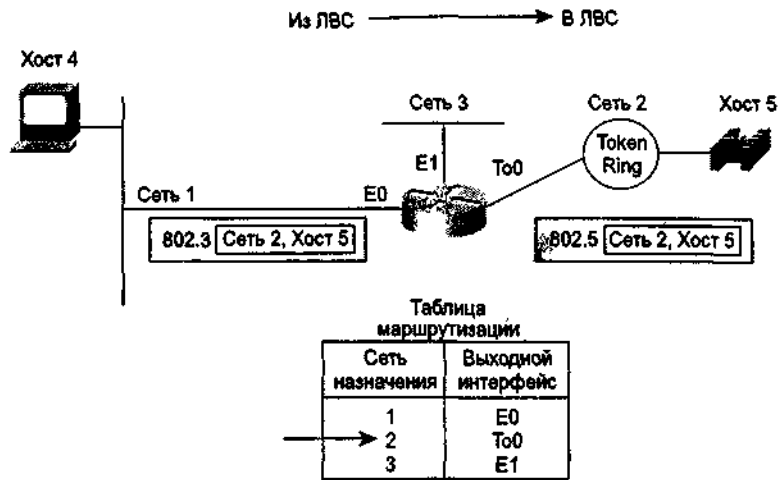


Рис. 11.29. При поиске маршрута маршрутизатор использует содержащийся в пакете сетевой адрес пункта назначения

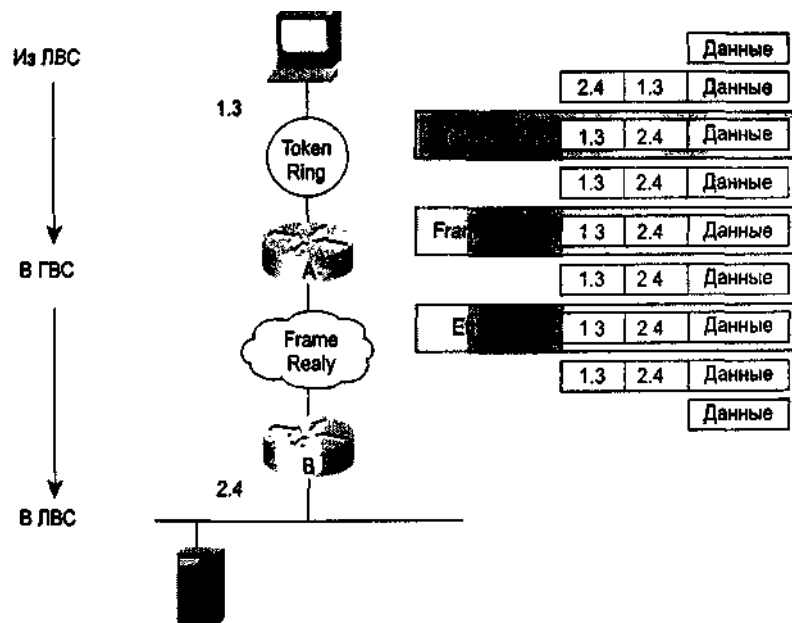


Рис. 11.30. При перенаправлении пакета маршрутизаторы сохраняют информацию о сквозном адресе

Маршрутизируемая связь осуществляется в следующей последовательности базовых шагов.

1. Рабочая станция посылает пакет файл-серверу, инкапсулируя его в кадр Token Ring, адресованный маршрутизатору А.
2. Когда маршрутизатор А получает кадр, он извлекает пакет из кадра Token Ring, инкапсулирует его в кадр Frame Relay и направляет этот кадр маршрутизатору В.
3. Маршрутизатор В извлекает пакет из кадра Frame Relay и переадресовывает его файл-серверу в составе вновь созданного кадра Ethernet.
4. Когда файл-сервер с адресом 2.4 принимает кадр Ethernet, он извлекает пакет и передает его соответствующему процессу более высокого уровня.

Маршрутизаторы обеспечивают возможность организации потока пакетов из локальной сети в глобальную за счет сохранения неизменными сквозных адресов источника и пункта назначения, инкапсулируя при этом пакет на порту в кадр канального уровня с форматом, соответствующим формату, используемому на следующем переходе пути.

Резюме

- К функциям межсетевого взаимодействия сетевого уровня относятся адресация сетей и выбор наилучшего пути для трафика.
- Маршрутизируемые протоколы направляют трафик пользователей, тогда как протоколы маршрутизации работают между маршрутизаторами, обеспечивая поддержание таблиц путей.
- Режим исследования сети при маршрутизации по вектору расстояния связан с обменом таблицами маршрутизации; одна из возможных проблем — медленная сходимости.
- При маршрутизации с учетом состояния канала связи маршрутизаторы рассчитывают кратчайшие пути к другим маршрутизаторам; одна из возможных проблем — противоречивые пакеты актуализации маршрутной информации.
- Сбалансированная гибридная маршрутизация содержит признаки как маршрутизации с учетом состояния канала связи, так и маршрутизации по вектору расстояния, используя найденные пути для нескольких протоколов.

Контрольные вопросы

1. Какое из приведенных ниже определений наилучшим образом описывает одну из функций уровня 3 (сетевого уровня) модели OSI?
 - A. Несет ответственность за надежную связь между узлами сети.
 - B.Его забота — физическая адресация и топология сети.
 - C.Определяет наилучший путь трафика через сеть.
 - D. Управляет обменом данными между объектами презентационного уровня.
2. Какая функция позволяет маршрутизаторам оценивать имеющиеся маршруты к пункту назначения и устанавливать предпочтительный способ обработки пакетов?
 - A.Функция компоновки данных.
 - B.Функция определения пути.
 - C.Интерфейсный протокол SDLC.
 - D. Протокол Frame Relay.
3. Как сетевой уровень посылает пакеты от источника в пункт назначения?
 - A. Используя таблицу IP-маршрутизации.
 - B.Используя ARP-ответы.
 - C.Обращаясь к серверу имен.
 - D. Обращаясь к мосту.
4. Какие две части адреса используются маршрутизатором для передачи трафика по сети?
 - A. Сетевой адрес и адрес хост-машины.
 - B.Сетевой адрес и MAC-адрес.
 - C.Адрес хост-машины и MAC-адрес.
 - D. MAC-адрес и маска подсети.
5. Какое из приведенных ниже определений наилучшим образом описывает маршрутизируемый протокол?
 - A. Обеспечивает достаточно информации, чтобы направить пакет от одной хост-машины к другой.
 - B.Обеспечивает информацию, необходимую для передачи пакетов вверх на следующий наивысший сетевой уровень.
 - C.Позволяет маршрутизаторам взаимодействовать с другими маршрутизаторами в целях ведения и обновления таблиц адресов.
 - D. Позволяет маршрутизаторам связывать вместе MAC- и IP-адрес.
6. Какое из приведенных ниже определений наилучшим образом описывает протокол маршрутизации?
 - A. Протокол, который выполняет маршрутизацию посредством реализованного в нем алгоритма.
 - B.Протокол, который определяет, как и когда связываются MAC- и IP-адреса.
 - C.Протокол, который определяет формат и использование полей в пакете данных.
 - D. Протокол, позволяющий пересылать пакеты между хост-машинами.
7. Каково одно из преимуществ алгоритмов, основанных на использовании вектора расстояния?
 - A. Малая вероятность счета до бесконечности.
 - B.Легко реализуются в очень больших сетях.
 - C.Не предрасположены к маршрутизации по кругу.
 - D. Просты в вычислении.
8. Какое из приведенных ниже определений наилучшим образом описывает алгоритм маршрутизации с учетом состояния канала связи?
 - A. Воссоздает точную топологию всего сетевого комплекса.
 - B.Требует минимальных вычислений.
 - C.Определяет направление и расстояние до любой связи в сетевом комплексе.
 - D. Имеет небольшие сетевые накладные расходы и уменьшает общий трафик.
9. Из-за чего возникает маршрутизация по кругу?
 - A. После видоизменения сетевого комплекса имеет место низкая сходимость.

- В. Искусственно создаются расщепленные горизонты.
 - С. Катастрофический отказ сегментов сети приводит к каскадному выходу из строя других сетевых сегментов.
 - Д. Сетевой администратор не установил и не инициировал маршруты по умолчанию.
10. Какое из приведенных ниже определений наилучшим образом описывает сбалансированную гибридную маршрутизацию?
- А. Для определения наилучших путей в ней используются векторы расстояния, но обновления таблиц маршрутизации инициируются фактом изменения топологии.
 - В. Во время периодов высокого трафика для определения наилучших путей между узлами топологии используются векторы расстояния.
 - С. Для определения наилучших путей используется информация о топологии, но при этом обновления таблиц маршрутизации происходят не часто.
 - Д. Для определения наилучших путей используется информация о топологии, но при этом для обхода неактивных сетевых каналов применяются векторы расстояния.

Глава 12

Пользовательский интерфейс маршрутизатора и режимы

В этой главе..

- Команды и процесс программирования маршрутизатора
- Пользовательский режим
- Привилегированный режим
- Команда помощи help
- Редактирование
- Когда, зачем и К2Й просматривать историю команд

Введение

В главе 11, "Сетевой уровень и маршрутизация", рассказывалось об использовании маршрутизаторов и операциях, выполняемых сетевым уровнем эталонной модели [взаимодействия открытых систем (OSI) при реализации ключевой функции по обеспечению межсетевого взаимодействия. В данной главе будет описана роль сетевого [администратора в управлении маршрутизатором, чтобы тот обеспечивал эффективную и своевременную доставку данных в сети.

Краткое описание интерфейса пользователя

Маршрутизаторы Cisco могут конфигурироваться с помощью интерфейса пользователя, исполняемого на консоли маршрутизатора или на терминале, а также через удаленный доступ. Перед тем как будет возможным ввод команд исполнительного режима EXEC, необходимо осуществить вход в маршрутизатор.

В целях безопасности маршрутизаторы Cisco имеют два уровня доступа к командам:

- *Пользовательский режим* — типовые задачи, включая проверку состояния маршрутизатора. В этом режиме изменять конфигурацию маршрутизатора не разрешается.
- *Привилегированный режим* — типовые задачи, включая изменение конфигурации маршрутизатора.

Вход в систему маршрутизатора: межсетевая операционная система компании Cisco (IOS)

При первом входе в маршрутизатор пользователь видит командную строку пользовательского режима, которая выглядит следующим образом:

```
Router>
```

Команды, доступные на пользовательском уровне, представляют собой подмножество команд, доступных в привилегированном режиме. Большинство этих команд позволяют выводить на экран информацию без изменения установок конфигурации маршрутизатора.

Чтобы получить доступ к полному набору команд, необходимо сначала активизировать привилегированный режим. О переходе в этот режим будет свидетельствовать появление в командной строке знака фунта (#). С привилегированного уровня также можно получить доступ к режиму глобального конфигурирования и другим специальным режимам конфигурирования, включая режимы конфигурирования интерфейса, подинтерфейса, линии, маршрутизатора, карты маршрутов и несколько дополнительных режимов конфигурирования (листинг 12.1).

Листинг 12.1. Вход и выход из маршрутизатора

```
Router con0 is now available.  
Press RETURN to get started.
```

```
User Access Verification
```

```
Password:
```

```
Router>
```

```
Router> enable
```

```
Password:
```

```
Router#
```

```
Router# /disable
```

```
Router>
```

```
Router> exit
```

Примечание

Следует помнить, что вид выводимой на экран информации изменяется в зависимости от конкретного уровня ОС IOS и конфигурации маршрутизатора.

Для выхода из системы необходимо набрать на клавиатуре команду exit (выход).

Команды пользовательского режима

При вводе в командной строке пользовательского или привилегированного режима знака вопроса (?) на экран выводится удобный в использовании список общеупотребительных команд. Например, если в командной строке Router> воспользоваться командой ?, то результатом будет список команд пользовательского режима, который показан в табл. 12.1.

Router> ?

Таблица 12.1. Команды пользовательского режима

Команда	Описание
access-enable	Создание временной записи в списке доступа
atmsig	Исполнение команд выдачи АТМ-сигналов
cd	Изменение текущего активного устройства
clear	Сброс функций
connect	Открытие терминального соединения
dir	Вывод списка файлов на данном устройстве
disable	Отключение исполнения привилегированных команд
disconnect	Разрыв существующего соединения в сети
enable	Включение исполнения привилегированных команд
exit	Выход из режима EXEC
help	Выдача описания интерактивной системы помощи
lat	Открытие LAT-соединения
lock	Блокировка терминала
login	Вход в систему под именем конкретного пользователя
logout	Выход из режима EXEC
mrinfo	Запрос многоадресному маршрутизатору относительно соседей и версии программного обеспечения
mstat	Вывод статистических данных после исполнения нескольких многоадресных трассировок маршрутов
mtrace	Выполнение трассировки обратного многоадресного пути от пункта назначения к источнику
name-connection	Присваивание имени существующему сетевому соединению
pad	Открытие X 29 РАО-соединения
ping	Посылка эхо-сообщений
PPP	Запуск исполнения протокола PPP
pwd	Вывод названия текущего активного устройства
resume	Восстановление активного сетевого соединения
rlogin	Открытие соединения удаленного доступа в систему
show	Показ текущих рабочих установок системы
slip	Запуск исполнения протокола IP для канала с последовательной передачей данных
systat	Вывод на экран информации о каналах терминала
telnet	Открытие Telnet-соединения
terminal	Установка параметров терминального канала

tn3270	Открытие TSH270-соединения
traceroute	Запуск трассировки до пункта назначения
tunnel	Открытие туннельного соединения
where	Вывод списка активных соединений
x3	Установка X 3 параметров РАО-устройства
xremote	Переход в режим удаленной работы XRemote

На экран выводится 22 строки, поэтому иногда внизу экрана будет появляться подсказка — More —, свидетельствующая о том, что выводимый результат исполнения команды содержит несколько экранных страниц, т е как в рассматриваемом примере, существуют еще другие команды.

Примечание

При работе с ОС IOS везде, где появляется подсказка - More -, переход к следующей экранной странице осуществляется после нажатия клавиши пробела Для перехода на следующую строку необходимо нажать клавишу перевода каретки <Return> (или на некоторых клавиатурах — клавишу <Enter>) Для возврата к командной строке следует нажать любую другую клавишу

Команды привилегированного режима

Для входа в привилегированный режим EXEC необходимо набрать на клавиатуре команду **enable** (или ее сокращение — **ena**)

```
Roter> ena
Password:
```

Также необходимо ввести пароль Ввод знака вопроса (?) в командной строке привилегированного режима

```
Router# ?
```

приведет к выводу на экран значительно более длинного списка команд Некоторые из этих команд показаны в табл 12 2

Примечание

Набор команд привилегированного режима EXEC включает команды пользовательского режима EXEC

Таблица 12.2. Команды привилегированного режима

Команда	Описание
access-enable	Создание временной записи в списке доступа
access-template	Создание временной записи в списке доступа
appn	Отсылка команд в подсистему APPN
atmsig	Исполнение команд выдачи ATM-сигналов
bfe	Установка ручных аварийных режимов
calendar	Управление аппаратно реализованной системой календаря
cd	Изменение текущего активного устройства
clear	Сброс функций
clock	Управление системными часами
cmt	Пуск или останов функций управления FDDI-соединениями
configure	Вход в режим конфигурирования
connect	Открытие терминального соединения

copy	Копирование конфигурации или образа ОС IOS
debug	Использование отладочных функций (см также undebg)
delete	Удаление файла
dir	Вывод списка файлов на данном устройстве
disable	Отключение исполнения привилегированных команд
disconnect	Разрыв существующего соединения в сети
enable	Включение исполнения привилегированных команд
erase	Стирание информации из флэш-памяти или памяти используемой для хранения конфигурации
exit	Выход из режима EXEC
format	Форматирование устройства
help	Выдача описания интерактивной системы помощи
lat	Открытие LAT-соединения
lock	Блокировка терминала
login	Вход в систему под именем конкретного пользователя
logout	Выход из режима EXEC
mbranch	Трассировка многоадресного маршрута вниз по ветви дерева
mrbranch	Обратная трассировка многоадресного маршрута вверх по ветви дерева
mrinfo	Запрос многоадресному маршрутизатору относительно соседей и версии программного обеспечения
mstat	Вывод статистических данных после исполнения нескольких многоадресных трассировок маршрутов
mtrace	Выполнение трассировки обратного многоадресного пути от пункта назначения к источнику
name-connection	Присваивание имени существующему сетевому соединению
ncia	Запуск/останов NCIA-сервера
pad	Открытие X 29 PAO-соединения
ping	Посылка эхо-сообщений
PPP	Запуск исполнения протокола PPP
pwd	Вывод названия текущего активного устройства
reload	Останов и выполнение холодного возврата
resume	Восстановление активного сетевого соединения
rlogin	Открытие соединения удаленного входа в систему
rsh	Исполнение удаленных команд
sdlc	Посылка тестовых SDLC-кадров
send	Посылка сообщения по tty-каналам (телетайпным)
setup	Исполнение функции команды setup
show	Показ текущих рабочих установок системы
slip	Запуск исполнения протокола IP для канала с последовательной передачей данных
squeeze	Включение на устройстве режима уплотнения
start-chat	Запуск скрипта режима диалоговой переписки в реальном времени по каналу
systat	Вывод на экран информации о каналах терминала
tarp	Определяет приемник команд процесса преобразования IP-адреса
telnet	Открытие Telnet-соединения
terminal	Установка параметров терминального канала
test	Тестирование подсистем, памяти и интерфейсов
tn3270	Открытие TM3270-соединения
traceroute	Запуск трассировки до пункта назначения
tunnel	Открытие туннельного соединения
undebg	Отключение функций отладки (см. также debug)
undelete	Отмена удаления файла
verify	Проверка контрольной суммы файла, заносимого во флеш-память

where	Вывод списка активных соединений
which-route	Просмотр таблицы OSI-маршрутов и вывод на экран результатов
write	Запись рабочей конфигурации в память, выдача ее в сеть или на терминал
x3	Установка X.3 параметров PAD-устройства
xremote	Переход в режим удаленной работы XRemote

Функции команды help

Предположим, необходимо установить часы маршрутизатора. Если пользователь не знает команды, с помощью которой это можно сделать, то для проверки синтаксиса установки часов он может воспользоваться командой help, результат исполнения которой для данного примера показан в листинге 12.2.

Листинг 12.2. Функции команды help

```
Router# clock
Translating "CLOCK"
% Unknown command or computer name, or unable to find computer address

Router# cl?
clear  clock

Router# clock
% Incomplete command.

Router# clock ?
set    Set the time and date

Router# clock set %
Incomplete command

Routert# clock set ?
Current Time ( hh : mm : ss )
```

Показанная в листинге 12.2 информация, выведенная командой help, свидетельствует о том, что необходимо еще ключевое слово set. На следующем этапе можно посмотреть синтаксис ввода времени и ввести текущее время в формате *часы, минуты, секунды*, как это показано в листинге 12.3.

Листинг 12.3. Проверка синтаксиса и подсказка команды

```
Router# clock set 19:56:00 % Incomplete command.
Router# clock set 19:56:00 ?
<1- 1>    Day of the month
MONTH    Month of the year

Router# clock set 19:56:00 04 8
% Invalid input detected at the '^' marker

Router# clock set 19:56:00 04 August
% Incomplete command.

Router# clock set 19:56:00 04 August ?
<1993-2035>  Year
```

Как видно из листинга 12.3, система говорит, что для завершения команды пользователь должен предоставить дополнительную информацию. Для автоматического повторения ввода предыдущей команды необходимо воспользоваться комбинацией клавиш <Ctrl+P> (или клавишей со стрелкой вверх). Затем, чтобы выяснить необходимые дополнительные аргументы, следует ввести пробел и знак вопроса (?). Теперь пользователь сможет завершить ввод команды.

Наличие знака вставки (^) и реакции системы помощи говорит о наличии ошибки. Чтобы получить перечень правильных синтаксических конструкций, необходимо ввести команду до той точки, где имеет место ошибка, а затем ввести знак вопроса (?). После этого надо ввести код, используя правильный синтаксис, и для исполнения команды нажать клавишу <Return>.

Следует помнить, что интерфейс пользователя обеспечивает проверку синтаксиса, помещая знак вставки (^) в том месте, где есть ошибка. Этот знак всегда появляется в командной последовательности там, где была введена неправильная команда, ключевое слово или аргумент. Указатель местоположения ошибки и интерактивная система помощи позволяют легко находить и исправлять синтаксические ошибки.

Применение команд редактирования

Пользовательский интерфейс имеет режим усовершенствованного редактирования, который обеспечивает реализацию набора основных функций редактирования. В текущей версии программного обеспечения режим усовершенствованного редактирования включается автоматически, однако его можно отключить и вернуться к режиму редактирования, который обеспечивался в предыдущих версиях. Отключение усовершенствованного режима может понадобиться в тех случаях, когда приходится иметь дело с написанными скриптами, которые плохо работают, если этот режим включен.

Чтобы переместить курсор в пределах командной строки для выполнения корректировок или изменений, используются комбинации клавиш, приведенные в табл. 12.3.

Таблица 12.3. Команды редактирования

Команда	Описание
Ctrl-A	Перемещение в начало командной строки
Ctrl-E	Перемещение в конец командной строки
Esc-B	Перемещение назад на одно слово
Ctrl-F	Перемещение вперед на один символ
Ctrl-B	Перемещение назад на один символ
Esc-F	Перемещение вперед на одно слово

Набор команд редактирования обеспечивает также реализацию функции горизонтальной прокрутки, что полезно для команд, не помещающихся в одной строке экрана. Когда курсор достигает правой границы, командная строка сдвигается на 10 символов влево. При этом первые 10 символов строки не видны, но для просмотра синтаксиса в начале команды возможна прокрутка в обратном направлении.

Для осуществления обратной прокрутки можно использовать комбинацию клавиш <Ctrl+B> или клавишу со стрелкой влево, нажимая их до тех пор, пока курсор не попадет в начало вводимой команды, или сразу нажать клавиши <Ctrl+A>, в результате чего курсор сразу возвращается непосредственно в начало строки.

Просмотр истории команд

Интерфейс пользователя предоставляет возможность просмотра истории или регистрационной записи команд, которые вводились. Эта функция особенно полезна при повторном вводе длинных или сложных команд или записей. Как показано в табл. 12.4, функция ведения истории команд позволяет выполнять следующие задачи:

- устанавливать размер буфера истории команд;
- повторно обращаться к командам;
- отключать функцию ведения истории команд.

Таблица 12.4. Команды функции истории команд

Команда	Описание
Ctrl-P или клавиша <i>со стрелкой вверх</i>	Обращение к последней (предыдущей) команде
ctrl-N или клавиша <i>со стрелкой вниз</i>	Обращение к последующей введенной команде
show history	Вывод содержимого буфера команд
terminal history [size <i>количество строк</i>]	Установка размера буфера команд
no terminal editing	Отключение режима усовершенствованного редактирования
terminal editing	Возобновление режима усовершенствованного редактирования
<i>Клавиша табулятора (Tab)</i>	Завершение ввода

По умолчанию функция ведения истории команд активизирована и система записывает в буфер истории 10 командных строк. Для изменения количества командных строк, записываемых системой в течение текущего терминального сеанса, необходимо воспользоваться командой `terminal history size` или `history size`. Максимально в буфер истории можно включить 256 команд.

Для того чтобы обратиться к командам в буфере истории, начиная с последней введенной, необходимо нажать комбинацию клавиш `<Ctrl+P>` или клавишу со стрелкой вверх. Для последовательного обращения к более старым командам надо повторно нажимать эти клавиши.

Чтобы возвратиться к последующим командам в буфере истории после обращения к ним с помощью клавиш `<Ctrl+P>` или клавиши со стрелкой вверх, следует нажать комбинацию клавиш `<Ctrl+N>` или клавишу со стрелкой вниз. Повторное нажатие этих клавиш приведет к последовательному вызову более свежих команд.

После ввода уникальных характеристик команды нажатие клавиши `<Tab>` приведет к тому, что интерфейс завершит ввод команды.

Большинство переносных компьютеров может также иметь дополнительные средства для выполнения выделения и копирования. Пользователь может скопировать предыдущую командную последовательность, затем вставить ее как текущую вводимую команду и нажать клавишу `<Return>`.

Нажатие комбинации клавиш `<Ctrl+Z>` выводит из режима конфигурирования.

Резюме

- Конфигурирование маршрутизаторов Cisco можно осуществлять через пользовательский интерфейс, исполняемый на консоли маршрутизатора, или на терминале.
- В целях безопасности маршрутизаторы Cisco имеют два уровня доступа к командам: пользовательский и привилегированный режимы.
- Используя интерфейс пользователя, можно.
 - входить в систему по паролю пользователя;
 - входить в привилегированный режим по паролю, вводимому после команды `enable`;
 - отключать функции или завершать сеанс.
 - Развитые функции помощи позволяют
 - завершать оформление команды и получать подсказки;
 - проверять синтаксис.
- Интерфейс пользователя имеет режим усовершенствованного редактирования, который обеспечивает реализацию ключевых функций редактирования.
- Интерфейс пользователя предоставляет возможность просмотра истории или регистрационной записи команд, которые вводились.

Контрольные вопросы

1. Какие два режима доступа к командам маршрутизатора существуют в маршрутизаторах Cisco?
 - A. Пользовательский и привилегированный.
 - B. Пользовательский и гостевой.
 - C. Привилегированный и гостевой.
 - D. Гостевой и анонимный.
2. Какой режим используется при внесении изменений в конфигурацию маршрутизаторов Cisco?
 - A. Пользовательский.
 - B. Привилегированный.
 - C. Администратора.
 - D. Корневой.
3. Что означает, когда в интерфейсе пользователя маршрутизатора Cisco появляется символа "больше чем" (>) ?
 - A. Режим входа в систему.
 - B. Режим помощи.
 - C. Пользовательский режим.
 - D. Привилегированный режим.
4. Какой из приведенных ниже символов свидетельствует о том, что данная командная строка является строкой привилегированного режима интерфейса пользователя маршрутизаторов Cisco?
 - A. #.
 - B. >.
 - C. <.
 - D. |#.
5. Какой из режимов предоставляет доступ к списку общеупотребительных команд, если при работе с интерфейсом пользователя маршрутизаторов Cisco ввести с клавиатуры символ знак вопроса ("?")?
 - A. Гостевой.
 - B. Только привилегированный.
 - C. Только пользовательский.
 - D. Пользовательский и привилегированный.
6. Что означает подсказка — More — , появляющаяся внизу экрана интерфейса пользователя маршрутизаторов Cisco?
 - A. Выводимая информация имеет несколько экранных страниц.
 - B. В страницах, выводимых вручную, имеются дополнительные детали.
 - C. Команда требует нескольких элементов.
 - D. Должны быть оговорены дополнительные условия.
7. Нажатие каких клавиш при работе с интерфейсом пользователя маршрутизаторов Cisco приводит к автоматическому повторению ввода предыдущей команды?
 - A. <Стрелка влево>
 - B. <Стрелка вправо>
 - C. <Ctrl+R>.
 - D. <Ctrl+PX
8. Что произойдет, если при работе с интерфейсом пользователя маршрутизаторов Cisco нажать клавишу со стрелкой вверх?
 - A. На экран будет выведен список всех пользователей, зарегистрированных в маршрутизаторе.
 - B. На экран будет выведена последняя введенная команда.
 - C. Будет распечатана информация, представленная на экране.
 - D. Текущий процесс будет приостановлен.
9. Что произойдет, если при работе с интерфейсом пользователя маршрутизаторов Cisco ввести символ вопросительного знака?
 - A. На экран будет выведен список всех пользователей, зарегистрированных в маршрутизаторе.
 - B. На экран будет выведена последняя введенная команда.

- C. Пользователь войдет в систему помощи.
 - D. Будет показан текущий режим работы.
10. Что произойдет, если набрать команду show ? в командной строке?
- A. Будет показан список пользователей, работающих в данный момент с маршрутизатором.
 - B. Будут показаны список всех активных соединений и их статус.
 - C. Будет показана последняя таблица.
 - D. Будет показан перечень подкоманд, которые могут применяться совместно с командой show.

Глава 13

Вывод информации о конфигурации маршрутизатора

В этой главе.

- Компоненты, участвующие в конфигурировании маршрутизатора
- Режим работы маршрутизатора
- Применение форм команды `show` для исследования состояния маршрутизатора
- Использование команды `telnet` для тестирования уровня приложений
- Использование команды `ping`, `trace` и `show ip route` для тестирования сетевого уровня
- Применение команды `show interface serial` для тестирования физического и канального уровней

Введение

В главе 12, "Пользовательский интерфейс маршрутизатора и режимы", рассказывалось о роли администратора сети в управлении маршрутизатором, чтобы тот обеспечивал эффективную и своевременную доставку данных в сети. В этой главе будут описаны процедуры и команды для доступа к маршрутизатору, проверки и обслуживания его составляющих и для тестирования установления связи в сети.

Компоненты маршрутизатора, участвующие в конфигурировании, и режимы работы маршрутизатора

В данном разделе рассказывается о компонентах маршрутизатора, которые играют ключевую роль в процессе конфигурирования. Знание компонентов, участвующих в процессе конфигурирования, обеспечивает лучшее понимание того, как маршрутизатор хранит и использует вводимые команды конфигурирования. Представление о шагах, имеющих место при инициализации маршрутизатора, помогает в определении сути и места возникновения проблем, которые могут появиться в момент запуска маршрутизатора.

Внешние источники конфигурации

Как показано на рис. 13.1, маршрутизатор можно конфигурировать с помощью многих внешних источников.

- После начальной инсталляции он может конфигурироваться с консольного терминала, который представляет собой компьютер, подключенный к маршрутизатору через порт консоли. К нему можно подключиться через модем, используя порт дополнительного устройства (AUX).
- Будучи инсталлированным в сети, он может конфигурироваться через каналы виртуального терминала с номерами от 0 до 4.
- Конфигурационный файл также может загружаться по сети с TFTP-сервера.

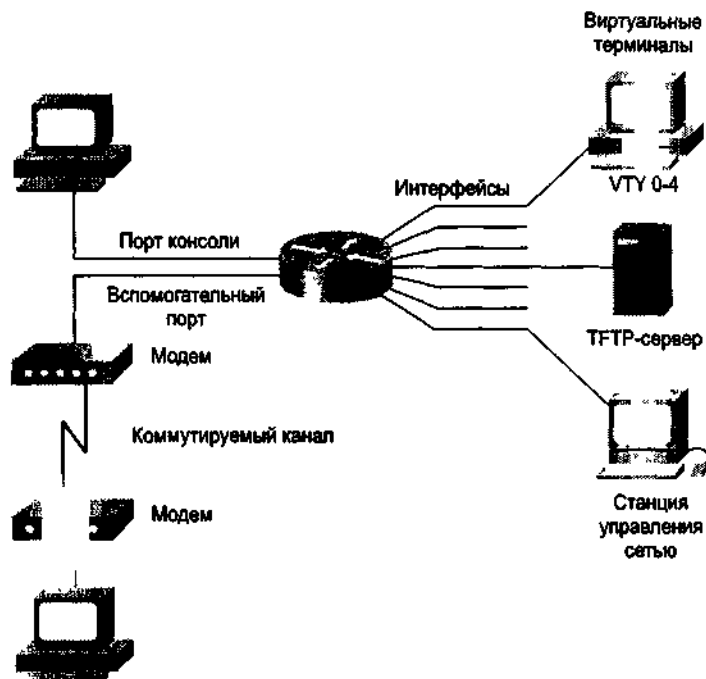


Рис. 13.1. Конфигурационная информация может поступать из различных источников

Внутренние компоненты маршрутизатора, участвующие в конфигурировании

Внутренняя архитектура маршрутизаторов Cisco поддерживает компоненты, которые играют важную роль в процессе его начального запуска (рис. 13.2). К внутренним компонентам, участвующим в процессе конфигурирования, относятся следующие.

- *ОЗУ/ДОЗУ*— хранит таблицы маршрутизации, ARP-кэш, кэш быстрой коммутации, буферы пакетов (область ОЗУ совместного пользования) и очереди захваченных пакетов. При включенном питании ОЗУ также играет роль временной и/или рабочей памяти для конфигурационного файла. При отключении питания или перезапуске содержимое ОЗУ теряется. Наконец, ОЗУ также содержит копию ОС IOS компании Cisco.
- *Энергонезависимое ОЗУ*— хранит резервную копию конфигурационного файла маршрутизатора. При отключении питания или перезапуске его содержимое сохраняется.
- *Флэш-память* — стираемое перепрограммируемое ПЗУ. Во флэш-памяти хранится образ операционной системы и микрокод. Она позволяет обновлять программное обеспечение без удаления или замены микросхем на плате процессора. Содержимое флэш-памяти не теряется при отключении питания или перезапуске. В ней может храниться несколько копий ОС IOS, а также конфигурационные файлы и загрузочные образы.
- *ПЗУ*— содержит программу диагностики по включению питания, программу начальной загрузки и программное обеспечение операционной системы. Для обновления версии программного обеспечения необходимо удалить и заменить на плате центрального процессора вставляемые микросхемы.
- *Интерфейсы* — соединения с сетью, через которые пакеты поступают в маршрутизатор и покидают его. Интерфейсы размещаются на материнской плате или в отдельных интерфейсных модулях.

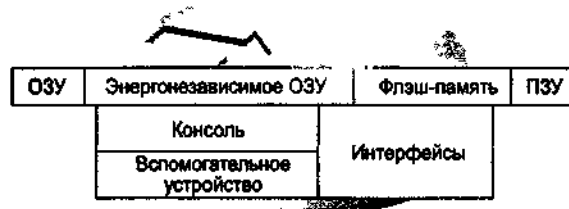


Рис. 13.2. Внутренние компоненты, участвующие в процессе маршрутизации, включают несколько элементов

Рабочее хранение информации в ОЗУ

ОЗУ — это область памяти, используемая для хранения информации во время работы. После подачи питания на маршрутизатор программа начальной загрузки выполняется из ПЗУ. Эта программа выполняет некоторые тесты и затем загружает в ОЗУ ОС IOS. Одной из частей ОС IOS является модуль управления исполнением команд EXEC, который принимает и выполняет команды, вводимые в маршрутизатор.

Как показано на рис. 13.3, маршрутизатор также хранит активный файл конфигурации, таблицы карт сети и списки адресов маршрутизации. Содержимое конфигурационного файла может быть выведено на экран удаленного терминала или на экран консоли. Сохраненная версия этого файла хранится в энергонезависимом ОЗУ. Каждый раз при инициализации маршрутизатора выполняется обращение к этому сохраненному файлу и его загрузка в основную память. Конфигурационный файл содержит информацию об общесистемных настройках, настройках процессов и интерфейсов, которая непосредственно определяет работу маршрутизатора и его интерфейсных портов.

Образ операционной системы не может быть выведен на экран терминала, обычно он исполняется из основного ОЗУ и загружается из одного из нескольких источников. Операционная система организована в виде подпрограмм, которые обрабатывают различные задачи, связанные с различными протоколами, перемещением данных, управлением таблицами и буферами, маршрутизацией пакетов актуализации и выполнением команд пользователя.

Режимы маршрутизатора

Независимо от того, как обращаются к маршрутизатору, через консоль или в рамках сеанса протокола Telnet через порт вспомогательного устройства, его можно перевести в один из нескольких режимов. Интерфейс пользователя ОС IOS обеспечивает доступ к режимам выполнения команд, каждый из которых обладает различными функциями.

- *Пользовательский режим EXEC* — это режим просмотра, в котором пользователь может только просматривать определенную информацию о маршрутизаторе, но не может ничего менять. В этом режиме используется командная строка вида `Router>`.
- *Привилегированный режим EXEC* — поддерживает команды отладки и тестирования, детальную проверку маршрутизатора, манипуляции с конфигурационным файлом и доступ к режимам конфигурирования. В нем используется командная строка вида `Router#`.
- *Режим начальной установки (setup)* — обеспечивает диалоговое взаимодействие с подсказками, через консоль, которое позволяет новому пользователю создать начальную базовую конфигурацию.
- *Режим глобального конфигурирования* — реализует мощные однострочные команды, решающие простые задачи конфигурирования. В нем используется командная строка вида `Router (config) #`.
- *Другие режимы конфигурирования* — в них выполняется более сложное многострочное конфигурирование. Они используют командную строку вида

Router(config-mode)#.

- Режим *RXBOOT* — это служебный режим, который наряду с другими вещами может быть использован для восстановления забытых паролей.

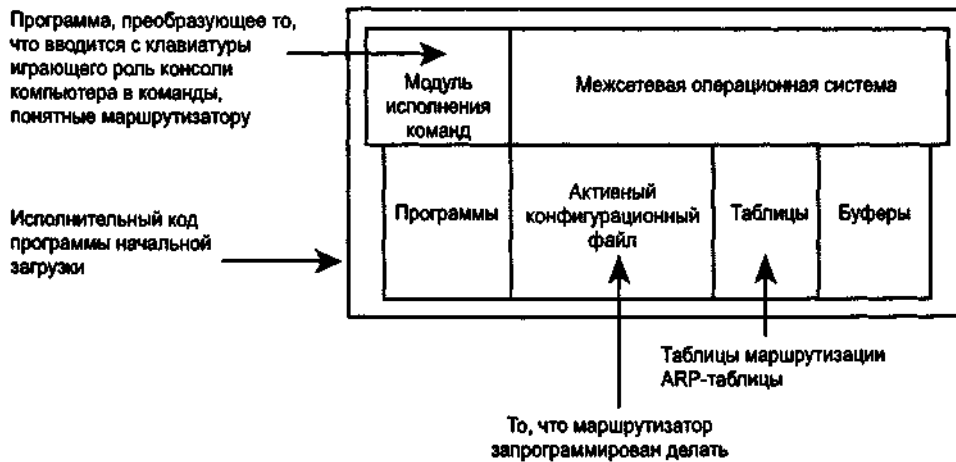


Рис. 13.3. В маршрутизаторе хранится активный конфигурационный файл

Проверка состояния маршрутизатора с помощью команд просмотра статуса

В данном разделе рассказывается об основных командах, которые можно использовать для определения текущего состояния маршрутизатора и которые помогают получить жизненно важную информацию, необходимую для контроля и устранения неисправностей в работе маршрутизатора.

Очень важно иметь возможность контроля правильности функционирования и состояния маршрутизатора в любой момент времени. Как показано на рис. 13.4, маршрутизаторы Cisco имеют ряд команд, которые позволяют определять правильность функционирования и место, где возникла проблема.

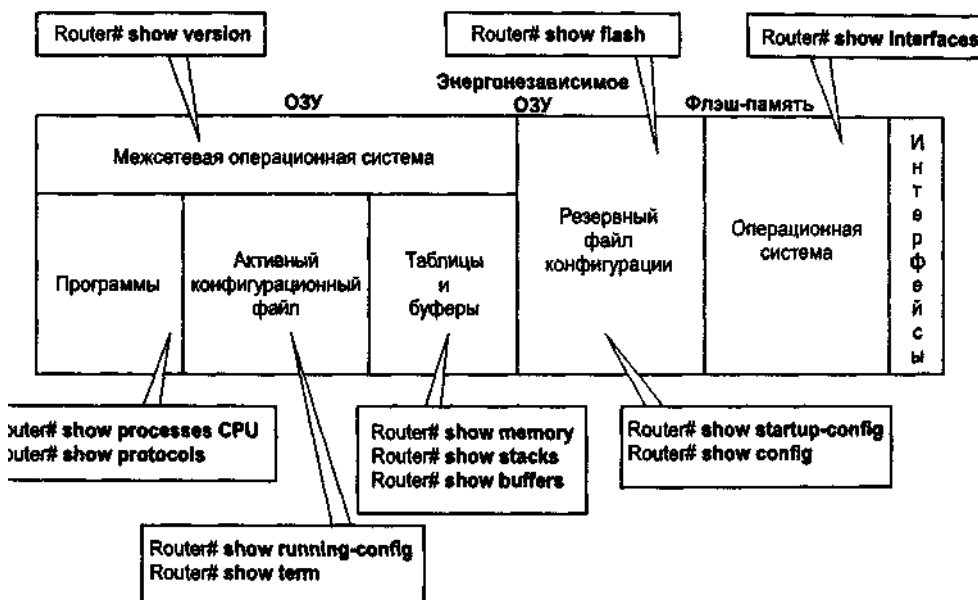


Рис. 13.4. Существует множество команд, применяемых для мониторинга конфигурации маршрутизатора

Команды проверки состояния маршрутизатора приведены в табл. 13.1.

Таблица 13.1 Команда состояния маршрутизатора.

Команда	Описание
show version	Выводит на экран данные о конфигурации аппаратной части системы, версии программного обеспечения, именах и источниках конфигурационных файлов и загрузочных образов, а также информацию о причинах последней перезагрузки системы
show process	Выводит информацию об активных процессах
show protocols	Выводит данные о сконфигурированных протоколах. Эта команда показывает статус всех сконфигурированных протоколов уровня 3(сетевого)
show memory	Показывает статистические данные о памяти маршрутизатора, включая статистику свободных пулов памяти
show stacks	Показывает содержимое стека используемых процессов и подпрограмм прерывания
show buffers	Обеспечивает статданные по пулам буферов маршрутизатора
show flash	Выводит информацию об устройстве флэш-памяти
show running-config (write term в ОС IOS версии 10.3 или в более ранних версиях)	Показывает содержание активного конфигурационного файла
show startup-config (show config в ОС IOS версии 10.3 или в более ранних версиях)	Выводит на экран содержание резервного конфигурационного файла
show interfaces	Показывает статистические данные по всем интерфейсам, сконфигурированным в маршрутизаторе

Примечание

Используемые в ОС IOS версии 10.3 и более ранние команды write term и show config были заменены новыми. В текущей версии эти команды продолжают выполнять свои функции, но больше не упоминаются в документации. В будущей версии эти команды поддерживаются. Пользователь знает, что перед ним активный конфигурационный файл, если сверху есть надпись Current Configuration ("Текущая конфигурация"). Точно так же, пользователь знает, что перед ним резервная копия конфигурационного файла, если вверху экрана есть сообщения об объеме использованной энергонезависимой памяти.

Команды show running-config и show startup-config

Команды show running-config (листинг 13.1) и show startup-config (листинг 13.2) относятся к наиболее часто используемым командам режима EXEC ОС IOS, которые позволяют администратору видеть текущую рабочую конфигурацию маршрутизатора или размер образа и команды начального конфигурирования, которые будут использоваться маршрутизатором при следующем перезапуске.

Листинг 13.1. Команда show running-config

```
Router# show running-config
Building configuration...
Current configuration:
!
version 11 . 1
!
```

--More--

Листинг 13.2. Команда show startup-config

```
Router# show startup-config
Using 1108 out of 130048 bytes
!
version 11.2
!

Hostname router
-- More --
```

Команда show interfaces

Команда `show interfaces` выводит на экран значения конфигурируемых параметров и статданные реального времени, связанные с последовательными интерфейсами (листинг 13.3).

Листинг 13.3. Команда show interfaces

```
Router# show interfaces
Serial0 is up, line protocol is up
Hardware is MK5025
Internet address is 183.8.64.129, subnet mask is 255.255.255.128
MTU 1500 bytes, BW 56 kbit, DLY 20000 usec, rely 255/255. load 9/255
Encapsulation HDLC, loopback not set, keepalive set (10 sec)
Last input 0:00:00, output 0:00:01, output hang never
Last clearing of show interfaces counters never
Output queue 0/40, 0 drops, input queue 0/75, 0 drops
Five minute input rate 1000 bits/sec, 0 packets/sec
1885 packets input, 624002 1 bytes, no buffer
Received 2 0457 broadcasts, 0 runts, 0 giants
3 input errors, 3 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
403591 packets output, 66717279 bytes, 0 underruns
0 output errors, 0 collisions, 8 interface resets, 0 restarts
45 carrier transitions
```

Команда show version

Команда `show version` выводит на экран информацию о версии ОС IOS компании Cisco, которая в данный момент выполняется маршрутизатором (листинг 13.4).

Листинг 13.4. Команда show version

```
Router# show version
Cisco Internetwork Operating System Software
IOS (tm) 4500 Software (C4500-J-M). Version 11.2
Copyright (c) 1986-1996 by Cisco Systems, Inc.
Compiled Fri 28-Jun-96 16:32 by rbeach
Image text-base: 0x600088A0, data-base: 0x6076E000
ROM: System Bootstrap, Version 5.1(1) RELEASE SOFTWARE (fcl)
ROM: 4500-XBOOT Bootstrap Software, Version 10.1(1) RELEASE SOFTWARE (fcl)
router uptime is 1 week, 3 days, 32 minutes
System restarted by reload
System image file is c4500-j-mz, booted via tftp from 171.69.1.129
- More -
```

Команда show protocols

Команда `show protocols` используется для вывода данных о протоколах, сконфигурированных

на маршрутизаторе. Эта команда показывает глобальный и специфический для интерфейса статус всех сконфигурированных протоколов уровня 3 (например, IP, DECnet, IPX и AppleTalk) (листинг 13.5).

Листинг 13.5. Команда show protocols

```
Router# show protocols
Globalvalues:
Internet Protocol routing is enabled
DECNET routing is enabled
XNS routing is enabled
Vines routing is enabled
AppleTalk routing s enabled
Novell rout ng is enabled
- More-
Ethernet0 is up, line protocol is up
Internet address is 183.8.126.2, subnet mask is 255.255.255.128
Decnet cost is 5
XNS address is 010.aa00.0400.0284
CLNS enabled
Vines metric is 32
AppleTalk address is 3012.9 , zone Id-e0
Novell address is 3010.aa00.0400.0284
- More -
```

Получение доступа к другим маршрутизаторам с помощью протокола Cisco Discovery Protocol

Протокол обнаружения, созданный в компании Cisco (Cisco Discovery Protocol, CDP), обеспечивает единственную разработки компании команду, которая позволяет администраторам иметь доступ к сводным кратким данным о том, как выглядит конфигурация других имеющих непосредственное соединение маршрутизаторов. Протокол CDP работает на канальном уровне, соединяя физическую среду передачи данных более низкого уровня с протоколами более высокого сетевого уровня (рис. 13.5). Поскольку он работает на этом уровне, то CDP-устройства, поддерживающие различные протоколы сетевого уровня, могут узнавать друг о друге. (Следует помнить, что канальный адрес является тем же самым, что MAC-адрес.)

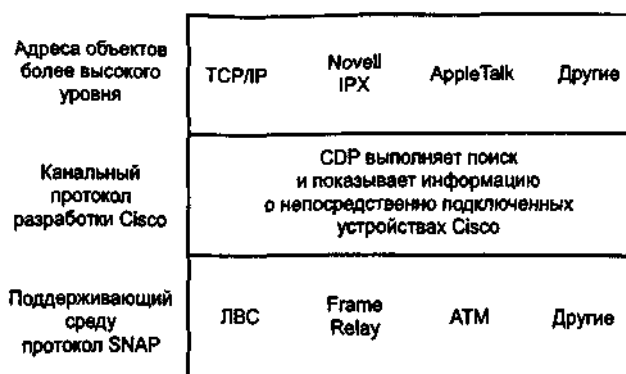


Рис. 13.5 Протокол CDP позволяет обнаружить соседние устройства в многопротокольных сетях

При запуске устройства, работающего с ОС IOS версии 10.3 или более поздней, протокол CDP запускается автоматически. После этого он может автоматически обнаружить соседние устройства Cisco, на которых тоже выполняется протокол CDP. Среди обнаруженных устройств будут не только те, которые работают с протоколом TCP/IP. Протокол CDP обнаруживает непосредственно соединенные устройства Cisco независимо от того, какой набор протоколов

уровней 3 и 4 на них исполняется.

Вывод записей протокола CDP о соседних устройствах

Основной задачей протокола CDP является получение данных о платформах соседних устройств и исполняемых ими протоколах. Для вывода на локальном маршрутизаторе обновленных записей протокола CDP используется команда **show cdp neighbors**.

На рис. 13.6 показано, как протокол CDP дает менеджеру системы полезную информацию. Каждый маршрутизатор, на котором исполняется протокол CDP, обменивается со своими соседями информацией обо всех известных ему протоколах. Администратор может посмотреть результаты этого обмена CDP-информацией на консоли, подсоединенной к маршрутизатору, сконфигурированному на работу с протоколом CDP на своих интерфейсах.

Менеджер сети использует команду show для вывода на экран информации о сетях, которые непосредственно подключены к маршрутизатору. Протокол же CDP обеспечивает информацию о каждом устройстве, которое может работать с ним. Предоставляемая информация включает следующие сведения.

- *Идентификаторы устройства* — например, сконфигурированное имя и имя домена (если есть).
- *Список адресов* — по крайней мере один для протокола SNMP и один адрес для каждого поддерживаемого протокола.
- *Идентификатор порта* — например, Ethernet 0, Ethernet I, Serial 0 и так далее.
- *Перечень функциональных возможностей* — например, если устройство работает не только как маршрутизатор, но и как мост с маршрутизацией от источника.

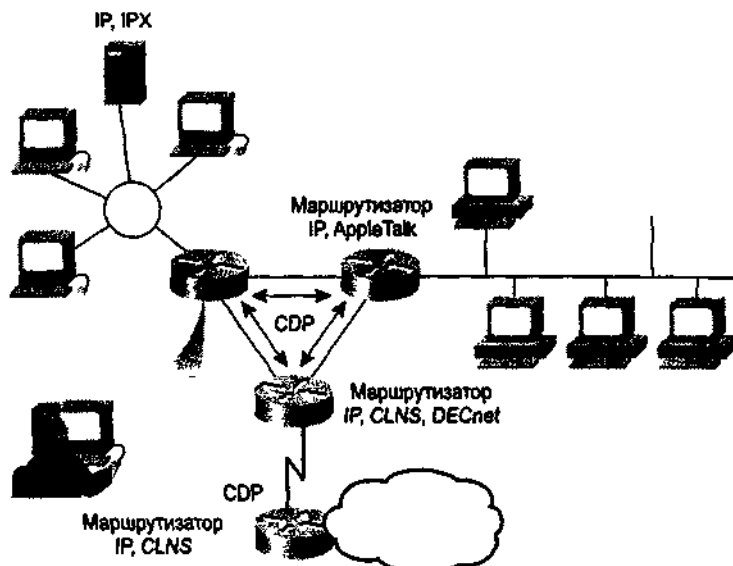


Рис. 13.6. Команда **show cdp neighbors** выводит на экран результаты процесса обнаружения протокола CDP

- *Версия* — информация, аналогичная той, что обеспечивается при выполнении локальной команды **show version**.
- *Платформа* — аппаратная платформа устройства, например Cisco 7000.

Обратите внимание на то, что маршрутизатор, изображенный внизу на рис. 13.6, не является непосредственно подключенным к маршрутизатору с консолью администратора. Для того чтобы получить CDP-информацию об этом устройстве, администратор должен организовать Telnet-сеанс с тем маршрутизатором, который имеет прямое соединение с этим планируемым устройством.

Пример конфигурирования протокола CDP

Протокол CDP начинает функционировать автоматически после запуска системы устройства. Если в изделие компании Cisco загружается ОС IOS версии 10.3 или более поздней, то обычно функция CDP начинает выполняться по умолчанию.

Хотя протокол CDP выполняется по умолчанию, тем не менее, необходимо разрешить его работу на интерфейсе устройства в явном виде, для чего следует применить команду `cdp enable`. Например, на рис. 13.7 показано использование команды `cdp enable` для интерфейсов E0 и S0 маршрутизатора с именем "Маршрутизатор А". Эта команда начинает исполнение функции динамического исследования протокола CDP на интерфейсах устройства. CDP-кадрами обмениваются только непосредственно соединенные соседние устройства. Маршрутизатор кэширует любую информацию, получаемую им от своих CDP-соседей. Если последующий CDP-кадр свидетельствует о том, что какая-либо информация о соседнем устройстве изменилась, то маршрутизатор выбрасывает старые данные и заменяет их новой информацией.

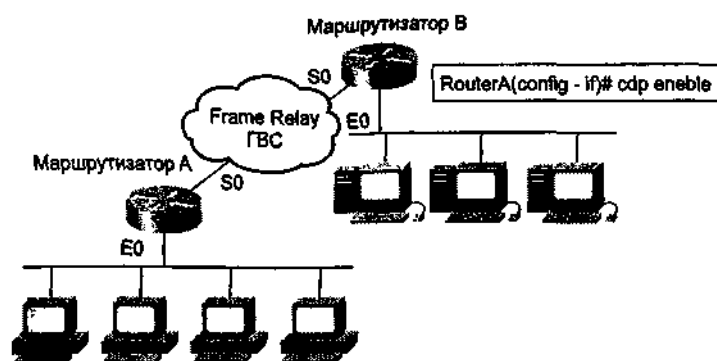


Рис. 13.7. Команда `cdp enable` разрешает выполнение протокола CDP на каждом интерфейсе отдельно

Для вывода информации об установках CDP-таймеров, статусе интерфейсов и методе инкапсуляции, которая используется протоколом CDP при передаче своих кадров процесса исследования и кадров с данными о соседях, применяется команда `show cdp interface` (листинг 13.6). По умолчанию таймеры устанавливают частоту обмена пакетами актуализации CDP-данных и предельный срок хранения CDP-записи. Эти таймеры автоматически устанавливаются на 60 и 180 секунд соответственно. Если устройство принимает пакет раньше или время удержания истекает, то устройство должно отбросить такую запись.

Листинг 13.6. Команда `show cdp interface`

```
routerA# show cdp interface
Serial0 is up, line protocol is up, encapsulation is Frame Relay
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
Ethernet0 is up, line protocol is up, encapsulation is ARPA
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
```

Вывод CDP-записи для конкретного устройства

Для вывода из кэша одной CDP-записи используется команда `show cdp entry имя устройства` (листинг 13.7). Следует отметить, что выводимые этой командой данные включают все адреса уровня 3, которые присутствуют в соседнем маршрутизаторе В; администратор может увидеть IP-адреса интересующего его CDP-соседа (в данном случае это маршрутизатор В), введя единственную команду на маршрутизаторе А.

Листинг 13.7. Команда show cdp entry имя устройства

```
routerA#show cdp entry routerB
-----
Device ID: routerB
Entry address(es):
  IP address: 198.92.68.18
Platform: 2501. Capabilities: Router
Interface: Ethernet0, Port ID (outgoing port): Ethernet0
Holdtime: 155 sec
Version
IOS (tm) GS Software (GS3), 11.2(13337)[asastry 161]
Copyright (c) 1986-1996 by Cisco Systems, Inc.
Compiled Tue 14-May-96 1:04
```

Значение времени удержания (holdtime) показывает, как давно был получен CDP-кадр с этой информацией. Выводимые этой командой данные также включают краткую информацию о версии программного обеспечения, используемого на маршрутизаторе B.

СОР проектировался и реализовывался как очень простой протокол с небольшими накладными расходами. Его кадр может быть маленьким по размеру, но, тем не менее, он предоставляет большое количество полезной информации о соседних маршрутизаторах.

Вывод данных о CDP-соседях

Для вывода содержимого пакетов актуализации протокола CDP, принимаемых локальным маршрутизатором, используется команда show cdp neighbors (листинг 13.8). Следует отметить, что для каждого порта локального маршрутизатора на экран выводится следующая информация.

- Идентификатор соседнего устройства.
- Тип и номер локального порта.
- Значение времени удержания в секундах.
- Код функции соседнего устройства.
- Аппаратная платформа соседнего устройства.
- Тип и номер удаленного порта на соседнем устройстве.

Листинг 13.8. Команда show cdp neighbors

```
RouterA#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge,
                  B - Source Route Bridge,
                  S - Switch, H - Host, I - IGMP
Device ID      Local Interface  Holdtime      Capability  Platform  Port ID
routerB        Eth 0            151           R           2501      Eth 0
routerB        Ser 0            165           R           2501      Ser 0

routerA#show cdp neighbors detail
Device ID: routerB
Entry address(es):
  IP address: 198.92.68.18
Platform: 2501, Capabilities: Router
Interface: Ethernet0, Port ID (outgoing port): Ethernet0
Holdtime: 143 sec
```

Для вывода на экран этой информации вместе информацией, выводимой командой show cdp entry, можно воспользоваться опцией show cdp neighbors detail.

Базовое тестирование взаимодействия в сети

В IP-сетях чаще всего встречаются проблемы, связанные с адресацией. Поэтому очень важно до выполнения дальнейших шагов по конфигурированию проверить конфигурацию адресов. Базовое тестирование сети должно выполняться в последовательности от одного слоя эталонной модели OSI к следующему. Каждая проверка, описываемая в данном разделе, относится к сетевым операциям конкретного уровня модели OSI. Как показано на рис. 13.8, командами, позволяющими протестировать сетевой комплекс, являются telnet, ping, trace, show ip route и show interfaces.

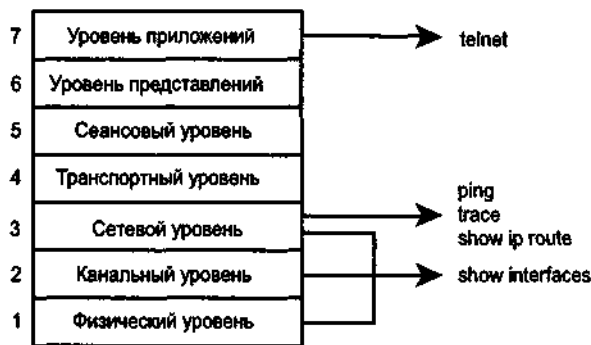


Рис. 13.8. Для проверки конфигурации используются команды telnet, ping и trace

Тестирование уровня приложений с помощью команды telnet

Другой способ получить сведения об удаленном маршрутизаторе — подключиться к нему. Это можно сделать с помощью простого приложения: протокола виртуального терминала Telnet, который входит в состав группы протоколов TCP/IP. С его помощью можно установить соединение между маршрутизатором и подключаемым устройством. Протокол Telnet позволяет верифицировать программное обеспечение уровня приложений, работающее в промежутке между отправляющей и принимающей рабочими станциями. Из имеющихся в наличии это — наиболее полный механизм тестирования. Маршрутизатор способен поддерживать до пяти одновременных входящих сеансов протокола Telnet.

Первоначально тестирование начинается с проверки приложений верхних уровней. Как показано на рис. 13.9, команда telnet обеспечивает возможность работы в режиме виртуального терминала, так что администраторы могут использовать операции протокола Telnet для установления соединений с другими маршрутизаторами, которые исполняют протокол TCP/IP.

Таким образом, на первом этапе проверяется возможность обращений к удаленному маршрутизатору. Например, успешное установление Telnet-соединения от маршрутизатора Йорк к маршрутизатору Париж является базовым тестом сетевого соединения между ними двумя. Если посредством протокола Telnet можно осуществить удаленный доступ к другому маршрутизатору, то тогда по крайней мере известно, что TCP/IP-приложение может связаться с удаленным маршрутизатором. Успешное установление Telnet-соединения свидетельствует о том, что приложение верхнего уровня (и службы более низких уровней) работает соответствующим образом.

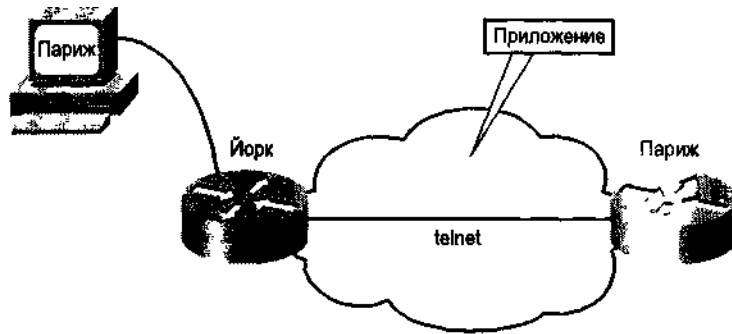


Рис. 13.9. Уровень приложений может тестироваться с помощью команды `telnet`

Если можно установить соединение по протоколу Telnet с одним маршрутизатором, а с другим нельзя, то вполне вероятно, что отказ протокола Telnet вызван конкретными проблемами, связанными с адресацией, присвоением имен или правами доступа. Эти проблемы могут присутствовать на локальном маршрутизаторе или на маршрутизаторе, выбранном в качестве абонента Telnet-сеанса. Тогда следует попробовать воспользоваться командой `ping`, которая позволяет осуществить сквозную проверку сетевого уровня.

Проверка сетевого уровня с помощью команды `ping`

В качестве помощи при диагностике возможности установления связи в сети многие сетевые протоколы поддерживают протокол типа запрос—ответ или протокол эхо-пакетов, который сам по себе является тестом, определяющим наличие или отсутствие маршрутизации пакетов протокола.

Как показано на рис. 13.10, команда `ping` посылает пакет хост-машине в пункте назначения и затем ожидает от нее ответный пакет. Результаты работы такого эхо-протокола могут помочь в оценке надежности пути до хост-машины, величины задержки в пути, а также определить, можно ли связаться с хост-машиной и работает ли она. Для того чтобы команда `ping` работала, необходимо, не только чтобы локальный маршрутизатор знал, как попасть в пункт назначения, но и чтобы маршрутизатор в пункте назначения знал, как добраться до источника.

В листинге 13.9 показано, как адресат команды `ping` 172.16.1.5 успешно отвечает на все пять посланных дейтаграмм. Восклицательный знак (!) означает каждый успешно посланный эхо-пакет. Если вместо этого на экране появляются точки (.), то это говорит о том, что приложение на маршрутизаторе превысило временной предел ожидания эхо-ответа на этот пакет от адресата команды `ping`. Команда пользовательского EXEC-режима `ping` может быть использована для диагностики базовой функции сети по установлению связи. Формальное название пинг-процесса — межсетевой протокол управляющих сообщений (Internet Control Message Protocol, ICMP).

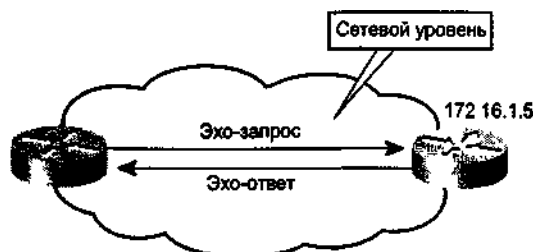


Рис. 13.10. Команда `ping` проверяет возможность установления связи в IP-сети

Листинг 13.9 Команда `ping`

```
Router> ping 172.16.1.5
Type escape sequence to abort.
Sending 5, 100 byte ICMP Echos to 172.16.1.5, timeout is 2 seconds:
```

!!!!!

Success rate is 100 percent, round-trip min/avg/max = 1/3/4 ms

Router>

Проверка сетевого уровня с помощью команды trace

Команда trace является идеальным средством для выяснения того, куда посылаются данные в сети. Эта команда использует ту же технологию, что и команда ping, только вместо проверки сквозной связи между отправителем и получателем она проверяет каждый шаг вдоль пути и позволяет увидеть возможный сквозной путь (рис. 13.11). Эта операция может выполняться либо на пользовательском, либо на привилегированном уровне режима EXEC. Команда trace использует свойство маршрутизаторов генерировать сообщения об ошибке при превышении пакетом своего установленного значения времени жизни (Time To Live, TTL). Эта команда посылает несколько пакетов и выводит на экран данные о времени прохождения туда и обратно для каждого из них. Преимуществом команды trace является то, что она показывает последний достижимый маршрутизатор вдоль пути следования пакетов. Эта функция называется *изоляция отказа*.

В листинге 13.10 показан пример прослеживания пути от Йорка до Рима. По маршруту следования путь должен пройти через Лондон и Париж. Если бы один из этих маршрутизаторов оказался недостижимым, то в листинге вместо имени маршрутизатора появились бы три звездочки (***).

Листинг 13.10. Команда trace

```
York# trace ROME
Type escape to abort.
Tracing the route to Rome (172.16.33.5)
 1 LONDON (172.16.12.3) 1000 msec 8 msec 4 msec
 2 PARIS (172.16.16.2) 8 msec 8 msec 8 msec
 3 ROME (172.16.33.5) 8 msec 8 msec 4 msec
York#
```

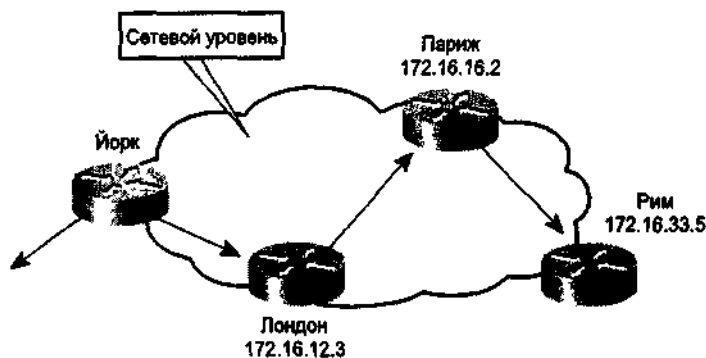


Рис. 13 11. Команда trace показывает адреса интерфейсов, используемые для достижения пункта назначения

Применение команды show ip route для проверки сетевого уровня

Маршрутизатор обладает несколькими мощными средствами, которые позволяют реально увидеть таблицу маршрутизации: направления, используемые маршрутизатором для определения того, как он будет направлять трафик по сети.

Следующий базовый тест также направлен на проверку сетевого уровня. Теперь с помощью команды show ip route проверяется наличие в таблице маршрутизации записи о намеченной сети назначения. В листинге 13.11 показывается, что Рим (131.100.33.0) достижим для

Парижа (131.108.16.2) через интерфейс Ethernet1.

Листинг 13.11. Команда ip route

```
Paris# show ip route
Codes: I - IGRP derived, R - RIP derived, O - OSPF den ved
       C - connected, S - static, E - EGP derived, B - BGP derived
       - IS-IS derived, D - EIGRP derived
       * - candidate default route, IA - OSPF inter area route E1 - OSPF external type
       1 route, E2 - OSPF external type 2 route
       LI - IS-IS level-1 route, L2 - IS-IS level -2 route EX - EIGRP external route
Gateway of last resort is not set
I 144.253.0.0 [100/1300] via 133.3.32.2, 0:00:22 Ethernet1
 131.108.0.0 is subnetted (mask is 255.255.255.0), 3 subnets
I   131.108.33.0 [100/180771] via 131.108.16.2, 0:01:29, Ethernet1
C   131.108.12.0 is directly connected, Ethernet1
C   101.108.16.0 is directly connected, Ethernet0
I 219.100.103.0 [100/1200] via 133.3.32.2, 0:00:22, Ethernet1
```

Проверка физического и канального уровней с помощью команды show interfaces serial

Как показано на рис. 13.12, интерфейс включает два элемента— физический (аппаратная часть) и логический (программная часть).

- Аппаратная часть — кабели, разъемы и интерфейсные модули — должна обеспечивать фактическое соединение двух устройств.
- Программная часть представляет собой сообщения, например сообщения типа "я живой", управляющую информацию и информацию пользователя, которые передаются между соседними устройствами. Эта информация представляет собой данные, которые ходят между двумя соединенными интерфейсами маршрутизаторов.

При проверке физического и канального уровней задаются следующие вопросы.

- Присутствует ли сигнал обнаружения несущей? Хорош ли физический канал связи между устройствами?
- Принимаются ли сообщения типа "я живой"? Могут ли пакеты данных посылаться по физическому каналу?

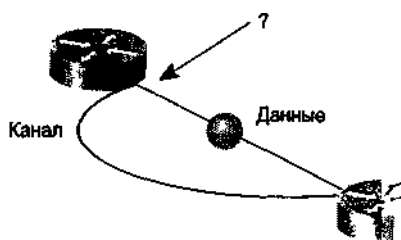


Рис. 13.12 Для проверки физического и канального уровней используется команда `show interfaces serial`

Одним из наиболее важных элементов информации, выводимой командой `show interfaces serial`, являются данные о состоянии канала и канального протокола. На рис. 13.13 показаны ключевая строка выводимого результата и смысловая нагрузка, стоящая за определениями статуса.

В данном примере статус канала определяется по наличию сигнала обнаружения несущей и соотносится с состоянием физического уровня. Однако канальный протокол, статус которого определяется по наличию прохождения кадров с сообщением "я живой", уже соотносится с механизмом формирования кадров на канальном уровне.

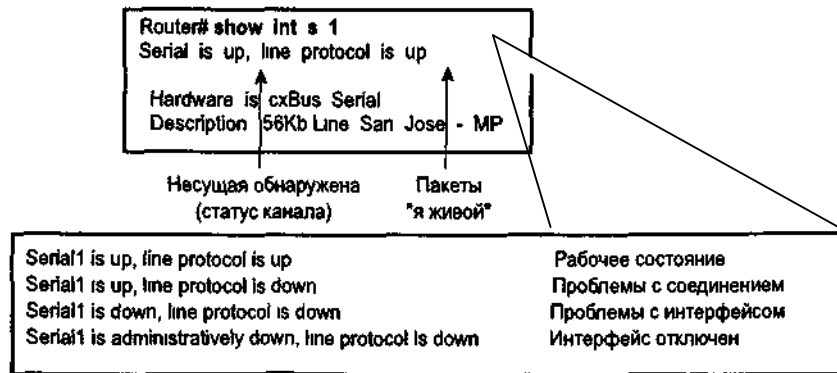


Рис 13.13. Для идентификации проблем в канале или с канальным протоколом используется команда `show interfaces serial`

Сброс показаний счетчиков команды `show interfaces`

Маршрутизатор ведет статистику, которая дает информацию о работе интерфейса. Для вывода на экран статистических данных, отражающих работу маршрутизатора с момента последнего обнуления счетчиков, используется команда `show interfaces` (см. выделенную жирным шрифтом строку листинга 13.12). В этом примере счетчики были обнулены две недели и четыре дня назад. Для сброса показаний счетчиков в нуль используется команда `clear counters`. Начиная счет с нуля, администратор получает ясную картину текущего состояния сети.

Листинг 13.12. Команда `show interfaces`

```

Router# show interfaces serial 1
Serial1 is up, line protocol is up
Hardware is cxBus Serial
Description: 56Kb Line San Jose - MP
Internet address is 150.136.190.20 , subnet mask is 255.255.255.0
MTU 1500 bytes, BW 56 Kbit, DLY 20000 usec, rely 255/255, load 1/255
Encapsulation HDLC, loopback not set, keepalive set (10 sec)
Last input 0:00:07, output 0:00:00, output hang never
Last clearing of show interfaces counters 2w4d
Output queue 0/40, 0 drops; input queue 0/75, 0 drops
Five minute input rate 0 bits/sec, 0 packets/sec
Five minute output rate 0 bits/sec, 0 packets/sec
 1626 packets input, 1347238 bytes, no buffer
 1627 Received 13983 broadcasts, 0 runts, 0 giants
   2 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 2 abort
  0 input packets with dribble condition detected
 2146 packets output, 2383680 bytes, 0 underruns
   0 output errors, 0 collisions, 2 interface resets, 0 restarts
   1 carrier transitions
  
```

Резюме

- Маршрутизатор состоит из конфигурируемых компонентов и имеет режимы для проверки, поддержания и изменения их конфигурации.
- Для проверки используются команды `show`.
- Для показа записей о соседних устройствах используется протокол `COP`.
- Доступ к другим маршрутизаторам возможен с помощью протокола `Telnet`.
- Возможности по установлению связи в сети должны проверяться уровнем за уровнем.
- В команды тестирования входят команды `ping` и `trac`.

Контрольные вопросы

1. Что из приведенного ниже описывает место, из которого конфигурируется маршрутизатор?
 - A. Будучи установленным в сеть, маршрутизатор может конфигурироваться с помощью виртуальных терминалов.
 - B. После выполнения начального конфигурирования маршрутизатор конфигурируется через виртуальные терминалы.
 - C. Будучи установленным в сеть, маршрутизатор может конфигурироваться через модем с консольного терминала.
 - D. После выполнения начального конфигурирования маршрутизатор конфигурируется через модем с использованием порта вспомогательного устройства.
2. Какой из следующих компонентов маршрутизатора имеет такие характеристики: держит операционную систему и микрокод, сохраняет свое содержимое при отключении питания или перезапуске и позволяет обновлять программное обеспечение без замены микросхем?
 - A. Энергонезависимое ОЗУ.
 - B. ОЗУ/ДОЗУ.
 - C. Флэш-память.
 - D. ПЗУ.
3. Что из приведенного ниже неправильно описывает функцию команды статуса маршрутизатора?
 - A. `show version` выводит на экран конфигурацию аппаратной части системы, имена и источники конфигурационных файлов и образы начальной загрузки.
 - B. `show memory` выводит на экран статистические данные о памяти маршрутизатора, включая статистику свободных пулов памяти.
 - C. `show buffers` выводит на экран статистические данные пулов буферов маршрутизатора.
 - D. `show interfaces` выводит на экран статистические данные по всем интерфейсам, сконфигурированным на маршрутизаторе.
4. Какое из приведенных ниже определений описывает функцию команды `show startup-config`?
 - A. Позволяет администратору увидеть текущую рабочую конфигурацию маршрутизатора.
 - B. Выводит сообщение, показывающее объем использованной энергонезависимой памяти.
 - C. Позволяет администратору увидеть причину последней перезагрузки системы.
 - D. Выводит сообщение Current Configuration (Текущая конфигурация).
5. Какие строки информации может выводить на экран команда `show interfaces serial`?
 - A. `IDS (trn) 4500 Software (C4500-J-M), Experimental Version 11.2.`
 - B. `DECNET routing is enabled.`
 - C. `Serial1 is up, line protocol is up.`
 - D. `System image file is "c4500-j-mz".`
6. Для чего используется команда `show cdp neighbors`?
 - A. Для получения моментального снимка маршрутизаторов в сети.
 - B. Для получения обзорной картины маршрутизаторов, непосредственно соединенных с сетью.
 - C. Для получения IP-адресов соседних маршрутизаторов.
 - D. Чтобы построить таблицу маршрутизации во всех маршрутизаторах, находящихся в сети по соседству.
7. Какие четыре важных элемента информации получают после выдачи команду `ping`?
 - A. Размер и количество ICMP-пакетов, продолжительность периода ожидания ответа, показатель успешности отправки эхо-пакетов и минимальное, среднее и максимальное время прохождения пакетов в оба конца.
 - B. Количество ICMP-пакетов, продолжительность периода ожидания ответа, показатель успешности отправки эхо-пакетов и минимальное, среднее и максимальное время прохождения пакетов в оба конца.
 - C. Размер и количество ICMP-пакетов, MAC-адрес, показатель успешности отправки эхо-пакетов и минимальное, среднее и максимальное время прохождения пакетов в оба конца.

- D. Количество ICMP-пакетов, продолжительность периода ожидания ответа, скорость передачи и минимальное, среднее и максимальное время прохождения пакетов в оба конца.
- 8. Какую информацию дает проверка сети с помощью команды trace?
 - A. Определяет, работает ли протокол канала.
 - B. Определяет наличие записи в таблице маршрутизации для намеченного маршрутизатора.
 - C. Показывает каждый маршрутизатор, который проходит пакет на пути к пункту назначения.
 - D. Определяет правильность функционирования приложений верхнего уровня.
- 9. Какую информацию дает проверка сети с помощью команды show interfaces serial?
 - A. Показывает статус канала связи и канального протокола.
 - B. Показывает, как маршрутизатор направляет трафик по сети.
 - C. Показывает путь, по которому следует пакет в сети.
 - D. Выводит на экран имена маршрутизаторов, стоящих в сети.
- 10. Какая команда вводится для того, чтобы просмотреть файл активной конфигурации маршрутизатора?
 - A. show running-config.
 - B. show config term.
 - C. show version.
 - D. show backup-config.

Глава 14

Запуск маршрутизатора и его начальное конфигурирование

В этой главе...

- Последовательность запуска
- Команды запуска
- Диалог конфигурирования системы
- Начальная установка глобальных параметров
- Начальная установка параметров интерфейсов
- Сценарий начальной установки и его использование

Введение

В главе 13, "Вывод информации о конфигурации маршрутизатора", рассказывалось о правильных процедурах и командах доступа к маршрутизатору, проверки и обслуживания его составляющих и для тестирования установления связи в сети. В данной главе рассказывается о том, как запускать маршрутизатор в первый раз, используя правильные команды и последовательность запуска, чтобы выполнить начальное конфигурирование маршрутизатора. Кроме того, будет подробно описана последовательность запуска маршрутизатора и рассказано о диалоге начальной установки, который используется маршрутизатором для создания файла начальной конфигурации.

Процедуры запуска межсетевой операционной системы Cisco (OS IOS)

Процедуры запуска ОС IOS используются для организации начальных операций маршрутизатора. Маршрутизатор должен обеспечивать надежную работу, связывая сети пользователей, на обслуживание которых он был сконфигурирован. Чтобы добиться этого, подпрограммы запуска должны выполнить следующее.

- Проверить, что маршрутизатор включился с полностью оттестированной аппаратной частью.
- Найти и загрузить в память ОС IOS, которую маршрутизатор использует в качестве своей операционной системы.
- Найти и выполнить операторы конфигурирования маршрутизатора, включая конфигурирование функций протоколов и адресов интерфейсов.

Маршрутизатор обеспечивает гарантию включения в работу с проверенной аппаратной частью. При подаче питания на маршрутизатор Cisco он выполняет так называемую автопроверку по включению питания. Во время этой автопроверки маршрутизатор выполняет находящиеся в постоянном запоминающем устройстве (ПЗУ) программы диагностики всех модулей. Эти диагностические программы осуществляют проверку базовых функций процессора, памяти и портов сетевых интерфейсов. После проверки функций аппаратуры маршрутизатор переходит к инициализации программного обеспечения.

Последовательность запуска

После автопроверки по включению питания в процессе инициализации маршрутизатора происходят следующие события, которые проиллюстрированы на рис. 14.1.

1. Из ПЗУ на плате центрального процессора извлекается и выполняется программа универсального начального загрузчика. *Начальная загрузка* представляет собой простую жестко заданную операцию загрузки команд, которые, в свою очередь, приводят к загрузке в память других команд или к переходу в другие режимы конфигурирования.
2. Исходный код операционной системы может располагаться в разных местах. Его местонахождение определяется по содержимому поля Boot регистра конфигурирования. Если поле Boot говорит о загрузке из флэш-памяти или по сети, то команды начальной загрузки системы в конфигурационном файле указывают точное местонахождение соответствующего образа ОС.
3. Загружается образ операционной системы. После этого операционная система определяет состав аппаратной и программной части и выводит получаемый в результате

список на терминал консоли.

4. Записанный в энергонезависимом оперативном запоминающем устройстве (энергонезависимом ОЗУ) конфигурационный файл загружается в главную память и выполняется построчно. Эти команды конфигурирования запускают процесс маршрутизации, вводят адреса интерфейсов, устанавливают характеристики сред передачи данных и т.д.
5. Если в энергонезависимом ОЗУ нет корректно оформленного конфигурационного файла, то операционная система переходит к выполнению работающей в режиме ответов на вопросы программы начального конфигурирования, называемой *диалогом конфигурирования системы*. Этот режим также называется *диалогом начальной установки*.

Команды режима запуска

Режим начальной установки не является режимом для ввода в маршрутизатор сложных функций протоколов. Начальная установка используется для формирования минимальной конфигурации устройства. При решении большинства задач конфигурирования администраторы используют не режим начальной установки, а различные команды специальных режимов конфигурирования.

В листинге 14.1 приведен перечень команд режима запуска для маршрутизаторов, работающих под управлением ОС IOS версии 10.3 или более ранней версии. Две команды в начале листинга 14.1 выводят на экран резервный и активный конфигурационные файлы. Команда `erase startup-config` удаляет резервную копию конфигурационного файла из энергонезависимого ОЗУ. Команда `reload` перезагружает маршрутизатор, заставляя его проходить через весь процесс конфигурирования. Последняя команда используется для входа в режим начальной установки из привилегированного режима EXEC.

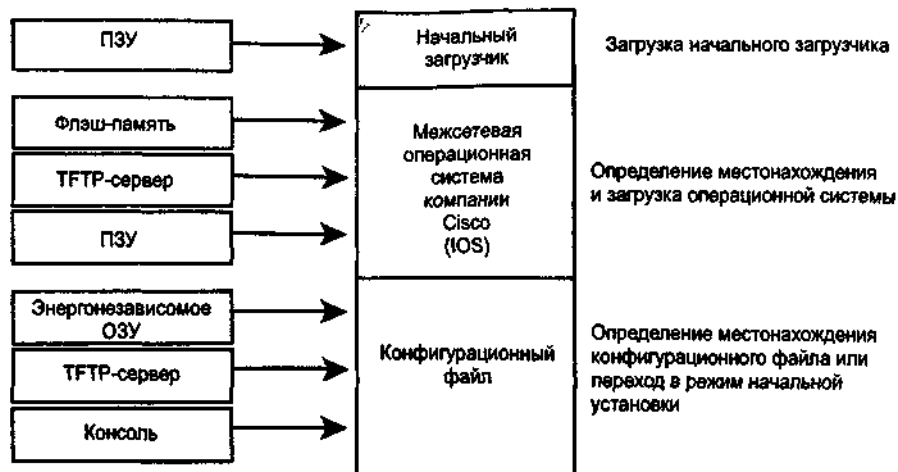


Рис. 14.1. После выполнения автопроверки маршрутизатора по включению питания инициализируется последовательность операций запуска

Листинг 14.1. Команды режима запуска для маршрутизаторов, выполняющих ОС IOS версии 10.3 или более ранней версии

```
Router# show startup-config
      (show config) *
Router# show running-config
      (write term) *
Router# erase startup-eonfig
      (write erase) *
Router# reload
Router# setup
```

Примечание

Используемые в ОС IOS версии 10.3 и более ранних версиях команды `show config`, `write term` и `write erase` заменены новыми командами. В текущей версии эти замененные команды продолжают выполнять свои функции, но в документации уже не упоминаются. В будущей версии поддержка этих команд будет упразднена.

Начальная установка: диалог конфигурирования системы

Одной из подпрограмм начального конфигурирования является подпрограмма режима начальной установки. Главная цель этого режима, показанного в листинге 14.2, состоит в создании минимальной конфигурации для любого маршрутизатора, который не может найти свой конфигурационный файл в каком-либо другом источнике.

Для многих подсказок диалога конфигурирования системы, выполняемого средствами команды `setup`, после вопроса в квадратных скобках ([]) имеются ответы по умолчанию. Нажатие клавиши `<Return>` (или `<Enter>`) позволяет воспользоваться ответом по умолчанию. Если система была предварительно сконфигурирована, то приводимые ответы по умолчанию представляют собой текущие сконфигурированные значения. Если система конфигурируется в первый раз, то приводятся значения по умолчанию, введенные изготовителем. В том случае, когда поставляемые изготовителем значения по умолчанию отсутствуют, как это имеет место при запросе пароля, после знака вопроса (?) на экран не выводится ничего

Листинг 14.2. Режим начальной установки

```
#setup
- System Configuration Dialog -
At any port you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.
Continue with configuration dialog? [yes].
First, would you like to see the current interface summary? [yes]
Interface      IP-Address      OK?  Method  Status  Protocol
TokenRing0     unassigned     NO   not set  down    down
Ethernet0     unassigned     NO   not set  down    down
Serial0       unassigned     NO   not set  down    down
Fddi0         unassigned     NO   not set  down    down
```

В этот момент вводом в командной строке слова по можно прекратить продолжение диалога конфигурирования системы и выйти из него. Чтобы начать процесс первоначального конфигурирования, необходимо ввести ответ `yes`. Для прекращения процесса и завершения процедуры запуска можно в любое время нажать комбинацию клавиш `<Ctrl+C>`. Если в ходе диалога появляется подсказка — `More` —, то для продолжения необходимо нажать клавишу пробела.

Установка глобальных параметров

Как показано в листинге 14.3, в этот момент на экране монитора появляется соответствующая подсказка. Она говорит о том, что маршрутизатор требует от пользователя ввода глобальных параметров, которые тот для него устанавливает. Эти параметры представляют собой конфигурационные значения, решения по которым принимаются пользователем. Первым глобальным параметром, который требуется ввести, является имя маршрутизатора, которое затем будет стоять в начале командной строки всех режимов конфигурирования ОС IOS. При начальном конфигурировании в квадратных скобках указывается имя маршрутизатора по умолчанию `[Router]`. Показанные в листинге 14.3 глобальные параметры используются также

для установки различных паролей, которые затем используются при работе с маршрутизатором.

Листинг 14.3. Подсказка, после которой вводятся глобальные параметры маршрутизатора

```
Configuring global parameters:
```

```
Enter host name [Router]
```

```
The enable secret is a one-way cryptographic secret used instead of the enable password when it exists.
```

```
Enter enable secret[<Use current secret>]
```

```
Enter enable password[san-fran]:
```

```
%Please choose a password that is different from the enable secret
```

```
Enter enable password[san-fran].
```

```
Enter virtual terminal password [san-fran]:
```

```
Configure SNMP Network Management? [no]:
```

Пользователю необходимо ввести так называемый enable secret-пароль. При вводе цепочки символов пароля в строке Enter enable secret символы обрабатываются специальным разработанным компанией Cisco алгоритмом шифрования. Это может увеличить степень защиты паролевой цепочки. Теперь, если кто-либо будет просматривать содержимое конфигурационного файла маршрутизатора, то пароль команды enable (так называемый enable-пароль) воспроизведется в виде бессмысленного набора символов. Режим начальной установки рекомендует, но не требует, чтобы enable-пароль отличался от enable secret-пароля.

Когда на консоли появляется запрос на ввод глобальных параметров, показанный в листинге 14.4, пользователь должен воспользоваться конфигурационными значениями, которые он определил для ввода в маршрутизатор. При положительном ответе на каждый запрос (ответ yes) по каждому протоколу могут появляться дополнительные вопросы.

Листинг 14.4. Запросы на ввод глобальных параметров, которые появляются на консоли

```
Configure IP? [yes]:
```

```
Configure IGRP routing? [yes]:
```

```
Your IGRP autonomous system number [1]: 200
```

```
Configure DECnet? [no]:
```

```
Configure XNS? [no] :
```

```
Configure Novell? [no]: yes
```

```
Configure Apollo? [no] :
```

```
Configure AppleTalk? [no]: yes
```

```
Multizone networks? [no]: yes
```

```
Configure Vines? [no]:
```

```
Configure bridging? [no]:
```

Начальная установка параметров интерфейсов

При появлении показанного в листинге 14.5 запроса на ввод параметров для каждого установленного интерфейса пользователь должен воспользоваться конфигурационными значениями, которые он определил для ввода в маршрутизатор в качестве параметров интерфейсов.

Листинг 14.5. Запросы на ввод параметров для каждого установленного интерфейса

```
Configuring interface parameters:
```

```
Configuring interface TokenRing0:
```

```
Is this interface in use? [yes]:
```

```
Tokenning ring speed (4 or 16)? [16]:
```

```
Configure IP on this interface? [no]: yes
```

```
IP address for this interface: 172.16.92.67
```

```
Number of bits in subnet field [0]:
```

```

Class B network is 172.16.0.0, 0 subnet bit; mask is 255.255.0.0
Configure Novell on this interface? [no]: yes
Novell network number [1]:
Configure interface Serial0:
Is this interface in use? [yes]:
Configure IP on this interface? [yes]
Configure IP unnumbered on this interface? [no]:
IP address for this interface: 172.16.97.67
Number of bits in subnet field [0]:
Class B network is 172.16.0.0, 0 subnet bits; mask is 255.255.0.0
Configure Novell on this interface? [yes]: no
Configuring Interface Serial 1:
Is this interface in use? [yes]: no

```

Сценарий начальной установки и его использование

После завершения конфигурирования всех установленных на маршрутизаторе интерфейсов программа команды режима начальной установки `setup` выводит на экран созданную конфигурацию, внешний вид которой показан в листинге 14.6. Далее программа команды `setup` спрашивает пользователя о том, хочет ли он использовать эту конфигурацию. Если ответ положителен (`yes`), то конфигурация выполняется и сохраняется в энергонезависимой памяти. Если ответ отрицателен (`no`), то конфигурация не сохраняется и процесс начинается снова. Для этого запроса нет ответа по умолчанию; пользователь должен ответить либо "да" (`yes`), либо "нет" (`no`). После положительного ответа на этот последний вопрос система готова к использованию. Если существует необходимость в модификации только что созданной конфигурации, это необходимо сделать вручную.

Листинг 14.6. Выводимая программой команды `setup` созданная конфигурация

```

The following configuration command script was created:
hostname router
enable secret 5 $ !Sg772S
enable password san-fran
enable password san-fran
line vty 0 4
password san-fran
snmp-server community
!
ip routing
no decnet routing
no xns routing
no apollo routing
appletalk routing
no cins routing
no vines
no bridge
no mop enabled
Interface Ethernet
Ip address 172.16.92.67 255.255.0.0
network 1
no mop enabled
!
interface Serial0
Ip address 172.16.97.67 255.255.0.0
Interface Serial1
shutdown
!
end
Use this configuration? [yes/no]: yes
[OK]
Use the enabled mode 'configure' command to modify this configuration.

```

Данный сценарий говорит, что для внесения изменений в конфигурационный файл после использования режима начальной установки следует использовать режим конфигурирования. Генерируемый командой setup файл сценария является аддитивным. С помощью этой команды можно активизировать функции, но отключить их нельзя. Также команда setup не поддерживает многие из новейших функций маршрутизатора и функции, которые требуют более сложного конфигурирования.

Резюме

Маршрутизатор инициализируется путем загрузки программы начальной загрузки, операционной системы и конфигурационного файла.

Если маршрутизатор не может найти конфигурационный файл, он входит в режим начальной установки.

Маршрутизатор сохраняет резервную копию созданной в режиме начальной установки новой конфигурации в энергонезависимой памяти.

Контрольные вопросы

1. Какая из приведенных ниже последовательностей шагов выполнения процесса запуска системы маршрутизаторов Cisco является правильной?
 - A. (1) Нахождение местоположения операционной системы и ее загрузка; (2) загрузка программы начального загрузчика; (3) тестирование аппаратной части; (4) нахождение местоположения конфигурационного файла и ее загрузка.
 - B. (1) Тестирование аппаратной части; (2) загрузка программы начального загрузчика; (3) нахождение местоположения операционной системы и ее загрузка; (4) нахождение местоположения конфигурационного файла и его загрузка.
 - C. (1) Загрузка программы начального загрузчика; (2) нахождение местоположения конфигурационного файла и его загрузка; (3) тестирование аппаратной части; (4) нахождение местоположения операционной системы и его загрузка.
 - D. (1) Тестирование аппаратной части; (2) загрузка программы начального загрузчика; (3) нахождение местоположения конфигурационного файла и ее загрузка; (4) нахождение местоположения операционной системы и ее загрузка.
2. Что из приведенного ниже является важной функцией автопроверки по включению питания?
 - A. Определение состава аппаратных и программных компонентов маршрутизатора и вывод этого перечня на терминал консоли.
 - B. Загрузка в память других команд.
 - C. Выполнение подпрограмм диагностики, которые проверяют принципиальную работоспособность аппаратной части маршрутизатора.
 - D. Запуск процесса маршрутизации, ввод адресов интерфейсов и установка характеристик сред передачи данных.
3. Что из приведенного ниже является важным результатом ввода в маршрутизатор ОС IOS?
 - A. Определение состава аппаратных и программных компонентов маршрутизатора и вывод этого перечня на терминал консоли.
 - B. Загрузка в память других команд.
 - C. Выполнение подпрограмм диагностики, которые проверяют принципиальную работоспособность аппаратной части маршрутизатора.
 - D. Запуск процесса маршрутизации, ввод адресов интерфейсов и установка характеристик сред передачи данных.
4. Что из приведенного ниже является важным результатом загрузки в маршрутизатор конфигурационного файла?
 - A. Определение состава аппаратных и программных компонентов маршрутизатора и вывод этого перечня на терминал консоли.
 - B. Загрузка в память других команд.
 - C. Выполнение подпрограмм диагностики, которые проверяют принципиальную работоспособность аппаратной части маршрутизатора.
 - D. Запуск процесса маршрутизации, ввод адресов интерфейсов и установка характеристик сред передачи данных.
5. Какова функция команды `erase startup-config`?
 - A. Удаляет из энергонезависимой памяти резервный конфигурационный файл.
 - B. Удаляет из флэш-памяти образ начального загрузчика.
 - C. Удаляет из энергонезависимой памяти рабочий образ ОС IOS.
 - D. Удаляет из флэш-памяти текущую рабочую конфигурацию.
6. Какова функция команды `reload`?
 - A. Загружает с TFTP-сервера резервную копию конфигурационного файла.
 - B. Сохраняет во флэш-памяти новый образ ОС IOS.
 - C. Перезагружает маршрутизатор.
 - D. Загружает в энергонезависимую память новый конфигурационный файл.

7. Когда выполняется режим начальной установки маршрутизатора?
- A. После того, как сохраненный конфигурационный файл загружается в главную память.
 - B. Когда сетевому администратору необходимо ввести в маршрутизатор конфигурацию сложной функции протокола.
 - C. Когда маршрутизатор начинает инициализацию программного обеспечения.
 - D. Когда маршрутизатор не может найти корректно оформленный конфигурационный файл.
8. Что из приведенного ниже правильно описывает процедуру начальной установки на маршрутизаторе глобальных параметров и параметров интерфейсов?
- A. Значения параметров по умолчанию указываются в строке каждого запроса в квадратных скобках.
 - B. Должно быть установлено имя маршрутизатора.
 - C. Можно, но этого жестко не требуется, установить `enable secret`-пароль.
 - D. Для каждого установленного интерфейса необходимо предоставить ответы на ряд вопросов.
9. Зачем может понадобиться выдача команд `show startup-config` и `show running-config`?
- A. Настало время обновления ОС IOS, и перед началом в маршрутизаторе необходимо удалить определенные процессы.
 - B. Для определения времени с момента загрузки маршрутизатора и текущих установок регистра.
 - C. Маршрутизатор неожиданно начал неправильно работать, и необходимо сравнить начальное состояние с состоянием на данный момент времени.
 - D. Для выяснения, откуда была загружена ОС IOS и какая версия используется.
10. Какой (какие) файл (файлы) можно обнаружить в энергонезависимой памяти?
- A. ОС IOS и конфигурационные файлы.
 - B. Конфигурационные файлы.
 - C. Резервную копию ОС IOS.
 - D. Ограниченную версию ОС IOS и файлы реестра.

Глава 15

Конфигурирование маршрутизатора

В этой главе...

- Процедуры задания местонахождения конфигурационных файлов и генерация информации для конфигурирования маршрутизатора
- Цели и функции режимов работы маршрутизатора
- Пользовательский режим EXEC
- Привилегированный режим EXEC
- Режим глобального конфигурирования
- Конфигурирование паролей
- Идентификация маршрутизатора

Введение

В главе 14, "Запуск маршрутизатора и его начальное конфигурирование", рассказывалось о том, как запустить маршрутизатор в первый раз, используя правильные команды и последовательность запуска, чтобы выполнить его начальное конфигурирование. В данной главе речь пойдет о применении режимов работы маршрутизатора и методов конфигурирования для обновления конфигурационного файла в маршрутизаторах, работающих под управлением межсетевой операционной системы компании Cisco Internetwork Operating System (OS IOS) текущей и более ранних версий.

Конфигурированию маршрутизатора

При запуске маршрутизатор использует следующую информацию, содержащуюся в конфигурационном файле.

- Версия ОС IOS.
- Идентификационные данные маршрутизатора.
- Местонахождение файла начального загрузчика.
- Информация о протоколах,
- Конфигурация интерфейсов

Конфигурационный файл содержит команды, которые индивидуализируют работу маршрутизатора. Как уже говорилось в главе 14, "Запуск маршрутизатора и его начальное конфигурирование", если конфигурационный файл отсутствует, то тогда диалог конфигурирования системы режима начальной установки помогает пользователю в процессе его создания.

Работа с конфигурационными файлами маршрутизаторов, работающих под управлением ОС IOS версии 11.0 или более поздней.

Информация о конфигурации маршрутизатора может генерироваться несколькими способами. Команда привилегированного режима EXEC `configure` может использоваться для конфигурирования с использованием либо виртуального (удаленного) терминала, либо терминала консоли, позволяя вводить изменения в конфигурацию в произвольный момент времени. Эта команда также может использоваться для загрузки конфигурации из сетевого сервера простейшего протокола передачи файлов Trivial File Transfer Protocol (TFTP-сервера), позволяя поддерживать и хранить информацию о конфигурации на центральной площадке.

На рис. 15.1 представлен сводный перечень команд конфигурирования, который включает команды, приведенные в табл. 15.1.

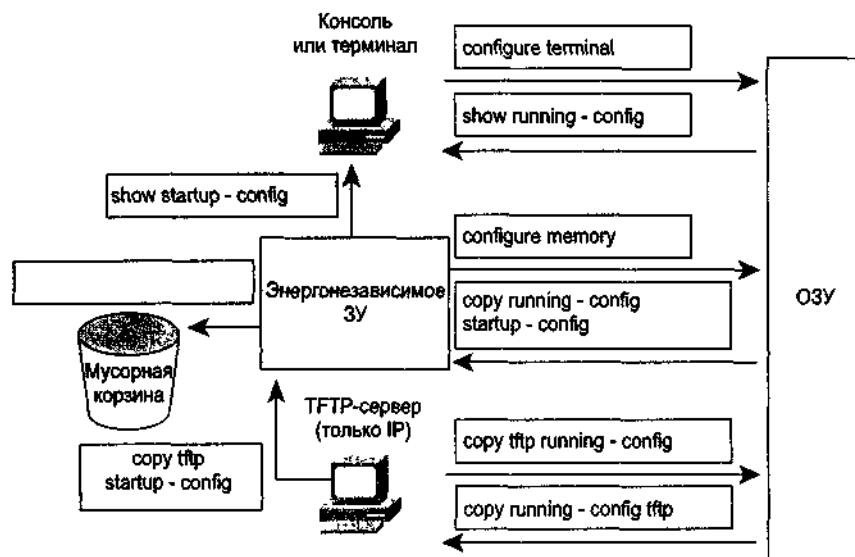


Рис. 15.1. Команды, используемые в маршрутизаторах, работающих под управлением ОС IOS версий 11.0 или более поздних версий

Таблица 15.1. Сводный перечень команд конфигурирования для маршрутизаторов, работающих под управлением ОС IOS версии 11.0 или более поздних версий

Команда	Описание
configure terminal	Конфигурирует маршрутизатор вручную с терминала консоли
configure memory	Загружает информацию о конфигурации из энергонезависимой памяти
copy tftp running-config	Загружает информацию о конфигурации с сетевого TFTP-сервера
show running-config	Выводит на экран текущую конфигурацию, находящуюся в ОЗУ
copy running-config startup-config	Сохраняет текущую находящуюся в ОЗУ конфигурацию в энергонезависимой памяти
copy running-config tftp	Сохраняет текущую находящуюся в ОЗУ конфигурацию на сетевом TFTP-сервере
show startup-config	Выводит на экран сохраненную конфигурацию, которая содержится в энергонезависимой памяти
erase startup-config	Стирает содержимое энергонезависимой памяти

Работа с конфигурационными файлами маршрутизаторов, работающих под управлением ОС IOS версий, предшествовавших версии 11.0

Команды, показанные на рис. 15.2, используются в маршрутизаторах, работающих под управлением ОС IOS версии 10.3 или более ранних версий, и уже заменены новыми командами, которые продолжают выполнять свою нормальную функцию в текущей версии ОС, но в документации больше не приводятся. В будущем релизе поддержка этих команд будет упразднена.

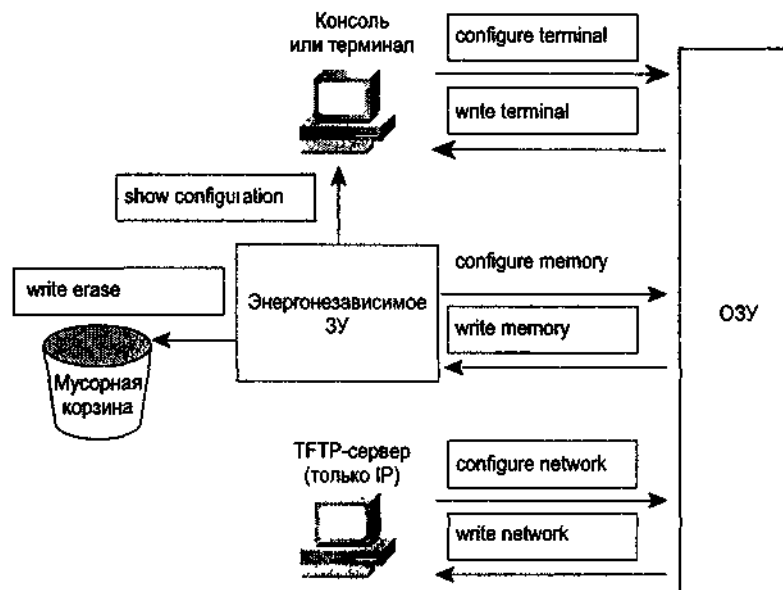


Рис. 15.2. Команды, используемые в маршрутизаторах, работающих под управлением ОС IOS версии 10.3 или более ранних версий

Использование TFTP-сервера

Текущая копия конфигурации может храниться на TFTP-сервере. Как показано в листинге 15.1, чтобы сохранить текущую находящуюся в ОЗУ конфигурацию маршрутизатора на сетевом TFTP-сервере, используется команда `copy running-config tftp`. Для этого выполните следующие действия.

1. Введите команду `copy running-config tftp`.
2. Введите IP-адрес хост-машины, на которой будет храниться конфигурационный файл.
3. Введите имя, которое пользователь хотел бы присвоить конфигурационному файлу.
4. Подтвердите выбор вводом ответа `yes` ("да").

ЛИСТИНГ 15.1. Команда `copy running-config tftp`

```
Tokyo# copy running-config tftp
Remote host  []? 131.108.2.155
Name of configuration file to write  [tokyo-config]?  tokyo.2
Write file tokyo.2 to 131.108.2.155?  [confirm]  y
Writing tokyo.2  !!!!!!!  [OK]
Tokyo#
```

Маршрутизатор может конфигурироваться путем загрузки конфигурационного файла хранящегося на одном из сетевых серверов. Для этого выполните следующие действия.

1. Введите команду `copy tftp running-config`, чтобы перейти в соответствующий режим конфигурирования (листинг 15.2).
2. В строке подсказки системы выберите относительный тип конфигурационного файла: сетевой или хост-файл. Сетевой конфигурационный файл содержит команды, которые применяются в отношении всех маршрутизаторов и серверов терминалов, находящихся в сети. Конфигурационный хост-файл содержит команды, которые применяются в отношении одного конкретного маршрутизатора.
3. В строке подсказки системы введите вариант IP-адреса удаленной хост-машины, из которой будет извлекаться конфигурационный файл. В пример ниже маршрутизатор конфигурируется из TFTP-сервера с IP-адресом 131.108.2.155. В следующей строке

подсказки системы введите имя конфигурационного файла или воспользуйтесь именем, заданным по умолчанию Система именования файлов аналогична используемой в UNIX-подобных операционных системах. По умолчанию для конфигурационного хост-файла принято имя *имя_узла-сети-config*, а для сетевого — *имя_сети-config*. В среде DOS имена файлов на сервере ограничены восемью символами в длину и тремя символами для расширения (например, *router.cfg*). Далее подтверждаются предоставленные системой имя файла и адрес сервера. В листинге 15.2 необходимо отметить, что вид командной строки маршрутизатора меняется на *tokyo* немедленно. Это свидетельствует о том, что реконфигурирование происходит сразу же после загрузки нового файла.

Листинг 15.2. Команда `copy tftp running-config`

```
Router# copy tftp running-config
Host or network configuration file [host]?
IP address of remote hose [255.255.255.255]? 131.108.2.155
Name of configuration file [Router-config]? tokyo.2
Configure using tokyo.2 from 131.108.2.155? [confirm] y
Booting tokyo.2 from 131.108.2.155:!! [OK-874/16000 bytes]
tokyo.2
```

Использование энергонезависимой памяти в маршрутизаторах, работающих под управлением ОС IOS версии 10.3

Команды, показанные в листинге 15.3, управляют содержимым энергонезависимой памяти (табл. 15.2).

Листинг 15.3. Команды работы с энергонезависимой памятью, используемые в маршрутизаторах с ОС IOS версии 10.3 или более ранних версий

```
Router# configure memory
[OK]
Router#

Router# write erase
[OK]
Router#

Router# write memory
[OK]
Router#

Router# show configuration
Using 5057 out of 32768 bytes
!
enable-password san-fran
!
interface Ethernet 0
ip address 131.108.100.5 255.255.255.0
!
-- More --
```

Таблица 15.2. Команды для управления содержимым энергонезависимой памяти в маршрутизаторах с ОС IOS версии 11.x

Команда	Описание
---------	----------

configure memory	Загружает информацию о конфигурации из энергонезависимой памяти
erase startup-config	Стирает содержимое энергонезависимой памяти
copy running-config startup-config	Сохраняет текущую находящуюся в ОЗУ (те, исполняемую) конфигурацию в энергонезависимой памяти (как конфигурацию запуска)
show startup-config	Выводит на экран сохраненную конфигурацию, которая содержится в энергонезависимой памяти

Использование энергонезависимой памяти в маршрутизаторах, работающих под управлением ОС IOS версии 11.0

Команды, показанные в листинге 15.3, используются в маршрутизаторах, работающих под управлением ОС IOS версии 10.3 или более ранних версий. Они уже заменены новыми командами (листинг 15.4), которые в текущей версии продолжают выполнять свои нормальные функции, но в документации больше не упоминаются. Поддержка этих команд в будущей версии будет упразднена.

Листинг 15.4. Команды ОС IOS версии 11.x, которые управляют содержимым энергонезависимой памяти

```
Router# configure memory
[OK]
Router#

Router# erase startup-config
[OK]
Router#

Router# copy running-config startup-config
[OK]
Router#

Router# show startup-config
Using 5057 out of 32768 bytes
!
enable-password san-fran
!
interface Ethernet 0
ip address 131.108.100.5 255.255.255.0
!
- More -
```

Краткие сведения о режимах маршрутизатора

Маршрутизатор в режиме EXEC интерпретирует вводимые с клавиатуры команды и выполняет соответствующие операции. Перед тем как пользователь сможет вводить команды режима EXEC, он должен зарегистрироваться в системе. Существуют два режима EXEC; команды режима EXEC, доступные в пользовательском режиме, представляют собой подмножество команд, доступных в привилегированном режиме. Находясь на привилегированном уровне, пользователь также может иметь доступ к режиму глобального конфигурирования и специальным режимам конфигурирования (некоторые из них показаны на рис. 15.3 и перечислены в табл. 15.3).

- Пользовательский режим EXEC
- Привилегированный режим EXEC
- Режим глобального конфигурирования
- Специальные режимы конфигурирования

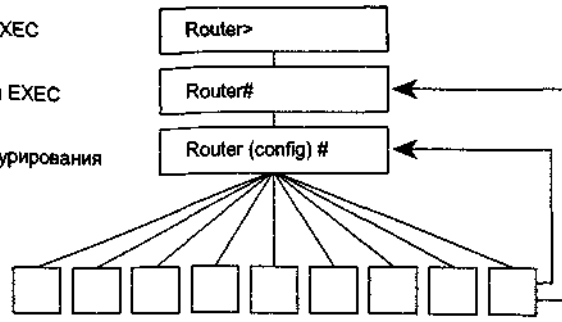


Рис 15.3. Режимы работы маршрутизатора, используемые при его конфигурировании

Таблица 15.3. Режимы конфигурирования и виды командной строки

Режим конфигурирования	Вид командной строки
Интерфейса	Router (config-if) #
Подынтерфейса	Router (config-subif) #
Контроллера	Router (config-controller) #
Карты виртуальных каналов	Router (config-map-list) #
Карты классов	Router (config-map-class) #
Канала	Router (config-line) #
Маршрутизатора	Router (config-router) #
IPX-маршрутизатора	Router (config-ipx-router) #
Карты маршрутов	Router (config-route-map) #

Если с клавиатуры вводится слово **exit** ("выход"), то маршрутизатор переходит на один уровень назад, что в конечном итоге позволяет полностью выйти из системы. В общем случае ввод слова **exit** в одном из специальных режимов конфигурирования возвращает пользователя в режим глобального конфигурирования. Нажатие клавиш <Ctrl+Z> приводит к полному выходу из режима конфигурирования и возвращает маршрутизатор в привилегированный режим EXEC.

Режимы конфигурирования

Команды режима глобального конфигурирования действуют в отношении характеристик, которые определяют поведение системы в целом. Они используются для общесистемного конфигурирования, требующего однострочных команд. Кроме того, команды режима глобального конфигурирования включают команды перехода в другие режимы конфигурирования, которые используются для создания конфигураций, требующих многострочных команд. Для входа в режим глобального конфигурирования, как показано в листинге 15.5, используется команда привилегированного режима EXEC `configure`. При вводе этой команды режим EXEC запрашивает источник команд конфигурирования.

Листинг 15.5 Команда привилегированного режима EXEC `configure`

```
Router# configure terminal
Router(config)# (commands)
Router(config)# exit
Router#

Router# configure terminal
Router(config)# router protocol
Router(config-router)# (commands)
Router(config-router)# exit
Router(config)# interface type port
Router(config-if)# (commands)
```



```
Router(config-if)# exit
Router(config)# exit
Router#
```

В качестве источника пользователь может задать терминал, энергонезависимую память или файл, хранящийся на сетевом сервере. По умолчанию команды вводятся с терминала консоли. Нажатие в этот момент клавиши <Return> начинает этот метод конфигурирования. Команды для активизации конкретного типа маршрутизации или конкретной функции интерфейса начинаются с команд глобального конфигурирования.

Для конфигурирования протокола маршрутизации, на возможность выполнения которого будет указывать появление командной строки вида Router (config-router); (листинг 15 6), сначала вводится глобальная команда типа протокола маршрутизатора.

Листинг 15.6. Конфигурирование протокола маршрутизации

```
Router# configure terminal
Router(config)# router protocol
Router(config-router)# (commands)
Router(config-router)#
```

Для конфигурирования интерфейса, на возможность выполнения которого будет указывать появление командной строки вида Router (config-if) # (листинг 15 7)| сначала вводится глобальная команда типа интерфейса и его номера.

Листинг 15.7. Конфигурирование интерфейса

```
Roter# configure terminal
Router(config)# interface type port
Router(config-if)# (commands)
Router(config-if)# exit
```

Ввод команд в любом из этих режимов следует заканчивать вводом команды **exit**.

Режим протокола IP-маршрутизации

Как показано в листинге 15.8, после активизации глобальной командой протокола маршрутизации на экране появляется командная строка режима конфигурирования маршрутизатора Router (config-router) # Для получения перечня команд конфигурирования маршрутизатора можно ввести знак вопроса (?)

Листинг 15.8. Командная строка режима конфигурирования маршрутизатора после активизации протокола маршрутизации

```
Router(config)# router?
bgp      Border Gateway Protocol (BGP)
egp      Exterior Gateway Protocol (EGP)
eigrp    Enhanced Interior Gateway Routing Protocol (EIGRP)
igrp     Interior Gateway Routing Protocol (IGRP)
isis     ISO IS-IS
iso-igrp IGRP for OSI networks
mobile   Mobile routes
odr      On Demand stub Routes
ospf     Open Shortest Path First (OSPF)
rip      Routing Information Protocol (RIP)
static   Static routes

Router(config)# router rip
Router(config-router) # ?
Router configuration commands
default-information  Control distribution of default information
```

```
default-metric      Set metric of redistributed routes
distance           Define an administrative distance
distribute-list     Filter networks in routing updates
exit               Exit from routing protocol configuration mode
- More -
```

Режим конфигурирования интерфейса

Так как все интерфейсы маршрутизатора автоматически находятся в режиме административного отключения, то многие их функции активизируются на поинтерфейсной основе. Команды конфигурирования интерфейса модифицируют работу портов Ethernet, Token Ring или последовательного порта. Кроме того, интерфейсные субкоманды всегда следуют за командой `interface`, поскольку она определяет тип интерфейса.

В приведенной ниже команде аргумент *type* включает значения **serial**, **ethernet**, **token ring** и др.

```
Router(config)# interface type port
Router(config)# interface type slot/port
```

Для административного отключения интерфейса используется команда

```
Router(config-if)# shutdown
```

Для включения интерфейса, который был отключен, используется команда

```
Router (config-if)# no shutdown
```

Показанная ниже команда используется для выхода из текущего активного режима конфигурирования интерфейса

```
Router(config-if)# exit
```

Примеры конфигурирования интерфейса

С интерфейсами связаны следующие команды:

```
Router(config)# interface serial 1/0
Router(config-if)# bandwidth 56
Router(config-if)# clockrate 56000
```

В каналах последовательной передачи данных одна сторона должна обеспечивать выдачу тактовых сигналов. Такую выдачу обеспечивает аппаратура передачи данных (data communication equipment, DCE), например блок службы канала/блок службы данных (channel service unit/data service unit, CSU/DSU). На другой стороне канала находится оконечное оборудование данных (data terminal equipment, DTE). По умолчанию маршрутизаторы Cisco являются DTE-устройствами, но в некоторых случаях они могут использоваться и в качестве DCE-устройств.

Если интерфейс используется для обеспечения тактирования, то тогда с помощью команды `clockrate` необходимо задать частоту тактовых импульсов. Команда `bandwidth` изменяет значение полосы пропускания по умолчанию, которое выводится на экран командой `show interface` и используется некоторыми протоколами маршрутизации, например протоколом внутренней маршрутизации между шлюзами Interior Gateway Routing Protocol (IGRP).

Для конфигурирования первичного интерфейса используются следующие команды:

```
Router(config)# interface serial 0
```

```
Router(config-if)# int & 0.1 point-to-point  
Router(config-if)# int & 0.2 point-to-point
```

В маршрутизаторах серии Cisco 4000 используются следующие команды:

```
Router(config)# interface ethernet 2  
Router(config-if)# media-type 10baseT
```

В маршрутизаторе Cisco 4000 на внешней стороне корпуса находятся два разъема для подключения к интерфейсу Ethernet: разъем интерфейса подключения вспомогательного устройства (attachment unit interface, AUI) и IOBaseT-разъем. По умолчанию используется разъем AUI, так что если пользователь хочет использовать другой тип подключения, то ему необходимо задать тип среды передачи данных (media-type) IOBaseT.

Методы конфигурирования

В данном разделе будет рассказано о командах, связанных с методами конфигурирования ОС IOS компании Cisco.

- Конфигурирование версии 11.x.
- Конфигурирование версии, предшествующей версии 11.0.
- Конфигурирование паролей.
- Конфигурирование идентификационных данных.
- Методы конфигурирования версии 11.x.

Команды, показанные на рис. 15.4, используются при работе с ОС IOS версии 11.0 и более поздней версии. На рис. 15.4 показаны способы для

- ввода операторов конфигурирования;
- сохранения изменений в резервной копии, которая будет использоваться маршрутизатором в момент запуска;
- проверки сделанных изменений;
- модификации или удаления операторов конфигурирования в случае возникновения такой необходимости.

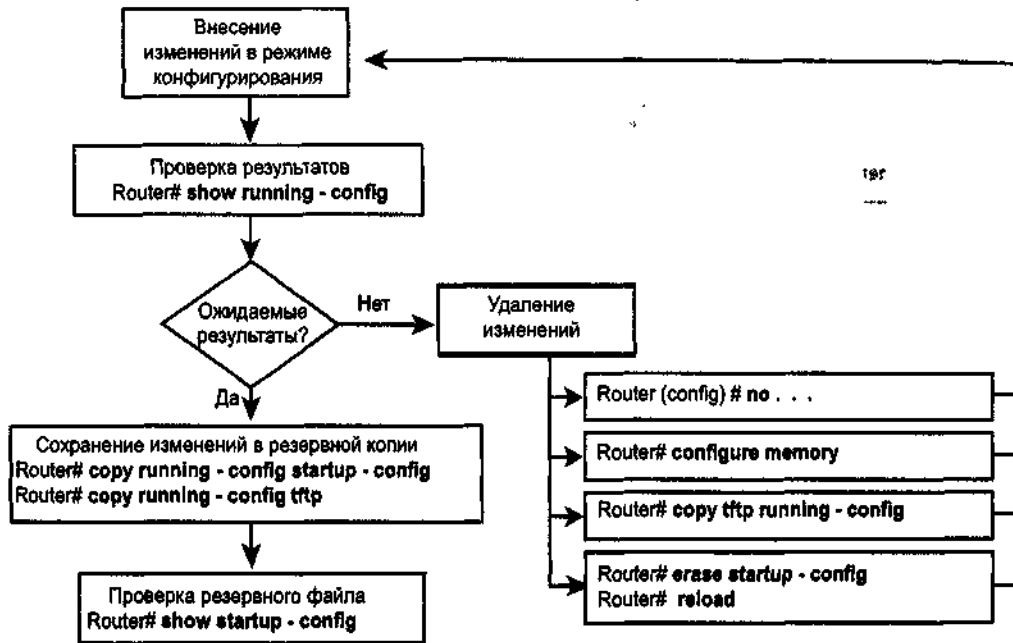


Рис. 15.4. Команды конфигурирования, используемые при реализации методов конфигурирования ОС IOS версии 11.x

Конфигурирование версии, предшествующей версии 11.0

Показанные на рис. 15.5 команды используются с ОС IOS версии 10.3 и более ранней версии. Они заменены новыми командами, которые в текущей версии продолжают выполнять свои функции, но в документации больше не приводятся. В будущей версии поддержка этих команд будет упразднена.

Конфигурирование паролей

Ограничивая доступ к системе за счет использования паролей, можно сделать систему более защищенной. Пароли могут устанавливаться как на отдельные каналы, так и на вход в привилегированный режим EXEC.

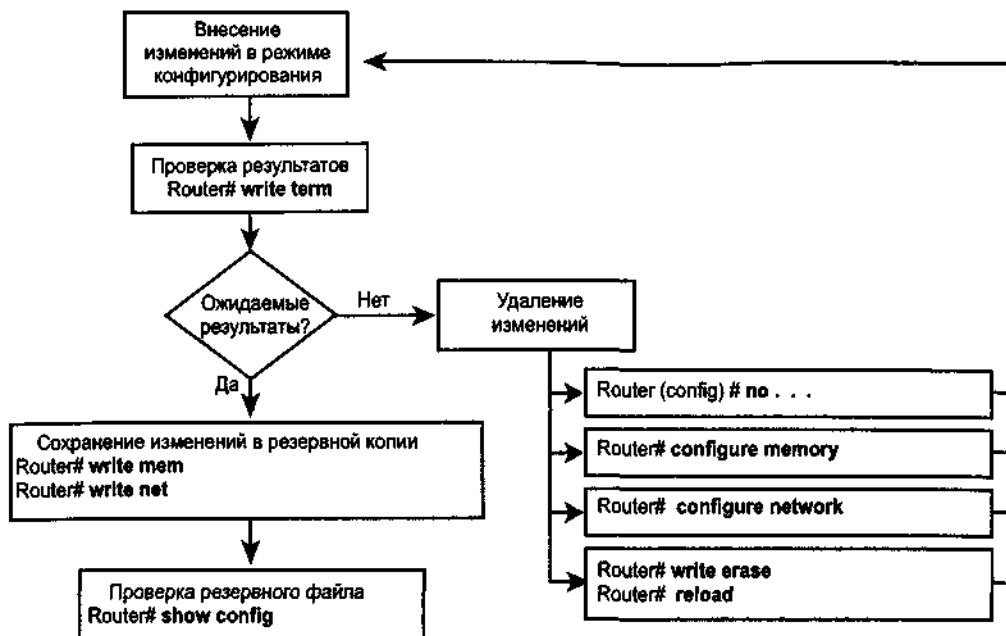


Рис. 15.5. Команды, используемые в маршрутизаторах, работающих под управлением ОС IOS версии 10.3 и более ранней версии

Команда line console 0 устанавливает пароль на терминал консоли:

```
Router(config)# line console 0
Router(config-line)# login
Router(config-line)# password Cisco
```

Команда line vty 0 4 устанавливает паролевую защиту на входящие сеансы протокола Telnet:

```
Router(config)# line vty 0 4
Router(config-line)# login
Router(config-line)# password cisco
```

Команда **enable password** ограничивает доступ к привилегированному режиму EXEC:

```
Router(config)# enable password san-fran
```

Пароль, указываемый после команды **enable secret** в диалоге конфигурирования системы по установке глобальных параметров, использует для видоизменения паролевой цепочки символов специальный процесс шифрования, разработанный компанией Cisco. Дополнительная защита паролей от вывода на экран в открытом виде может быть достигнута с помощью команды **service password-encryption**. Однако используемый здесь алгоритм шифрования не удовлетворяет требованиям стандарта шифрования данных Data Encryption Standard (DES):

```
Router(config)# service password-encryption
(команды конфигурирования паролей)
Router(config)# no service password-encryption
```

Конфигурирование идентификационных данных

Конфигурация сетевых устройств определяет поведение сети. Для управления конфигурациями устройств необходимо вести список и сравнивать конфигурационные файлы работающих устройств, хранить конфигурационные файлы на сетевых серверах для коллективного доступа, устанавливать и обновлять версии программного обеспечения.

Одной из первых базовых задач является присвоение маршрутизатору имени. Имя маршрутизатора будет считаться именем хост-машины и являться тем именем, которое выводится в системной командной строке. Если имя не сконфигурировано, то в системе имя маршрутизатора по умолчанию — Router. Можно присваивать имя в режиме глобального конфигурирования. В примере, показанном на рис. 15.6, маршрутизатору присваивается имя Токуо.

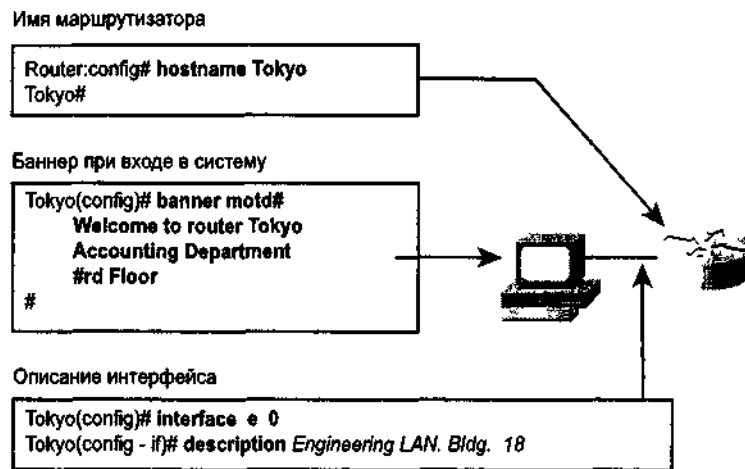


Рис. 15.6. Идентификационные данные маршрутизатора могут задаваться в режиме глобального конфигурирования

Возможно конфигурирование баннера с сообщением дня, который будет выводиться на всех подключенных терминалах. Этот баннер выводится при регистрации в системе и полезен для передачи сообщений, касающихся всех пользователей сети, например сообщений о приближающемся гашении системы. Для конфигурирования подобного сообщения в режиме глобального конфигурирования применяется команда `banner motd`.

Резюме

- В момент запуска маршрутизатор использует информацию из файла конфигурации.
- Конфигурационные файлы могут вводиться с консоли, из энергонезависимой памяти или с TFTP-сервера.
- Команды, используемые с ОС IOS версии 10.3 и более ранних версий, уже заменены новыми командами.
- В режиме EXEC интерпретируются вводимые команды и выполняются соответствующие операции.
- Маршрутизатор имеет несколько режимов работы.
- Привилегированный режим, который используется для копирования и управления содержанием конфигурационных файлов в целом.
- Режим глобального конфигурирования, который используется для однострочных команд и команд, изменяющих настройки всего маршрутизатора.
- Другие конфигурационные режимы, используемые для многострочных команд и выполнения детального конфигурирования.
- Возможна защита системы за счет ограничения доступа путем применения паролей. Конфигурация сетевых устройств определяет поведение сети.

Контрольные вопросы

1. Что из приведенного ниже *не* является функцией команды привилегированного режима EXEC configure?
 - A. Конфигурирование маршрутизатора с виртуального терминала.
 - B. Конфигурирование TFTP-сервера с виртуального терминала.
 - C. Конфигурирование маршрутизатора с терминала консоли.
 - D. Загрузка конфигурационного файла из сетевого TFTP-сервера.
2. Какова функция команды configure memory?
 - A. Выполняет загрузку конфигурационной информации из энергонезависимой памяти.
 - B. Стирает содержимое энергонезависимой памяти.
 - C. Сохраняет в энергонезависимой памяти текущую конфигурацию, находящуюся в ОЗУ.
 - D. Выводит на экран конфигурацию, сохраненную в энергонезависимой памяти.
3. Какова функция команды copy running-config startup-config?
 - A. Загружает конфигурационную информацию из энергонезависимой памяти.
 - B. Стирает содержимое энергонезависимой памяти.
 - C. Сохраняет в энергонезависимой памяти текущую конфигурацию, находящуюся в ОЗУ.
 - D. Выводит на экран конфигурацию, сохраненную в энергонезависимой памяти.
4. Если необходимо выйти из режима конфигурирования, то какую из следующих команд следует ввести?
 - A. exit.
 - B. no config-mode.
 - C. <Ctrl+E>.
 - D. <Ctrl+Z>.
5. Если планируется конфигурирование интерфейса, то какой вид должна иметь командная строка маршрутизатора?
 - A. Router(config)f.
 - B. Router(config-in)I.
 - C. Router (config-intf)#.
 - D. Router(config-if)I.
6. Что из приведенного ниже соответствует правильному порядку процесса конфигурирования маршрутизатора? (Предполагается, что изменения в маршрутизаторе с помощью режима конфигурирования уже были сделаны.)
 - A. (1) Сохранение изменений в резервной копии; (2) Принятие решения относительно того, являются ли изменения желаемым результатом; (3) Проверка результатов; (4) Проверка резервного файла.
 - B. (1) Проверка результатов; (2) Принятие решения относительно того, являются ли изменения желаемым результатом; (3) Сохранение изменений в резервной копии; (4) Проверка резервного файла.
 - C. (1) Принятие решения относительно того, являются ли изменения желаемым результатом; (2) Проверка резервного файла; (3) Сохранение изменений в резервной копии; (4) Проверка результатов.
 - D. (1) Проверка результатов; (2) Сохранение изменений в резервной копии; (3) Принятие решения относительно того, являются ли изменения желаемым результатом; (4) Проверка резервного файла.
7. Какую из приведенных ниже команд можно использовать для сохранения изменений конфигурации маршрутизатора в резервной копии конфигурационного файла?
 - A. Router# copy running-config tftp.
 - B. Router#t show running-config.
 - C. RouterI config mem.
 - D. Router#t copy tftp running-config.
8. Какая из следующих команд *не* является командой удаления изменений в конфигурации маршрутизатора?
 - A. Router(config)# no

- B. Router# config mem.
 - C. Router1 copy running-config startup-config.
 - D. Router# copy tftp running-config.
9. Что из приведенного ниже правильно описывает конфигурирование в маршрутизаторе паролей?
- A. Все пароли устанавливаются в привилегированном режиме EXEC.
 - B. Все пароли видоизменяют паролевую цепочку символов.
 - C. Пароль может быть установлен на все входящие сеансы протокола Telnet.
 - D. Команда enable password ограничивает доступ к пользовательскому режиму EXEC.
10. Что из приведенного ниже *не* описывает процедуру конфигурирования пароля в маршрутизаторах?
- A. Пароли могут устанавливаться при работе в любом режиме конфигурирования.
 - B. Пароль может быть установлен на доступ с любого терминала консоли.
 - C. Пароль, устанавливаемый после команды enable secret, использует процесс шифрования, который видоизменяет паролевую цепочку символов.
 - D. Установка всех паролей начинается в режиме глобального конфигурирования.

Глава 16

Источники загрузки ОС IOS

В этой главе

- Процесс, используемый для нахождения местоположения межсетевой операционной системы (ОС IOS)
- Команды, позволяющие находить информации» об ОС IOS
- Процедура задания системы, используемой для начальной загрузки ОС IOS
- Применение TFTP-сервера для загрузки системного программного обеспечения в маршрутизатор
- Проверка маршрутизатора с целью оценки его способности работать с системным программным обеспечением
- Команды для создания и загрузки резервных копий образов системного программного обеспечения
- Правила именования файлов с системным программным обеспечением

Введение

В главе 15, "Конфигурирование маршрутизатора", рассказывалось об использовании режимов маршрутизатора и методов конфигурирования для обновления конфигурационных файлов маршрутизаторов, работающих под управлением текущей и более ранних версий ОС IOS. В данной главе речь пойдет о многочисленных источниках получения ОС IOS, выполнении команд, позволяющих загрузить ее в маршрутизатор, создавать и поддерживать резервные копии файлов ОС и обновлять версию. Кроме того, будет рассказано о функциях регистра конфигурирования и об определении версии файла, имеющегося в распоряжении. В этой главе также описано использование TFTP-сервера в качестве источника программного обеспечения

Обнаружение местоположения ОС IOS

Тип источника ОС IOS, используемого по умолчанию, зависит от аппаратной платформы, но в большинстве случаев маршрутизатор обращается к командам конфигурирования, записанным в энергонезависимой памяти. Для этого ОС IOS предлагает несколько возможных альтернатив. Можно задать другие источники, где маршрутизатор должен искать программное обеспечение, или маршрутизатор в случае необходимости загрузки программного обеспечения может воспользоваться своей собственной аварийной последовательностью действий.

Как показано на рис 16 1, установки в регистре конфигурирования позволяют иметь следующие альтернативы вариантов начальной загрузки ОС IOS.

Можно с помощью команд режима конфигурирования `boot system` задать последовательность использования маршрутизатором аварийных источников. Затем эти операторы с помощью команды `copy running-config startup-config` сохраняются в энергонезависимой памяти для использования при следующем запуске. После этого в случае необходимости маршрутизатор будет последовательно использовать данные команды при каждом перезапуске.

Если в энергонезависимой памяти нет команд `boot system`, которыми мог бы воспользоваться маршрутизатор, то он перейдет в аварийный режим и воспользуется образом ОС IOS по умолчанию, который хранится во флэш-памяти.

Если флэш-память пуста, то маршрутизатор попытается воспользоваться следующей альтернативой: загрузкой с TFTP-сервера. Для формирования имени файла, из которого будет осуществляться начальная загрузка хранимого на сетевом сервере образа системы по умолчанию, маршрутизатор использует значение из регистра конфигурирования.

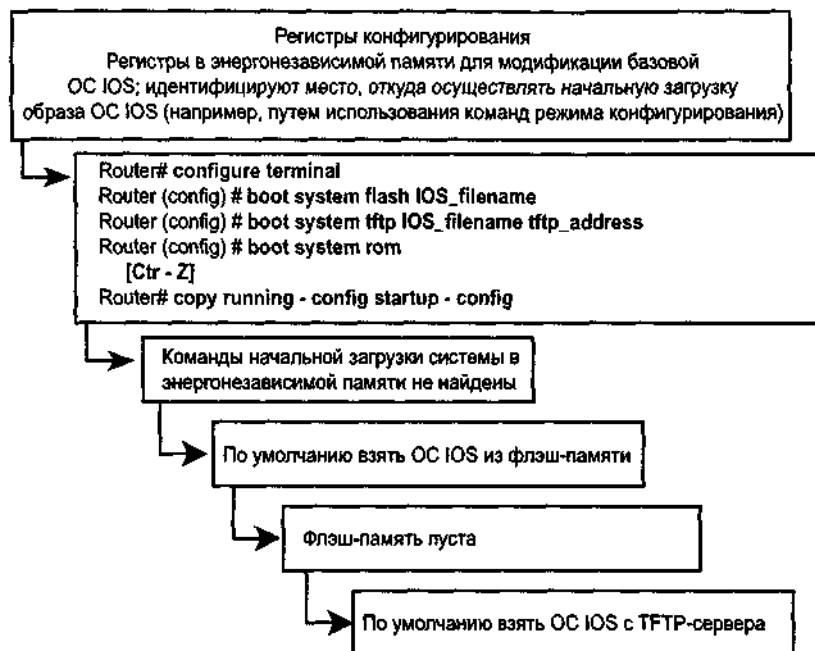


Рис. 16.1. Установки в регистре конфигурирования позволяют задать альтернативные источники для начальной загрузки ОС IOS

Значения в регистре конфигурирования

Порядок, в котором маршрутизатор ищет информацию для начальной загрузки системы, зависит от установки в поле начальной загрузки регистра конфигурирования. Установки регистра конфигурирования по умолчанию могут быть изменены с помощью команды режима конфигурирования `config-register`. В качестве аргумента для этой команды используется число в шестнадцатеричной форме.

```

Router# configure terminal
Router(config)# config-register 0x10F
[Ctrl-Z]
  
```

В данном примере регистр конфигурирования устанавливается таким образом, что для получения информации о варианте начальной загрузки системы маршрутизатор будет проверять файл запуска, находящийся в энергонезависимой памяти. Регистр конфигурирования представляет собой 16-разрядный регистр, организованный в энергонезависимой памяти. Младшие четыре разряда регистра конфигурирования (биты 3, 2, 1 и 0) формируют поле начальной загрузки. Чтобы изменить значение в поле начальной загрузки, оставив для всех других битов установки по умолчанию, необходимо следовать следующим указаниям (табл. 16.1).

Если необходимо войти в монитор ПЗУ, который главным образом является средой программиста, установите регистр конфигурирования в значение `0x100`. Находясь в мониторе ПЗУ, загрузите операционную систему вручную, используя в командной строке монитора команду `B`. (Это значение устанавливает биты поля начальной загрузки в состояние 0-0-0-0.)

- Для конфигурирования системы на автоматическую начальную загрузку из ПЗУ установите регистр конфигурирования в значение `0x101`. (Это значение устанавливает биты поля начальной загрузки в состояние 0-0-0-1.)
- Для конфигурирования системы на использование команд начальной загрузки из энергонезависимой памяти установите регистр конфигурирования в любое значение от `0x102` до `0x10F`. Это значение используется по умолчанию. (Данные значения устанавливают биты поля начальной загрузки в состояния от

0-0-1-0 до 1-1-1-1.)

- Для проверки установки поля начальной загрузки, например с целью верификации исполнения команды `config-register`, используется команда `show version`.

Таблица 16.1. Значения, используемые в команде `config-register`

Значение	Описание
0 ^X 100	Использование режима монитора ПЗУ (ручная загрузка с применением команды B)
0x101	Автоматическая загрузка из ПЗУ (вариант по умолчанию, если маршрутизатор не оснащен флэш-памятью)
От 0x102 до 0x10F	Проверка энергонезависимой памяти на наличие команд начальной загрузки системы (значение 0x102 является значением по умолчанию, если маршрутизатор оснащен флэш-памятью)

Команда `show version`

Команда `show version` выводит информацию о версии ОС IOS, выполняемой в данный момент на маршрутизаторе. Сюда входит и вывод установки в поле начальной загрузки. В примере, который иллюстрирует листинг 16.1, версия ОС IOS и описательная информация выведены во второй строке результата. Данный листинг показывает, что используется экспериментальная версия релиза 11.2. Строка

`System image file is "c4500-f-mz", booted via tftp from 171.69.1.129` указывает имя образа системы. О порядке именования образов в ОС IOS версии 11.2 будет рассказано ниже в этой главе. Сейчас важно отметить ту часть имени файла, которая свидетельствует о том, что данный образ предназначен для платформы Cisco 4500.

Листинг 16.1. Команда `show version`

```
Router# show version
Cisco Internetwork Operating System Software
IOS (tm) 4500 Software (C4500-J-M),
  Experimental Version 11.2(19960626:214907) ]
Copyright (c)1986-1006 by Cisco Systems, Inc.
Compiled Fri 28-Jun-96 16:32 by rbeach
Image text-base: 0x600088A0, data-base: 0x6076E000

ROM: System Bootstrap, Version 5.1(1) [daveu 1], RELEASE SOFTWARE
(fcl)
ROM: 4500-XBOOT Bootstrap Software, Version 10.1(1), RELEASE SOFTWARE
(fcl)

router uptime is 1 week, 3 days, 32 minutes
System restarted by reload
System image file is "c4500-f-mz", booted via tftp from 171.69.1.129
Cisco 4500 (R4K) processor (revision 0x00) with 2768K/1684K bytes of
Memory
Processor board ID 012P941
R4600 processor, implementation 32, Revision 1.0
G.703/E1 software, Version 1.0
Bridging software
SuperLAT software copyright 1990 by Meridian Technology Corp.
X.25 software, Version 2.0, NET2, BFE and GOSIP compliant
TN 270 Emulation software (copyright 1994 by TGV Inc.)
Primary Rate ISDN software, Version 1.0
2 Ethernet/IEEE 802.3 interfaces.
48 Serial network interfaces.
2 Channelized T1/PRI ports.
```

128K bytes of non-volatile configuration memory.
8192K bytes of processor board System flash (Read/Write)
4096K bytes of processor board Boot flash (Read/Write)

Далее в выводимом результате команда `show version` показывает информацию о типе платформы, на которой выполняется в данный момент версия ОС IOS.

Варианты начальной загрузки программного обеспечения

Для задания аварийной последовательности загрузки ОС IOS можно ввести несколько команд начальной загрузки системы `boot system`. Ниже приведены три примера, иллюстрирующие записи о начальной загрузке системы, которые задают, что образ ОС IOS сначала будет загружаться из флэш-памяти, потом с сетевого сервера и, наконец, из ПЗУ.

- *Флэш-память.* Применяя этот подход, можно копировать образ системы без внесения изменений в электрически стираемом программируемом постоянном запоминающем устройстве (ЭСППЗУ). Хранимая во флэш-памяти информация не восприимчива к сбоям в сети, которые могут иметь место при загрузке образов системы с TFTP-серверов.

```
Router# configure terminal
Router (config)# boot system flash gsnew-image
[Ctrl-Z]
Router# copy running-config startup-config
```

- *Сетевой сервер.* В целях обеспечения наличия резервной копии на случай повреждения информации во флэш-памяти можно задать загрузку образа системы с TFTP-сервера.

```
Router# configure terminal
Router(config)# boot system tftp test exe 172.16.13.111
[Ctrl-Z]
Router# copy running-config startup-config
```

- *ПЗУ.* Если флэш-память повреждена и сетевой сервер не способен к загрузке образа, то последним вариантом начальной загрузки является загрузка из ПЗУ. Однако с большой долей вероятности образ системы, находящийся в ПЗУ, будет представлять собой подмножество ОС IOS, в котором отсутствуют протоколы, функции и конфигурации полной версии ОС IOS. Этот образ также может быть более старой версией ОС IOS, если с момента покупки маршрутизатора уже проводилось обновление программного обеспечения.

```
Router# configure terminal
Router(config)# boot system rom
[Ctrl-Z]
Router# copy running-config startup-config
```

Команда `copy running-config startup-config` сохраняет команду в энергонезависимой памяти. В случае возникновения необходимости маршрутизатор будет выполнять команды `boot system` в том порядке, в котором они первоначально вводились в режиме конфигурирования.

Примечание

В результатах, выводимых командами `show running-config` и `show startup-config`, нет никаких свидетельств об установках в регистре конфигурирования.

Подготовка к работе с TFTP-сервером

Производственные сетевые комплексы обычно охватывают широкие области и содержат несколько маршрутизаторов. Для этих географически разбросанных маршрутизаторов необходимо место, которое бы играло роль источника или в котором бы хранились резервные копии образов программного обеспечения. Использование TFTP-сервера позволяет выгружать и загружать образы и конфигурационные файлы по сети.

Роль TFTP-сервера может играть другой маршрутизатор, или это может быть хост-система. TFTP-сервером может быть как рабочая станция с операционной системой UNIX, так и портативный компьютер (laptop), работающий под управлением DOS или Windows. Хост-машиной TFTP может быть любая система с загруженным и работающим протоколом TFTP, которая способна поддерживать передачу файлов в TCP/IP-сети.

Пусть необходимо перекопировать программное обеспечение между хост-машиной TFTP и флэш-памятью маршрутизатора. Чтобы использовать TFTP-сервер, следует обязательно проверить выполнение следующих предварительных условий.

Необходимо проверить маршрутизатор, чтобы удостовериться, что флэш-память видна, и в нее можно записывать. Также надо проверить, что маршрутизатор имеет достаточно места во флэш-памяти, чтобы вместить образ ОС IOS.

```
Router#t show flash  
4096 kbytes of flash memory on embedded flash (in XX).
```

```
file      offset      length      name  
0         0x40        1204637     xk09140z  
[903848/2097152 bytes free]
```

Необходимо проверить TFTP-сервер, чтобы удостовериться в его доступности по TCP/IP-сети. Одним из методов такой проверки является использование команды ping.

```
Router# ping tftp-address
```

Необходимо проверить TFTP-сервер и удостовериться, что файл или файловое пространство для образа ОС IOS известны. Для выполнения операций по выгрузке и загрузке необходимо задать путь или имя файла.

```
Is gs7-j-mz. 112-0.11
```

Выполнение этих предварительных шагов повышает эффективность работы. Если сразу заняться копированием файла, то достаточно велик шанс того, что оно не удастся и придется устранять проблемы, вызванные сбоями в копировании.

Команда show flash

Команда show flash используется для проверки достаточности в системе объема памяти под планируемый к загрузке образ ОС IOS. В примере, приведенном ниже, маршрутизатор имеет флэш-память объемом 4Мбайт, которые все свободны.

```
Router# show flash  
4096K bytes of flash memory sized on embedded flash  
File name/status  
0 mater/California//ill/bin/g7-j-mz.112-0.11 [deleted]  
[0/4194304 bytes free/total]
```

Необходимо сравнить свободный объем с объемом образа ОС IOS. Источником данных о размере образа может быть документ заказа на программное обеспечение или конфигурационный файл программного обеспечения, который можно найти на Web-сервере интерактивной связи с компанией Cisco (Cisco Connection Online, CCO).

Если свободной памяти недостаточно, то копирование или загрузка образа будут невозможны. При наличии подобного препятствия можно либо попытаться получить меньший по размеру образ ОС IOS, либо увеличить в маршрутизаторе доступный объем памяти.

Правила именования ОС IOS

Изделия компании Cisco уже давно вышли за рамки просто маршрутизаторов и включают множество платформ для всех уровней спектра сетевых продуктов. В целях оптимизации работы ОС IOS на этих различных платформах компания Cisco работает над разработкой множества различных образов ОС IOS. Эти образы приспособлены под различные платформы, доступные ресурсы памяти и наборы функций, которые хотят иметь заказчики в своих сетевых устройствах.

В ОС IOS версии 112 правила, принятые для именования программного обеспечения, предусматривают наличие в названии следующих трех частей (табл. 16.2).

- Первая часть названия образа содержит платформу, на которой он выполняется.
- Вторая часть имени образа идентифицирует специальные возможности образа. Буква или ряд букв обозначают наборы функций, поддерживаемые образом.
- Третья часть имени образа задает его место выполнения и является ли он zip-упакованным.

Условные обозначения в названии ОС IOS, значения полей имени, содержимое образа и другие детали могут изменяться. Для получения свежей информации следует обращаться в местное торговое представительство, канал дистрибуции или на Web-сервер ССО.

Таблица 16.2. Правила именования для ОС IOS версии 11.2

Пример названия	Аппаратная платформа	Функциональные возможности	Место выполнения, статус сжатия
cra25-cg-l	CiscoPro2500 (cra25)	Сервер общего применения/сервер с удаленным доступом, ISDN (eg)	Переместимая, без уплотнения (I)
igs-inr-1	Cisco ICG, 25xx и 3xxx (igs)	Подмножество IP, Novell IPX и базовый вариант IBM (inr)	Переместимая, без уплотнения (I)
c4500-aj-m	Cisco 4500 и 4700 (c4500)	APPN и подмножество уровня предприятия для моделей нижнего и среднего класса (aj)	ОЗУ, без уплотнения (m)
gs7-k-mz	Cisco 7000 и 7010	Уровень предприятия для моделей верхнего класса	ОЗУ, zip-уплотнение (mz)

Создание резервных копий образов программного обеспечения

Образ системного программного обеспечения может быть скопирован на сетевой сервер. Такая копия может играть роль резервной и использоваться для проверки идентичности копии во флэш-памяти и исходного дискового файла. Листинг 16.2 и рис. 16.2 иллюстрируют применение команды `show flash` для получения имени файла образа системного программного обеспечения (xk09140z) и команды `copy flash tftp` для его копирования на TFTP-сервер.

Листинг 16.2. Команды `show flash` и `copy flash tftp`

- Команда `show version` выводит информацию о версии ОС IOS, исполняемой на маршрутизаторе в данный момент времени.
- Для задания аварийной последовательности начальной загрузки ОС IOS можно вводить несколько команд начальной загрузки системы. Маршрутизаторы могут загружать ОС IOS из флэш-памяти, с TFTP-сервера или из ПЗУ.
- В целях проверки наличия в системе достаточного объема памяти для загрузки желаемого образа ОС IOS используется команда `show flash`.
- Согласно правилам именования, принятым для ОС IOS версии 11.2, имя программного обеспечения содержит три части.
- Платформа, на которой исполняется образ.
- Специальные возможности образа.
- Место исполнения образа и является ли он zip-уплотненным.
- Образ системы может быть скопирован на сетевой сервер. Копия образа системы может служить в качестве резервной копии и использоваться для проверки совпадения копии во флэш-памяти с исходным дисковым файлом.
- Новый образ может загружаться из TFTP-сервера с помощью команды `copy tftp flash`.
- Если необходимо загрузить резервную копию ОС IOS, можно воспользоваться видоизмененной командой `copy tftp flash` и загрузить тот образ, который ранее был выгружен на TFTP-сервер.

Контрольные вопросы

1. Что из приведенного ниже представляет собой последовательность, используемую маршрутизатором, для автоматического возврата в исходное состояние и обнаружения местонахождения источника ОС IOS?
 - A. (1) Флэш-память; (2) энергонезависимое ЗУ; (3) TFTP-сервер.
 - B. (1) Энергонезависимое ЗУ; (2) TFTP-сервер; (3) флэш-память.
 - C. (1) Энергонезависимое ЗУ; (2) флэш-память; (3) TFTP-сервер.
 - D. (1) TFTP-сервер; (2) флэш-память; (3) энергонезависимое ЗУ.
2. Что из приведенного ниже *не* описывает установки регистра конфигурирования для начальной загрузки ОС IOS?
 - A. Порядок, в котором маршрутизатор ищет информацию о начальной загрузке системы, зависит от установки в поле начальной загрузки.
 - B. Изменение установки регистра конфигурирования осуществляется с помощью команды `config-register`.
 - C. При установке значения в поле начальной загрузки регистра конфигурирования используется шестнадцатеричное число.
 - D. Для проверки установки поля начальной загрузки используется команда `show running-config`.
3. Что из приведенного ниже *не* выводится на экран командой ОС IOS `show version`?
 - A. Статистические данные по сконфигурированным интерфейсам.
 - B. Тип платформы, на которой исполняется ОС C. Установка регистра конфигурирования.
 - D. Версия ОС IOS.
4. Что из приведенного ниже *не* является частью процесса задания аварийной последовательности для начальной загрузки ОС IOS?
 - A. В режиме глобального конфигурирования вводятся команды начальной загрузки системы.
 - B. Для задания всей аварийной последовательности используется одна команда начальной загрузки системы.
 - C. Сохранение в энергонезависимой памяти команд начальной загрузки с помощью команды `copy running-config startup-config`.
 - D. Если необходимо, то во время отработки аварийного режима команды начальной загрузки системы исполняются в той последовательности, в которой они вводились.
5. Что из приведенного ниже правильно описывает подготовку к использованию TFTP-сервера для копирования программного обеспечения во флэш-память?
 - A. TFTP-сервер должен быть другим маршрутизатором или хост-системой, например рабочей станцией с ОС UNIX или портативным компьютером.
 - B. Хост-машина TFTP должна быть системой, подключенной к сети Ethernet.
 - C. Должно быть идентифицировано имя маршрутизатора, содержащего флэш-память.
 - D. Должна быть разрешена работа флэш-памяти.
6. Какой способ является самым быстрым для проверки достижимости TFTP-сервера перед попыткой пересылки файла образа ОС IOS?
 - A. Проследить путь к TFTP-серверу с помощью команды `tracert`.
 - B. Пропинговать TFTP-сервер с помощью команды `ping`.
 - C. Установить с TFTP-сервером Telnet-соединение с помощью команды `telnet`.
 - D. Позвонить администратору TFTP-сервера.
7. Для чего необходимо определять размер файла образа ОС IOS на TFTP-сервере перед пересылкой его в маршрутизатор?
 - A. Чтобы проверить достаточность пространства во флэш-памяти для его сохранения.
 - B. Для верификации файла на предмет пригодности версии ОС IOS для данного маршрутизатора.
 - C. Для завершения операции пересылки протокола TFTP.
 - D. Для определения времени выгрузки файла и, таким образом, для оценки объема времени, в течение которого маршрутизатор не будет выполнять свою основную функцию.
8. Зачем создается резервная копия образа ОС IOS?

- A. Для проверки того, что копия во флэш-памяти совпадает с копией в ПЗУ.
 - B. Для получения аварийной копии текущего образа перед копированием образа в новый маршрутизатор.
 - C. Для создания аварийной копии текущего образа как части процедур во время восстановления после отказа системы.
 - D. Для создания аварийной копии текущего образа перед переходом на новую версию.
9. Что, по-вашему, содержит ограниченную версию ОС IOS?
- A. ПЗУ.
 - B. Флэш-память.
 - C. TFTP-сервер.
 - D. Монитор ПЗУ.
10. Какую команду следует выдать, если необходимо обновить старую версию ОС IOS путем загрузки нового образа с TFTP-сервера?
- A. `boot system tftp 131.21.11.3.`
 - B. `copy tftp flash***.`
 - C. `show flash.`
 - D. `tftp ios.exe.`

Глава 17

Конфигурирование IP-адресов интерфейсов маршрутизатора

В этой главе ..

- TCP/IP-адреса, адреса хост-машин и широковещания
- Формат IP-адресов
- Процессы, используемые для конфигурирования IP-адресов, в том числе логические сетевые адреса и сетевые маски
- Конфигурирование сервера имен
- Команды вывода на экран
- Верификация IP-адресов с использованием команд `telnet`, `ping`, `trace`

Введение

В главе 16, "Источники загрузки ОС IOS", рассказывалось об использовании различных источников получения кода межсетевой операционной системы компании Cisco (ОС IOS), о выполнении команд для загрузки ОС IOS в маршрутизатор, создании и хранении резервных копий файлов и обновлении версии ОС IOS. В данной главе будет подробно рассказано о классах IP-адресов, сетевых адресах и адресах узлов, а также о масках подсетей. Кроме того, здесь будут изложены основные концепции, которые надо четко представлять, прежде чем приступать к конфигурированию IP-адресов.

Краткие сведения о TCP/IP-адресах

В среде TCP/IP конечные станции обмениваются информацией с серверами или другими конечными станциями. Это происходит благодаря тому, что каждый узел, использующий группу протоколов TCP/IP, имеет уникальный 32-разрядный логический адрес, известный как *IP-адрес*.

Часто в сетевом комплексе трафик передается на основе названия организации, а не на основе имени конкретного человека или хост-машины. Если вместо адресов используются имена, то, до того как трафик может быть доставлен по месту назначения, каждое имя должно быть преобразовано в числовой адрес. Месторасположение организации диктует путь, по которому данные следуют в сетевом комплексе.

Каждая компания в многосетевом комплексе имеет уникальный 32-разрядный логический адрес. Он является уникальным адресом сети, с которой необходимо установить связь прежде, чем можно будет связаться с отдельной хост-машиной внутри компании. Сеть каждой компании имеет свой адрес, хост-машины, находящиеся в этой сети, используют один и тот же сетевой адрес, но каждая хост-машина внутри сети идентифицируется своим уникальным адресом — адресом хост-машины (рис 17.1).

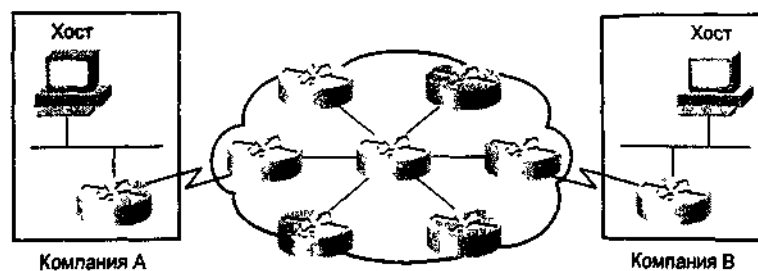


Рис. 17.1 Прежде чем установить контакт с отдельной хост-машиной в компании, необходимо определить уникальный 32-разрядный логический адрес сети

Концепции конфигурирования IP-адресов

В данном разделе рассказывается об основных концепциях, которые необходимо знать прежде, чем приступать к конфигурированию IP-адресов. Исследуя различные требования сети, можно выбрать правильный класс адреса и определить порядок разбиения на IP-подсети.

Адреса хост-машин

Каждое устройство или интерфейс должны иметь ненулевой номер хост-машины. Адрес хост-машины, состоящий из единиц, зарезервирован для режима IP-широковещания в сети (рис. 17.2). Нулевое значение означает "эта сеть" или "сам провод" (например, 172.16.0.0). В некоторых ранних

вариантах реализации протокола TCP/IP нулевое значение также использовалось для IP-широковещания, но теперь это делается редко. Таблица маршрутизации (табл. 17.1) содержит записи с сетевыми адресами или адресами проводов; как правило, она не содержит никакой информации о хост-машинах.

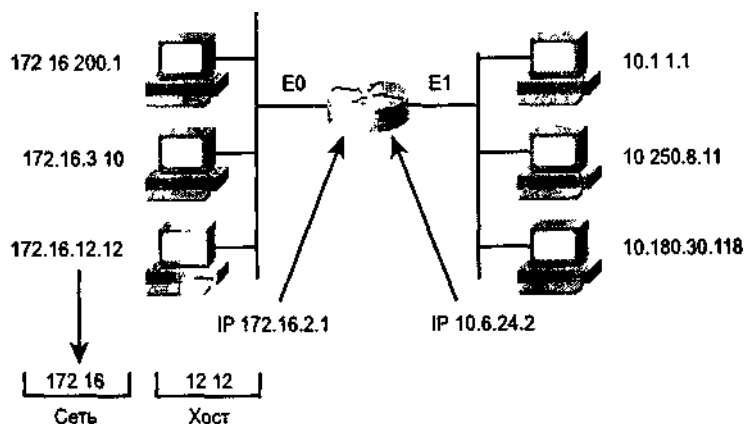


Рис. 17.2 Все хост-машины должны иметь ненулевые IP-адреса

Наличие у интерфейса IP-адреса с адресом подсети позволяет системе принимать и передавать пакеты; задавать локальный адрес устройства и диапазон адресов, которые используют один кабель с устройством.

17.1. Таблица маршрутизации с записями сетевых адресов

Сеть	Интерфейс
172.16.0.0	E0
10.0.0.0	E1

Пример разбиения на подсети

На рис. 17.3 показана небольшая сеть с назначенными адресами интерфейсов, масками подсетей и получающимися в результате номерами подсетей (табл. 17.2). Количество битов в каждой подсетевой маске показывается в виде числа /8, стоящего за маской.

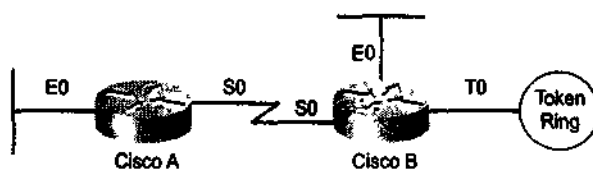


Рис. 17.3. Сети назначаются адреса интерфейсов, маски подсети и получающиеся в результате номера подсетей

Таблица 17.2. Назначения в сети

Адрес интерфейса	Маска подсети	Номер подсети
Cisco A		
EO: 172. 16. 2. 1	255. 255. 255. 0/8	172.16.2.0
SO: 172. 16. 1. 1	255. 255. 255. 0/8	172.16.1.0
Cisco B		
SO: 172. 16. 1. 2	255. 255. 255. 0/8	172.16.1.0
EO: 172. 31. 4. 1	255. 255. 255. 0/8	172.31.4.0
TO: 172. 31. 16.1	255. 255. 255. 0/8	172.31.16.0

Адрес широковещания

В сети Internet поддерживается режим широковещания. Широковещательные сообщения представляют собой такие сообщения, которые должны быть услышаны всеми хост-машинами, находящимися в сети. Широковещательный адрес формируется путем использования IP-адреса, состоящего из единиц.

ОС IOS поддерживает два типа широковещания: направленные и лавинные. Лавинные широковещательные пакеты (представляемые адресом 255.255.255.255) не распространяются между сетями и считаются локальными широковещательными пакетами (рис. 17.4). Разрешено использование направленных широковещаний, которые перенаправляются маршрутизатором. Пакеты направленного широковещания содержат все единицы в хостовой части адреса.

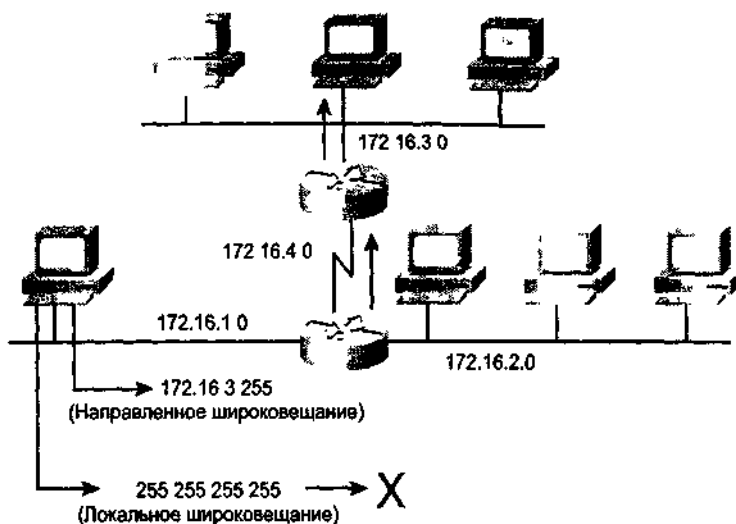


Рис 17.4 Широковещание может осуществляться локально или на подсеть

Конфигурирование IP-адресов

Для установки на интерфейсе логического сетевого адреса используется команда **ip address**:

```
Router(config-if) # ip address ip-address subnet-mask
```

где *ip-address* — 32-разрядное двоичное число в десятичном представлении с разделением точками, *subnet-mask* — тоже 32-разрядное двоичное число в десятичном представлении с разделением точками, причем единицы соответствуют позициям, которые должны совпадать, а нули указывают несовпадающие позиции. Команда **ip address** назначает адрес и маску подсети и запускает на интерфейсе IP-обработку.

Для задания формата сетевых масок для текущего сеанса используется команда **term ip netmask-format**:

```
Router(config)# term ip netmask-format
```

Эта команда устанавливает формат маски сети (табл. 17.3). Возможны следующие форматы сетевой маски:

- с суммой битов;
- десятичный с разделением точками (формат по умолчанию);

- шестнадцатеричный.

Таблица 17.3. Команды, связанные с IP-адресами

Уровень команды	Команда	Назначение
Router(config-if)#	ip address ip-address <i>subnet-mask</i>	Присваивает адрес и номер подсети интерфейсу, начинает IP-обработку
Router#	term ip netmask-format{bit count decimal hexadecimal}	Устанавливает формат сетевой маски для текущего сеанса
Router (config-if)#	ip netmask-format {bit count decimal hexadecimal}	Устанавливает формат сетевой маски для конкретного канала

IP-имена хост-машин

ОС IOS ведет таблицу имен хост-машин и соответствующих им адресов, также называемую *отображением хост-адресов*. В протоколе Telnet имена хост-машин используются для идентификации сетевых устройств (хостов). Для того чтобы общаться с другими IP-устройствами, маршрутизатор и другие сетевые устройства должны уметь соотносить имена хост-машин с IP-адресами.

Команда `ip host` делает в конфигурационном файле маршрутизатора статическую запись об отображении имени в адрес (табл 17.4).

Таблица 17.4. Команда ip host

Команда ip host	Описание
<i>name</i>	Любое имя, которое предпочитает пользователь для описания пункта назначения
<i>top-port -number</i>	Необязательный номер, который идентифицирует TCP-порт для использования, когда имя хост-машины используется с командой режима EXEC <code>connect</code> или командой <code>telnet</code> . Для работы с протоколом Telnet по умолчанию стоит port23
Address	IP-адрес или адреса, по которым можно связаться с устройством

Приведенная ниже команда задает статическое отображение имени хост-машины на IP-адрес.

```
Router(config)# ip host name [top-port-number] address [address] ...
ip host tokyo 1.0.0.5 2.0.0.8
ip host kyoto 1.0.0.4
```

где 1.0.0.5 2.0.0.8 являются двумя сетевыми адресами для хоста с именем tokyo, а 1.0.0.4 определяет имя kyoto в качестве эквивалента адресу 1.0.0.4.

Конфигурирование сервера имен

Команда `ip name-server` задает те хост-машины, которые могут предоставить сервис имен. В одной команде можно задавать максимум шесть IP-адресов серверов имен:

```
Router(config)# ip name-server server-address! [[server-address2] [server-address 6]
```

Для отображения доменных имен на IP-адреса необходимо идентифицировать имена хост-машин, а затем задать сервер имен и активизировать систему доменных имен Domain Name System (DNS). После этого каждый раз, когда операционная система будет получать команду или адрес, которые она не сможет распознать, она будет обращаться в DNS за IP-адресом этого

устройства.

Схемы отображения "имя-адрес"

Каждый уникальный IP-адрес может иметь соответствующее ему имя хост-машины. ОС IOS управляет кэшем отображения "имя хост-машины—адрес", который используется командами режима EXEC. Этот кэш убыстряет процесс преобразования имен в адреса.

В протоколе IP определена схема присвоения имен, которая позволяет идентифицировать устройства по их месту в IP-сети. Например, имя ftp.cisco.com идентифицирует домен протокола передачи файлов (FTP) для устройств Cisco. Для отслеживания имен доменов в IP-сети задается сервер имен, который управляет кэшем имен.

Служба DNS активизируется по умолчанию с адресом сервера 255.255.255.255, который является адресом локального широковещания. Как показано ниже, команда `no ip domain-lookup` отключает в маршрутизаторе преобразование имен в адреса:

```
Router(config)# no ip domain-lookup
```

Это означает, что маршрутизатор не будет переадресовывать широковещательные DNS-пакеты.

Вывод информации об именах хост-машин

Для вывода находящегося в кэше списка имен хост-машин и адресов используется команда `show hosts`, которая показана в листинге 17.1.

Листинг 17.1. Команда `show hosts`

```
Router# show hosts
Default domain is not set
Name/address lookup uses static mappings

Host      Flags      Age      Type      Address(es)
TOKYO     (perm, OK) 5        IP        144.253.100.200 133.3.13.2
          133.3.5.1 133.3.10.1
S         (perm, OK) **       IP        172.16.100.156
LUBBOCK   (perm, OK) 5        IP        183.8.128.12 153.50.3.2
AMARILLO (perm, OK) **       IP        153.50.129.200 153.50.3.1
BELLEVUE (perm, OK) **       IP        144.253.100.201 153.50.193.2
          153.50.65.1 153.50.33.1
BOSTON    (perm, OK) **       IP        144.253.100.203 192.3.63.129
          192.3.63.33 192.3.63.65
CHICAGO   (perm, OK) 5        IP        183.8.0.129 183.8.128.130
          183.8.64.130
Router    (perm, OK) **       IP        144.253.100.202 183.8.128.2
          183.8.128.129 183.8.64.129
FARGO     (perm, OK) **       IP        183.8.0.130 183.8.64.100
HARTFORD (perm, OK) **       IP        192.3.63.196 192.3.63.34
          192.3.63.66
HOUSTON   (perm, OK) **       IP        153.50.129.1 153.50.65.2
--More --
```

В табл. 17.5 приведены значения столбцов результата выполнения команды `show hosts`, сведения в которых могут быть использованы для получения специфической информации о записи с именем хост-машины.

Таблица 17.5. Результат выполнения команды `show hosts`

Поле результата	Описание
Host	Имена хост-машин, о которых стало известно маршрутизатору
Flag	Описание того, как поступила информация, и ее текущий статус
perm	Ручное конфигурирование в статической таблице хост-машин
temp	Получено в результате использования службы DNS
ок	Текущая запись
EX	Запись превысила временной предел нахождения в таблице, или срок ее достоверности истек
Age	Время в часах с момента обращения программного обеспечения к записи
Type	Поле протокола
Address (es)	Логические адреса, связанные с именем хост-машины

Верификация конфигурации адресов

Проблемы адресации являются наиболее часто встречающимися в IP-сетях. Поэтому важно сначала проверить конфигурацию адресов и только потом продолжать конфигурирование. Приведенные ниже три команды позволяют верифицировать конфигурацию адресов в сети.

- `telnet` — команда, которая верифицирует работу программного обеспечения уровня приложений между отправителем и получателем. Она представляет собой наиболее полный механизм тестирования из имеющихся.
- `ping` — использует межсетевой протокол управляющих сообщений (Internet Control Message Protocol, ICMP) для верификации соединения на аппаратном уровне и логический адрес сетевого уровня. Это самый основной механизм тестирования.
- `trac` — использует значения параметра времени* жизни (Time To Live, TTL) для генерации сообщений от каждого из маршрутизаторов, задействуемых по пути следования пакета. Это очень мощное средство для локализации отказов по пути от отправителя к получателю.

Команда telnet

`telnet` — это простая команда, которая используется для того, чтобы посмотреть, можно ли установить соединение с маршрутизатором. Если с маршрутизатором не удастся установить Telnet-сеанс, но его можно пропинговать с помощью команды `ping`, то тогда понятно, что проблема заключается в функциональности маршрутизатора верхнего уровня. В этом случае, возможно, надо перезагрузить маршрутизатор и попытаться снова установить с ним сеанс.

Команда ping

Команда `ping` посылает ICMP эхо-пакеты и поддерживается как в пользовательском, так и в привилегированном режиме EXEC. В приведенном ниже примере время прохождения одного эхо-пакета превысило заданный предел ожидания, о чем говорит точка (.) в выводимой информации, а четыре были успешно приняты, что показано восклицательными знаками (!).

```
Router> ping 172.16.101.1
Type escape sequence to abort.
Sending 5 100-byte ICMP echoes to 172.16.101.1. timeout is 2 seconds:
.!!!!
Success rate is 80 percent, round-trip min/avg/max = 6/6/6 ms Router>
```

В табл. 17.6 приведены символы, обозначающие результат ping-тестирования, которые могут встретиться в информации, выводимой командой `ping`.

Таблица 17.6. Команда ping для тестирования возможности установления связи в IP сетях

Символ	Определение
!	Успешный прием эхо-ответа
.	Превышение временного предела ожидания ответной дейтаграммы
U	Ошибка недостижимости пункта назначения
C	Пакет столкнулся с перегрузкой в сети
I	Исполнение команды ping было прервано (например, в результате нажатия комбинации клавиш <Ctrl+Shift-6 X)
?	Неизвестный тип пакета
&	Пакет превысил значение параметра TTL

Расширенная команда ping

Расширенная команда ping поддерживается только из привилегированного режима EXEC. Как показано в листинге 17.2, расширенный режим команды ping можно использовать для задания поддерживаемых опций заголовков, используемых в сети Internet. Для того чтобы войти в расширенный режим, необходимо в строке подсказки Extended commands ("Расширенные команды") ввести букву "y".

Листинг 17.2. Расширенная команда ping, которая поддерживается только из привилегированного режима EXEC

```
Router# ping
Protocol [ip]:
Target IP address: 192.168.101.162
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2] :
Extended commands [n] : y
Source address:
Type of service [0]:
Set DF bit in IP header? [no]: yes
Data pattern [0xABCD] :
Loose, Strict, Record, Timestamp, Verbose [non]:
Sweep range of sizes [n] :
Type escape sequence to abort.
Sending 5 100-byte ICMP echoes to 192.168.101.162. timeout is 2 seconds :
!!!!!!
Success rate is 100 percent (5/5), roundrobin min/avg/max = 24/26/28 ms
Router#
```

Команда trace

При использовании команды trace (листинг 17.3) имена хост-машин выводятся в том случае, если имеет место динамическое преобразование адресов или они преобразуются с помощью записей в статической таблице хост-машин. Выводимые временные значения отражают время, необходимое для возврата каждого из трех зондирующих пакетов.

Листинг 17.3. Команда trace

```
Router# trace aba.nyc.mil
Type escape sequence to abort.
Tracing the route to aba.nyc.mil (26.0.0.73)
 1. debris.cisco.com (172.16.1.6) 1000 msec 8 msec 4 msec
 2. barmet-gw.cisco.com (172.16.16.2) 8 msec 4 msec 4 msec
```

3. external-a-gateway.stanford.edu (192.42.110.225) 8 msec 4 msec 4 msec
4. bb2.su.barmet.net (131.119.254.6) 8 msec 8 msec 8 msec
5. su.arc.barmet.net (131.119.3.8) 12 msec 12 msec 8 msec
6. moffett-flt-mb.in.mil (192.52.195.1) 216 msec 120 msec 132 msec
7. aba.nyc.mil (26.0.0.73) 412 msec * 664 msec

Когда процесс трассировки достигает намеченного пункта назначения, на экран выводится символ звездочки (*). Обычно это происходит в результате приема пакета с сообщением о недостижимости порта и превышения временного предела ожидания ответа на зондирующий пакет. Другие ответы, которые могут быть получены по команде trace, приведены в табл. 17.7.

Примечание

Команда trace поддерживается межсетевым протоколом (IP), службой сетевого сервиса без установления соединения (Connectionless Network Service, CLNS), службой виртуальной интегрированной сети (Virtual Integrated Network Service, VINES) и протоколом AppleTalk.

Таблица 17.7. Ответы команды trace

Ответ	Определение
! Н	Зондирующий пакет был принят маршрутизатором, но не переадресован, что обычно бывает из-за наложенного списка доступа
P	Протокол недостижим
N	Сеть недостижима
и	Порт недостижим
*	Превышение временного предела ожидания

Резюме

В среде TCP/IP конечные станции обмениваются информацией с серверами или другими конечными станциями. Это происходит благодаря тому, что каждый узел, использующий группу протоколов TCP/IP, имеет уникальный 32-разрядный логический адрес, известный под названием *IP-адрес*.

Наличие у интерфейса IP-адреса с адресом подсети позволяет достичь трех целей:

- Система имеет возможность обрабатывать прием и передачу пакетов.
- Задается локальный адрес устройства
- Задается диапазон адресов, которые используют один кабель с устройством.

Широковещательные сообщения — это такие сообщения, которые должны быть услышаны всеми хост-машинами, находящимися в сети.

Команда ip address используется для присвоения данному интерфейсу логического сетевого адреса.

Команда ip hosts осуществляет статическую запись "имя—адрес" в конфигурационный файл маршрутизатора.

Команда ip name-server задает те хост-машины, которые могут предоставить сервис работы с именами.

Команда show hosts используется для вывода находящегося в кэше списка имен хост-машин и их адресов.

Для верификации конфигурации IP-адресов могут использоваться команды telnet, ping И trace.

Контрольные вопросы

1. Что из приведенного ниже наилучшим образом описывает функцию адреса широковещания?
 - A. Посылает сообщение в единственный пункт назначения в сети.
 - B. Копирует сообщения и посылает их по конкретному подмножеству сетевых адресов.
 - C. Посылает сообщение всем узлам в сети.
 - D. Посылает сообщение каждому узлу, к которому маршрутизатор имеет доступ.
2. Какова цель использования команды trace?
 - A. Это наиболее полный механизм тестирования из имеющихся.
 - B. Это самый основной механизм тестирования.
 - C. Она добавляет IP-адрес и имя в таблицу маршрутизатора.
 - D. Она локализует отказы по пути от отправителя к получателю.
3. Каково назначение команды ip name-server?
 - A. Задает хост-машины, которые могут предоставить сервис работы с именами.
 - B. Определяет схему присвоения имен, которая позволяет идентифицировать устройства по их местоположению.
 - C. Идентифицирует TCP-порт, который необходим при использовании имени хост-машины.
 - D. Генерирует сообщения от каждого маршрутизатора, задействованного по пути прохождения дейтаграммы.
4. Если необходимо отобразить имя домена на IP-адрес, то что надо сделать сначала?
 - A. Идентифицировать имена хост-машин.
 - B. Задать сервер имен.
 - C. Активизировать службу DNS.
 - D. Обратиться в службу DNS за IP-адресом этого устройства.
5. Каково назначение команды по ip domain-lookup?
 - A. Задает хост-машины, которые могут предоставить сервис работы с именами.
 - B. Определяет схему присвоения имен, которая позволяет идентифицировать устройства по их местоположению.
 - C. Включает в маршрутизаторе функцию преобразования "имя-адрес".
 - D. Отключает в маршрутизаторе функцию преобразования "имя— адрес".
6. Что из приведенного ниже наилучшим образом описывает функцию команды show hosts?
 - A. Идентифицирует маску подсети, используемую в пункте назначения.
 - B. Управляет кэшем отображения имен на адреса, который используется командами режима EXEC.
 - C. Используется для вывода на экран находящегося в кэше списка имен и адресов.
 - D. Показывает имя хост-машины по IP-адресу.
7. Какова функция команды telnet?
 - A. Проверяет работоспособность программного обеспечения уровня приложений на участке между станцией-отправителем и станцией-получателем.
 - B. Проверяет возможность соединения на физическом уровне и логический адрес сетевого уровня.
 - C. Генерирует сообщения от каждого маршрутизатора, задействованного вдоль пути перемещения пакета
 - D. Показывает продолжительность времени в часах с момента обращения программного обеспечения к записи.
8. Какова функция команды ping?
 - A. Проверяет работоспособность программного обеспечения уровня приложений на участке между станцией-отправителем и станцией-получателем.
 - B. Использует протокол ICMP для проверки возможности соединения на физическом уровне и логического адреса сетевого уровня.

- C. Присваивает значения для генерации сообщений от каждого маршрутизатора, задействованного вдоль пути перемещения пакета.
 - D. Описывает, как отсылалась информация, и ее текущий статус.
9. Какую команду следует использовать для занесения статической записи отображения "имя-адрес" в конфигурационный файл маршрутизатора?
- A. ip perm.
 - B. ip route.
 - C. ip name.
 - D. ip host.
10. Что из приведенного ниже наилучшим образом описывает функцию расширенной команды ping?
- A. Используется для задания поддерживаемых в сети Internet-заголовков.
 - B. Используется для задания временных рамок возврата ping-пакета.
 - C. Используется для диагностики причин задержки или невозвращения ping-пакета.
 - D. Используется для отслеживания прохождения дейтаграммы через каждый маршрутизатор.

Глава 18

Конфигурирование маршрутизатора и протоколы маршрутизации RIP и IGRP

В этой главе...

- Режим начального конфигурирования маршрутизатора режим начальной установки
- Таблица IP-маршрутизации
- Команды статической маршрутизации
- Команды маршрутизации по умолчанию
- Команды динамической маршрутизации, включая протоколы RIP и IGRP

Введение

В главе 17, "Конфигурирование IP-адресов интерфейсов маршрутизатора", был описан процесс конфигурирования адресов межсетевого протокола (IP). В данной главе будет рассказано о начальном конфигурировании маршрутизатора на применение таких протоколов IP-маршрутизации, как протокол маршрутной информации (Routing Information Protocol, RIP) и протокол внутренней маршрутизации между шлюзами (Interior Gateway Routing Protocol, IGRP)

Начальное конфигурирование маршрутизатора

После тестирования аппаратной части и загрузки образа ОС IOS маршрутизатор находит и выполняет операторы конфигурирования. Эти операторы дают подробную информацию об атрибутах данного конкретного маршрутизатора, функциях протоколов и адресах интерфейсов. Однако, если маршрутизатор сталкивается с начальной ситуацией, когда он не может обнаружить достоверный конфигурационный файл запуска, он переключается в режим начального конфигурирования, называемый *режимом начальной установки*.

Благодаря средствам команды режима начальной установки (команды `setup`) пользователь имеет возможность вводить ответы на вопросы диалога конфигурирования системы. Эти средства запрашивают у пользователя основную информацию о конфигурации. Представляемые пользователем ответы позволяют маршрутизатору сформировать достаточную, но функционально минимальную конфигурацию, при этом:

- определяется перечень используемых интерфейсов;
- предоставляется возможность ввода глобальных параметров;
- предоставляется возможность ввода параметра интерфейсов;
- осуществляется просмотр скрипта начальной установки;
- предоставляется возможность ввода подтверждения пользователя на использование данной конфигурации.

После того как пользователь утверждает информацию, введенную в режиме начальной установки, маршрутизатор использует эти записи в качестве рабочей конфигурации. Он также записывает эту конфигурацию в энергонезависимую память в качестве нового конфигурационного файла запуска. Теперь пользователь может использовать маршрутизатор. Для введения дополнительных изменений относительно протоколов и интерфейсов пользователь должен войти в режим EXEC и ввести команду `configure`.

Начальная таблица IP-маршрутизации

Как показано на рис. 18.1, первоначально маршрутизатор должен обратиться к записям о непосредственно подключенных к нему сетях или подсетях. Каждый интерфейс должен быть сконфигурирован соответствующим IP-адресом и маской. ОС IOS узнает эту информацию об IP-адресе и маске из конфигурационных данных, получаемых из какого-либо источника. Первоначальным источником адресных данных является тот человек, который вносит их в конфигурацию.

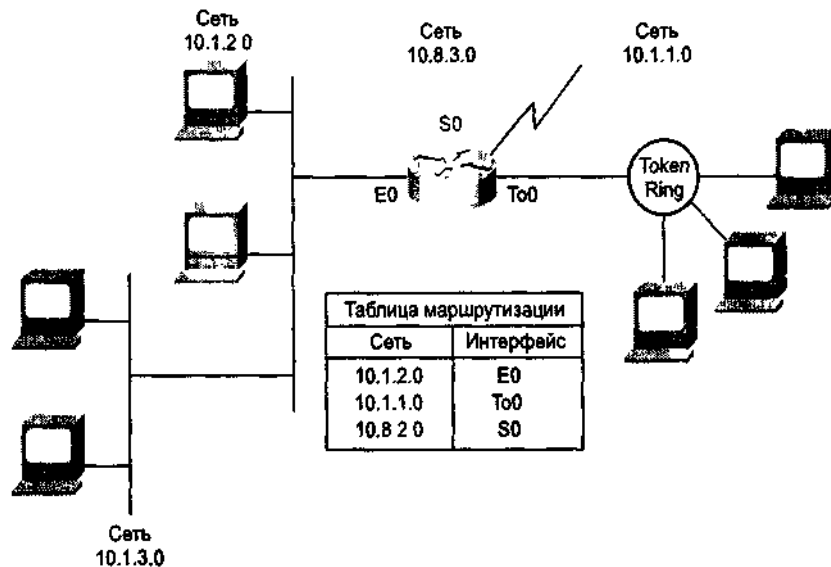


Рис 18.1. Маршрутизатор поддерживает таблицу соответствия адресов и портов

В данном разделе рассматривается ситуация, когда маршрутизатор запускается в начальных условиях, т.е. при отсутствии других источников информации о конфигурации запуска. При таких условиях запуска маршрутизатора можно будет воспользоваться средствами команды режима начальной установки и ввести ответы на запросы системы относительно информации по базовой конфигурации маршрутизатора. Вводимые ответы включают команды соответствия "адрес—порт", позволяющие сделать установки интерфейсов для работы с протоколом IP. Маршрутизаторы узнают о путях к пунктам назначения тремя различными способами.

- *Статические маршруты* — задаются системным администратором вручную как единственный путь к пункту назначения. Полезен с точки зрения управления безопасностью сети и уменьшения трафика (рис. 18.2).
- *Маршруты по умолчанию* — задаются системным администратором вручную в качестве пути, который используется в случаях, когда другой маршрут к пункту назначения неизвестен (рис. 18.3).
- *Динамические маршруты* — маршрутизатор узнает о путях к пунктам назначения, принимая периодические пакеты актуализации маршрутной информации от других маршрутизаторов.

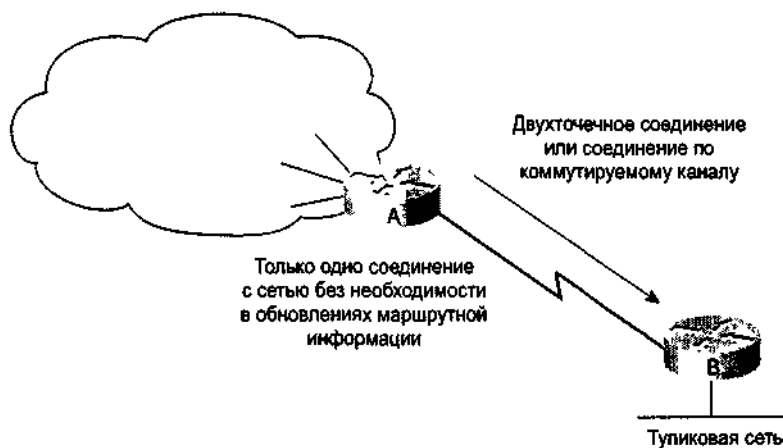


Рис 18.2. Фиксированный маршрут до адреса отражает те знания, которые известны администратору

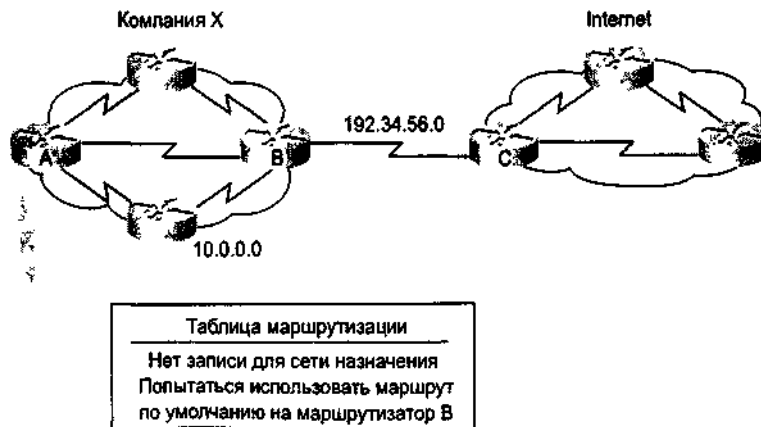


Рис. 18.3 Маршрут по умолчанию используется в тех случаях, когда следующий переход пути не имеет явного отражения в таблице маршрутизации

Конфигурирование статических маршрутов

Статические маршруты представляют собой задаваемые пользователем маршруты, которые заставляют двигающиеся между отправителем и получателем пакеты идти по конкретному пути. Статический маршрут устанавливается командой `ip route` со следующим синтаксисом:

```
ip route network [mask] {address | interface} [distance]
```

Параметры имеют такое смысловое значение (табл. 18.1).

Таблица 18.1. Описание параметров статической маршрутизации

Параметр	Описание
<i>Network</i>	Сеть или подсеть пункта назначения
<i>mask</i>	Маска подсети
<i>Ethernet 0</i>	Имя интерфейса, которым надо воспользоваться, чтобы попасть на адрес пункта назначения
<i>address</i>	IP-адрес маршрутизатора следующего перехода
<i>interface</i>	Имя интерфейса, которым надо воспользоваться, чтобы попасть в сеть пункта назначения
<i>distance</i>	Административное расстояние

Административное расстояние представляет собой рейтинг достоверности маршрутной информации, выражаемый числами со значениями от 0 до 255. Чем больше число, тем ниже рейтинг достоверности. Например, значение административного расстояния, равное 253, свидетельствует о чрезвычайно низком рейтинге достоверности.

Статические маршруты позволяют вручную конфигурировать таблицу маршрутизации, и до тех пор, пока путь активен, подобная запись в таблице не подвергается динамическим изменениям.

Статический маршрут может отражать некоторые специальные сведения о ситуации в сети, которые известны сетевому администратору. Как правило, значения административного расстояния, введенные вручную, являются низкими. Пакеты актуализации маршрутной информации не посылаются в канал, заданный в качестве статического маршрута, что сохраняет, таким образом, полосу пропускания.

Пример статического маршрута

Показанный на рис. 18.4 пример содержит следующие значения.

<code>ip route 172,16.1.0</code>	Задаёт статический маршрут до подсети пункта назначения.
<code>255.255.255.0</code>	Маска подсети, которая говорит о том, что для разбиения на подсети используется 8 разрядов
<code>172.16.2.1</code>	IP-адрес маршрутизатора следующего перехода на пути к пункту назначения

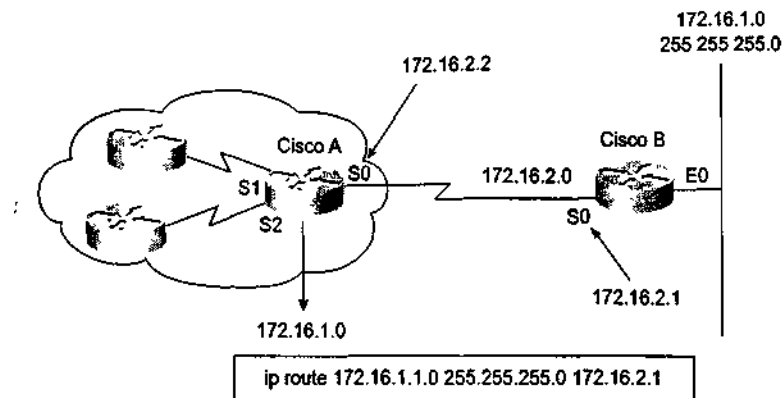


Рис. 18.4. В маршрутизаторе Cisco A сконфигурирован статический маршрут к сети 172.16.1.0

Для маршрутизатора Cisco A назначение статического маршрута для выхода на тупиковую сеть 172.16.1.0 является приемлемым, поскольку существует только один способ добраться до этой сети. Назначение статического маршрута для выхода на "облако" сетей в маршрутизаторе Cisco B тоже возможно. Однако в этом случае необходимо назначить статический маршрут для каждой сети назначения, так что здесь может быть более подходящим назначение маршрута по умолчанию.

Конфигурирование маршрута по умолчанию

Маршрутизатор может и не знать маршрутов ко всем другим сетям. Для обеспечения возможности полной маршрутизации общепринятой практикой является использование нескольких маршрутизаторов в качестве маршрутизаторов по умолчанию с одновременным указанием остальным маршрутизаторам путей по умолчанию к этим первым маршрутизаторам.

Маршрут по умолчанию устанавливается с помощью команды `ip default-network`, имеющей следующий синтаксис:

```
ip default-network network-number
```

где *network-number* — номер IP-сети или подсети, определенной в качестве пункта назначения по умолчанию.

Если в таблице маршрутизации отсутствует запись о сети пункта назначения, то пакет посылается в сеть по умолчанию. Сеть по умолчанию должна присутствовать в таблице маршрутизации. Наличие маршрутов по умолчанию позволяет иметь более короткие таблицы маршрутизации.

Применение номера сети по умолчанию осуществляется тогда, когда нужен маршрут, но при этом имеется только частичная информация о сети пункта назначения. Так как маршрутизатор не имеет полного знания обо всех сетях назначения, он может воспользоваться номером сети по умолчанию для указания направления, которому надо следовать в случае неизвестных

номеров сетей.

Пример маршрута по умолчанию

В примере, показанном на рис. 18.5, глобальная команда `ip default-network 192.168.17.0` задает пакетам, записи для которых отсутствуют в таблице маршрутизации, сеть класса С 192.168.17.0 в качестве пути до пункта назначения. Маршрутизатору А, возможно, нужен брандмауэр для пакетов актуализации маршрутной информации, так как администратору сети компании X не надо, чтобы из общественной сети приходили пакеты с обновлениями маршрутных данных. Также маршрутизатору А, вероятно, нужен механизм, который бы позволил сгруппировать сети, использующие стратегию маршрутизации, принятую в компании X. Одним из таких механизмов является номер автономной системы.

Автономная система состоит из маршрутизаторов, эксплуатируемых одним или несколькими операторами, которые представляют внешнему миру совместимую картину маршрутизации.

Сетевым информационным центром (Network Information Center) каждому предприятию назначается уникальный 16-разрядный номер автономной системы. И протокол маршрутизации, например протокол IGRP компании Cisco, требует задания в конфигурации этого уникального назначаемого номера автономной системы.

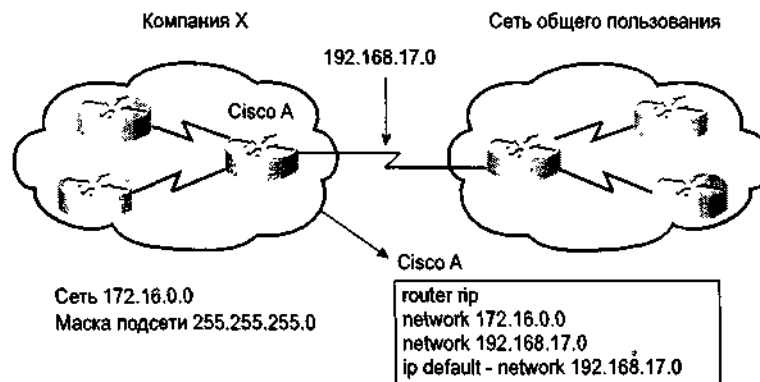


Рис. 18.5. Команда `ip default-network` указывает, куда посылаются пакеты, если маршрутизатор не знает, как добраться до пункта назначения

Протоколы внутренней или внешней маршрутизации

Как показано на рис. 18.6, протокол внешней маршрутизации, например протокол пограничного шлюза (Border Gateway Protocol, BGP), используется для связи между автономными системами. Протокол внутренней маршрутизации, например протокол RIP, используется внутри одной автономной системы.

На межсетевом уровне группы протоколов TCP/IP маршрутизатор для выполнения маршрутизации через реализацию конкретного алгоритма может использовать протокол IP-маршрутизации. Примерами протоколов IP-маршрутизации являются следующие.

- *Протокол маршрутной информации (RIP)* — протокол маршрутизации на основе вектора расстояния.
- *Протокол внутренней маршрутизации между шлюзами (IGRP)* — протокол маршрутизации на основе вектора расстояния разработки компании Cisco.

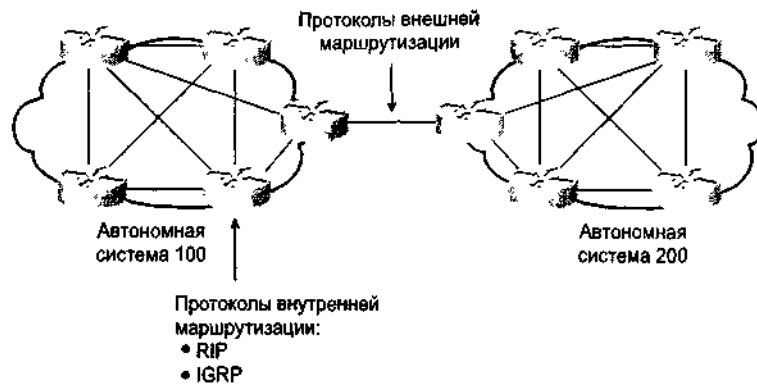


Рис. 18.6. Протоколы внешней маршрутизации используются для связи между автономными системами, а протоколы внутренней маршрутизации используются внутри одной автономной системы

- *Открытый протокол выбора первого кратчайшего пути (Open Shortest Path First, OSPF)* — протокол маршрутизации с учетом состояния канала связи.
- *Усовершенствованный протокол IGRP* — протокол сбалансированный гибридной маршрутизации.

В данной главе основное внимание уделяется первым двум из этих протоколов.

Задачи, связанные с конфигурированием IP-маршрутизации

Как показано на рис. 18.7, выбор протокола IP в качестве протокола маршрутизации связан с установкой как глобальных параметров, так и параметров интерфейсов.

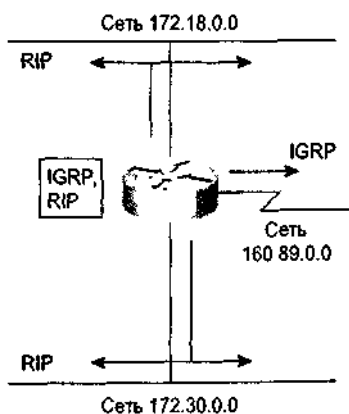


Рис. 18.7. При желании маршрутизатор может использовать несколько протоколов маршрутизации

Глобальные задачи включают:

- выбор протокола маршрутизации: RIP или IGRP.
- назначение номеров IP-сетей без задания значений номеров подсети.

Интерфейсная задача состоит в назначении сетевых/подсетевых адресов и соответствующей маски подсети.

Для общения с другими маршрутизаторами в процессе динамической маршрутизации используется широковещание и многоадресная рассылка. Метрика маршрутизации помогает маршрутизаторам находить наилучший путь к каждой сети или подсети.

Конфигурирование динамической маршрутизации

Для конфигурирования динамической маршрутизации используются две основные команды: `router` и `network`. Команда `router` запускает процесс маршрутизации, вводя исходное определение протокола IP-маршрутизации, и имеет следующую форму:

```
Router(config)# router protocol [keyword]
```

Затем для каждого процесса IP-маршрутизации необходима команда `network`:

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

Параметры задают следующее.

<i>Protocol</i>	Любой из протоколов RIP, IGRP, OSPF или усовершенствованный протокол IGRP
<i>network</i>	Например номер автономной системы, который используется с теми протоколами, которые требуют его наличия, скажем, протокол IGRP. Команда <code>network</code> необходима, так как она позволяет процессу маршрутизации определить интерфейсы, которые будут участвовать в отсылке и приеме пакетов актуализации маршрутной информации
<i>network-number</i>	Номер непосредственно подключенной сети

Номер сети должен основываться на номерах сетей, назначаемых Центром информации о сетях, а не на номерах подсетей или адресах отдельно взятых хост-машин.

Протокол RIP

Первоначально спецификация протокола RIP была изложена в документе RFC 1058. Ключевые характеристики протокола RIP:

- это протокол с маршрутизацией на основе вектора расстояния;
- в качестве метрики при выборе пути используется количество переходов (рис. 18.8);
- максимально допустимое количество переходов — 15;
- по умолчанию пакеты актуализации маршрутной информации посылаются в режиме широковещания каждые 30 секунд.

Выбор протокола RIP в качестве протокола маршрутизации осуществляется командой `router rip`:

```
Router(config)# router rip
```

Команда `network` назначает адрес сети, с которой маршрутизатор имеет непосредственное соединение. Этот адрес имеет в основе адрес, назначаемый Центром информации о сетях:

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

Процесс маршрутизации связывает интерфейсы с соответствующими адресами и начинает обработку пакетов в заданных сетях.

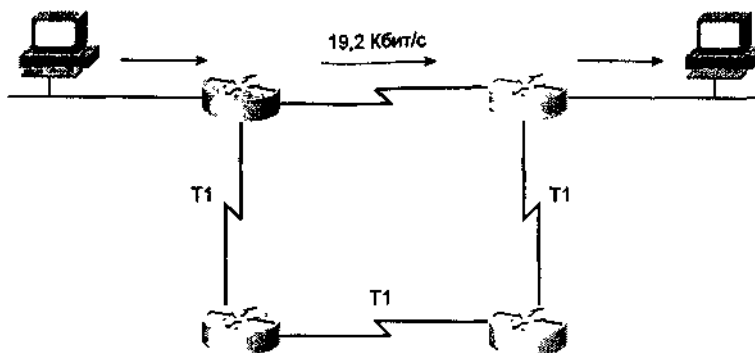


Рис. 18.8. Выбор пути осуществляется на основе значения количества переходов

Пример конфигурирования протокола RIP

В показанном на рис. 18.9 примере

- команда `router rip` определяет выбор протокола RIP в качестве протокола маршрутизации;
- команда `network 1.0.0.0` задает непосредственно подключенную сеть;
- команда `network 2.0.0.0` задает непосредственно подключенную сеть.

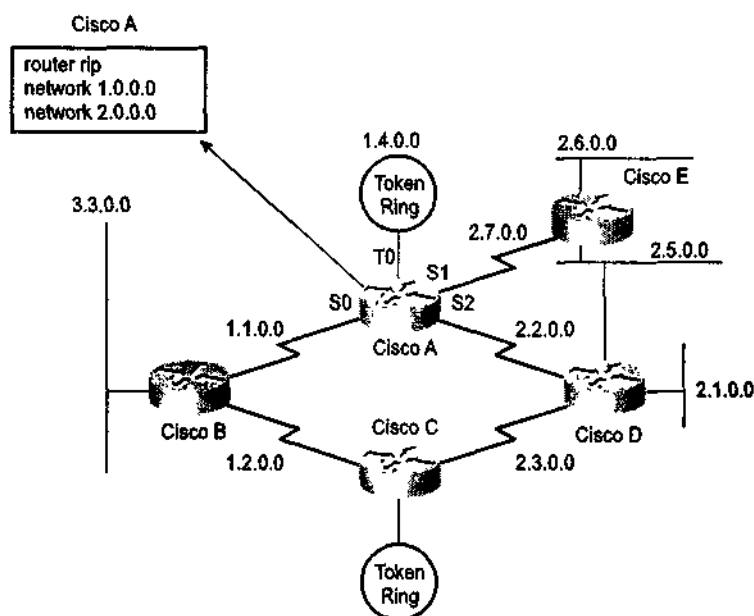


Рис. 18.9. Маршрутизатор Cisco A посылает информацию в сети 1.0.0.0 и 2.0.0.0

Интерфейсы маршрутизатора Cisco A, подключенные к сетям 1.0.0.0 и 2.0.0.0, посылают и принимают RIP-пакеты актуализации маршрутной информации. Эти пакеты позволяют маршрутизатору узнать топологию сети.

Мониторинг IP-маршрутизации

Для просмотра информации протокола RIP используется команда `show ip protocol`. Как показано в листинге 18.1, эта команда выводит значения таймеров процесса маршрутизации и сетевую информацию, имеющую отношение ко всему маршрутизатору.

Листинг 18.1. Команда `show ip protocol`, наблюдающая за поведением протокола RIP

```
Route > show ip protocol
Routing Protocol is rip
  Sending updates every 30 seconds, next due in 13 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  Outgoing update filter list fo all interface is not set
  Incoming update filter list fo all interface is not set
  Redistributing: rip
  Routing for Networks:
    183.8.0.0
    144.253.0.0
  Routing Information Sources:
  Gateway          Distance      Last Update
  183.8.128.12     120          0:00:14
  183.8.64.130     120          0:00:19
  183.8.128.130    120          0:00:03
Distance: (default is 120)
```

Эта информация может использоваться для идентификации маршрутизатора, подозреваемого в поставке плохой маршрутной информации.

Маршрутизатор посылает обновления таблицы маршрутной информации каждые 30 секунд. (Этот интервал является конфигурируемым.) Последний пакет актуализации был отослан 17 секунд назад, следующий будет послан через 13 секунд. Маршрутизатор поставляет маршруты для сетей, перечисленных в строке с заголовком `Routing for Networks`.

Вывод содержимого таблицы IP-маршрутизации

Как показано в листинге 18.2, содержимое таблицы IP-маршрутизации выводится командой `show ip route`. Таблица маршрутизации содержит записи обо всех известных сетях и подсетях и хранит код, указывающий на способ получения этой информации.

Листинг 18.2. Команда `show ip route`, показывающая содержание локальной таблицы маршрутизации

```
Route > show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area E1 - OSPF external
       type 1, E2 - OSPF external type 2, E-EGP i - IS-IS, LI - IS-IS level 1, L2 - IS-
       IS level 2 * - candidate default
Gateway of last resort is not set
  144.253.0.0 is subnetted (mask is 255.255.255.0), 1 subnets
C    144.253.100.0 is directly connected. Ethernet1
R    133.3.0.0
R    153.50.0.0 [120/1] via 183.8.128.12, 00:00:09, Ethernet0
    183.8.0.0 is subnetted (mask is 255.255.255.128), 4 subnets
R    183.8.0.128 [120/1] via 183.8.128.130.00, 00:00:17, Serial0
    [120/1] via 183.8.64.130, 00:00:17, Serial1
C    183.8.128.0 is directly connected, Ethernet0
C    183.8.64.128 is directly connected, Serial1
C    183.8.128.128 is directly connected, Ethernet0
R    192.3.63.0
```

Значения отражают следующее:

- `C` указывает сеть, внесенную в конфигурацию с помощью команды `network`;
- `R` указывает на запись, полученную через протокол RIP;
- `via` дает ссылку на маршрутизатор, который сообщил об этом маршруте;
- значение таймера `00:00:09` означает, что RIP-пакеты актуализации маршрутной

информации генерируются каждые 9 секунд;

- административное расстояние равно 120;
- количество переходов до маршрутизатора 153.50.0.0 равно 1.

Протокол IGRP

IGRP представляет собой протокол маршрутизации по вектору расстояния, который был разработан компанией Cisco. Этот протокол посылает пакеты актуализации маршрутной информации с 90-секундным интервалом, в которых содержатся сведения о сетях для конкретной автономной системы.

Ниже приведены некоторые ключевые характеристики протокола IGRP.

- Универсальность, позволяющая автоматически справляться с неопределенными сложными топологиями.
- Гибкость в работе с сегментами, имеющими различные характеристики по полосе пропускания и величине задержки.
- Масштабируемость вплоть до работоспособности в сверхбольших сетях.

Как показано на рис. 18.10, для определения сложной составной метрики протокол маршрутизации IGRP использует набор переменных. Используемая им метрика не имеет свойственного протоколу RIP ограничения по количеству переходов. Она включает следующие составляющие.

- Ширина полосы пропускания.
- Величина задержки.
- Уровень нагрузки.
- Надежность канала.
- Размер максимального блока передачи в канале.

Выбор протокола IGRP в качестве протокола маршрутизации осуществляется с помощью команды `router igrp`:

```
Router(config)# router igrp autonomous-system
```

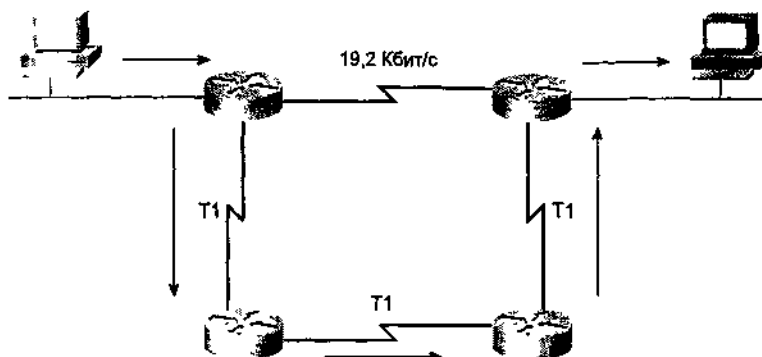


Рис. 18.10. В протоколе IGRP маршрутизация осуществляется на основе сложной составной метрики

где параметр задает следующее.

Autonomous-system

Идентифицирует маршрутизаторные IGRP-процессы, которые будут

коллективно использовать маршрутную информацию.

Команда `network` задает все непосредственно подсоединенные сети, подлежащие включению в таблицу маршрутизации:

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

где параметр определяет следующее:

`network-number` Задает непосредственно подключенную сеть, причем это номер, присвоенный. Центром информации о сетях, а не номер подсети или адрес отдельной хост-машины.

Пример конфигурирования протокола IGRP

В показанном на рис. 18.11 примере:

- команда `router igrp 109` выбирает для автономной системы 109 в качестве протокола маршрутизации протокол IGRP;
- команда `network 1.0.0.0` задает непосредственно подключенную сеть;
- команда `network 2.0.0.0` задает непосредственно подключенную сеть.

Для автономной системы 109 в качестве протокола маршрутизации выбран протокол IGRP. Все интерфейсы, подключенные к сетям 1.0.0.0 и 2.0.0.0, обрабатывают IP-трафик.

Команда `show ip protocol`

Как показано в листинге 18.3, команда `show ip protocol` выводит данные о параметрах, фильтрах и сетевую информацию, относящуюся ко всему маршрутизатору. В выводимом этой командой результате также показывается алгоритм протокола IGRP, используемый для вычисления метрик в процессе маршрутизации. Здесь показываются значения весов метрик K1—K5 и максимальное количество переходов.

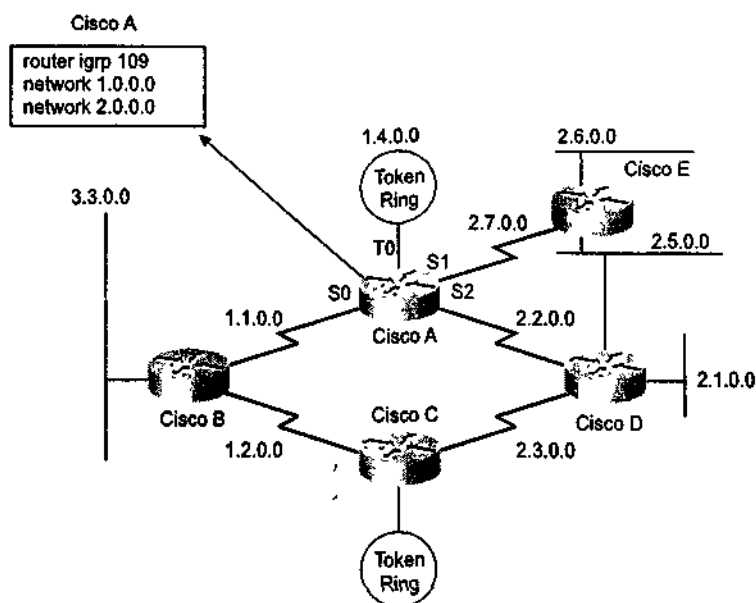


Рис. 18.11. Для создания IGRP-маршрутизатора используются команды `router igrp` и `network`

Листинг 18.3. Команда `show ip protocol`

```

Route > show ip protocol
Routing Protocol is igmp 300
  Sending updates every 90 seconds, next due in 55 seconds
  Invalid after 270 seconds, hold down 280, flushed after 360
  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
  IGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  IGRP maximum hopcount 100
  IGRP maximum metric variance 1
  Redistributing igmp 300
  Routing for Networks:
    183.8.0.0
    144.253.0.0
Routing Information Sources
Gateway                Distance            last Update
144.253.100.1          100                 0:00:52
183.8.128.12           100                 0:00:43
183.8.64.130           100                 0:01:02
  Distance: (default is 100)
-- More --

```

Команда show ip interface

Как показано в листинге 18.4, команда `show ip interface` выводит на экран данные о статусе и глобальные параметры, связанные с интерфейсом. ОС IOS автоматически вводит в таблицу маршрутизации маршрут через прямое подключение, если интерфейс таков, что программное обеспечение имеет возможность посылать и принимать через него пакеты. Такой интерфейс отмечается словом "up" (т.е. интерфейс в рабочем состоянии и активен. — *Прим. перев.*). Если интерфейс не может быть использован, то он удаляется из таблицы маршрутизации. Удаление записи позволяет реализовать резервные маршруты, если таковые существуют.

Листинг 18.4. Команда show ip interface

```

Route > show ip interfaces
Ethernet0 is up, line protocol is up
  Internet address is 183.8.128.2, subnet mask is 255.255.255.128
  Broadcast address is 255.255.255.255
  Address determined by non-volatile memory
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is enabled
  Outgoing access list is not set
  Inbound access list is not set
  Proxy ARP is enabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachable are always sent
  ICMP mask replies are never sent
  IP fast switching enabled
  IP fast switching on the same interface is disabled
  IP SSE switching is disabled
  Route Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  Probe proxy name replies are disabled
  — More —

```

Команда show ip route

Команда `show ip route`, как показано в листинге 18.5, выводит содержимое таблицы IP-маршрутизации. В таблице хранятся перечень всех известных сетей и подсетей, а также значения метрики, связанной с каждой записью. Следует отметить, что в приведенном примере информация поступала от протокола IGRP и из данных о прямых подключениях.

Листинг 18.5. Команда `show ip route`

```
Router> show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B -
BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       E1 - OSPF external type 1, E2 - OSPF external type 2, E-EGP i - IS-IS, LI - IS-IS
       level 1, L2 - IS-IS level 2 * - candidate default
Gateway of last resort is not set
144.253.0.0 is subnetted (mask is 255.255.255.0). 1 subnets
C 144.253.100.0 is directly connected, Ethernet1
I 133.3.0.0 [100/1200] via 144.253.100.200, 00:00:57, Ethernet1
I 153.50.0.0 [100/1200] via 183.8.128.12, 00:00:05, Ethernet0
 183.8.0.0 is subnetted (mask is 255.255.255.128), 4 subnets
I 183.8.0.128 [100/180 71] via 183.8.64.130, 00:00:27, Serial1 [100/180 71] via
 183.8.128.130, 00:00:27, Serial0
C 183.8.128.0 is directly connected, Ethernet0
C 183.8.64.128 is directly connected, Serial1
C 183.8.128.128 is directly connected, Serial0
I 172.16.0.0 [100/1200] via 144.253.100.1, 00:00:55, Ethernet1
I 192.3.63.0 [100/1300] via 144.253.100.200, 00:00:58, Ethernet1
```

Команда `debug ip rip`

Показанная в листинге 18.6 команда `debug ip rip` выводит содержание пакетов актуализации маршрутной информации протокола RIP в том виде, в каком эти данные посылаются и принимаются. В примере, приведенном ниже, пакет актуализации был отослан адресатом 183.8.128.130. В нем содержатся сведения о трех маршрутизаторах, причем один из них недостижим, так как количество переходов до него превышает 15. Затем пакеты актуализации отсылались в режиме широковещания через адрес 183.8.128.2.

Листинг 8.6. Команда `debug ip rip`

```
Router# debug ip rip
RIP Protocol debugging is on
Routerft
RIP: received update from 183.8.128.130 on Serial0
 183.8.0.128 in 1 hops
 183.8.64.128 in 1 hops
 0.0.0.0 in 1 hops (inaccessible)
RIP: received update from 183.8.64.140 on Serial1
 183.8.0.128 in 1 hops
 183.9.128.128 in 1 hops
 0.0.0.0 in 1 hops (inaccessible)
RIP: received update from 183.8.128.130 on Serial0
 183.8.0.128 in 1 hops
 183.8.64.128 in 1 hops
 0.0.0.0 in 1 hops (inaccessible)
RIP: sending update to 255.255.255.255 via Ethernet0 (183.8.128.2)
 subnet 183.8.0.128, metric 2
 subnet 183.8.64.128, metric 1
 subnet 183.8.128.128, metric 1
 default 0.0.0.0, metric 1
 network 144.253.0.0, metric 1
RIP: sending update to 255.255.255.255 via Ethernet1 (144.253.100.202)
 default 0.0.0.0, metric 16
 network 153.50.0.0, metric 2
```

```
network 183.8.0.0, metric 1
```

Резюме

- Первоначально маршрутизатор должен обращаться к записям о сетях или подсетях, подключенных непосредственно.
- Маршрутизаторы узнают о путях к пунктам назначения тремя различными способами:
- через статические маршруты;
- через маршруты по умолчанию;
- через динамические маршруты.
- Команда `ip route` устанавливает статический маршрут.
- Команда `ip default-network` устанавливает маршрут по умолчанию.
- Маршрутизаторы могут быть сконфигурированы на использование сразу нескольких протоколов IP-маршрутизации, например протоколов RIP и IGRP.

Контрольные вопросы

1. К какому типу записей маршрутизатор обращается первоначально?
 - A. К записям о сетях и подсетях, подключенных непосредственно.
 - B. К записям, полученным им от ОС IOS.
 - C. К записям с известной информацией об IP-адресе и маске.
 - D. К записям, которые были получены от других маршрутизаторов.
2. Что из приведенного ниже наилучшим образом описывает статический маршрут?
 - A. Запись в таблице маршрутизации, которая используется для направления кадров, следующий переход для которых не имеет явного отражения в таблице маршрутизации.
 - B. Маршрут, который в явном виде конфигурируется и вводится в таблицу маршрутизации и имеет преимущество над маршрутами, выбранными протоколами динамической маршрутизации.
 - C. Маршрут, который автоматически подстраивается под топологию сети или изменения в трафике.
 - D. Маршрут, который принудительно подстраивается для направления кадров внутри топологии сети.
3. Что из приведенного ниже наилучшим образом описывает маршрут по умолчанию?
 - A. Запись в таблице маршрутизации, которая используется для направления кадров, следующий переход для которых не имеет явного отражения в таблице маршрутизации.
 - B. Маршрут, который в явном виде конфигурируется и вводится в таблицу маршрутизации.
 - C. Маршрут, который автоматически подстраивается под топологию сети или изменения в трафике.
 - D. Маршрут, который принудительно подстраивается для направления кадров внутри топологии сети.
4. Для чего используются протоколы внешней маршрутизации?
 - A. Для осуществления передачи между узлами сети.
 - B. Для доставки информации в рамках одной автономной системы.
 - C. Для обмена информацией между автономными системами.
 - D. Для установки инфраструктуры, совместимой между сетями.
5. Для чего используются протоколы внутренней маршрутизации?
 - A. Для установки инфраструктуры, совместимой между сетями.
 - B. Для обмена информацией между автономными системами.
 - C. Для осуществления передачи между узлами сети.
 - D. Используются внутри одной автономной системы.
6. Что из приведенного ниже относится к задачам глобального конфигурирования?
 - A. Назначение сетевых IP-адресов путем задания значений номеров подсетей.
 - B. Выбор протокола маршрутизации: RIP или IGRP.
 - C. Назначение сетевых/подсетевых адресов и соответствующей маски подсети.
 - D. Установка значения метрики маршрутизации для нахождения наилучшего пути к каждой сети.
7. Какую метрику использует протокол RIP для определения наилучшего пути, которым должно следовать сообщение?
 - A. Полоса пропускания.
 - B. Количество переходов.
 - C. Изменяется для каждого сообщения.
 - D. Административное расстояние.
8. Есть подозрение, что один из маршрутизаторов в сети посылает плохую маршрутную информацию. Какую команду можно использовать для проверки?
 - A. Router(config)# show ip protocol.
 - B. Router# show ip protocol.

- C. Router> show ip protocol.
 - D. Router(config-router)# show ip protocol.
9. Для чего выводится содержимое таблицы IP-маршрутизации?
- A. Для установки плана обновления информации в маршрутизаторе.
 - B. Для идентификации пар значений адресов сетей назначений и количества переходов.
 - C. Для прослеживания путей поступления дейтаграмм.
 - D. Для установки значений параметров и фильтров в маршрутизаторе.
10. Если необходимо узнать, на работу с каким протоколом маршрутизации сконфигурирован маршрутизатор, то какую команду следует использовать?
- A. Router> **show router protocol.**
 - B. Router(config)> **show ip protocol.**
 - C. Router(config)# **show router protocol.**
 - D. Router> **show ip protocol.**

Глава 19

Управление сетью

В этой главе.

- Назначение ревизий различных типов
- Цель создания карты сети
- Программные средства для управления сетью и их функции
- Характеристики и функции протоколов SNMP и CMIP
- Некоторые методы устранения неполадок в сети
- Цель выполнения оценки производительности сети

Введение

В этой книге до сих пор говорилось о том, как проектировать и создавать сети. Рассказывалось о том, как выбирать, прокладывать и тестировать кабель, как определять месторасположение помещений для коммутационного оборудования. Однако проектирование сети и ее практическая реализация являются только частью того, что необходимо знать. Также необходимо знать о техническом сопровождении сети и сохранении ее работоспособности на приемлемом уровне. Это означает, что администратор должен знать о способах устранения неисправностей при их возникновении. Кроме того, администратору необходимо знать, когда следует расширить или изменить конфигурацию сети, чтобы подогнать ее под изменившиеся требования, которые на нее возлагаются. В данной главе рассказывается об управлении сетью с помощью таких методик, как документирование, аудит, мониторинг функционирования и оценка производительности.

Первые шаги в управлении сетью

Может показаться, что после того, как сеть установлена и работает, можно расслабиться. Но опытный администратор знает, что это совершенно неправильный подход. Прежде всего необходимо задокументировать сеть. Далее, точное знание о предположительных характеристиках работы сети значительно облегчит работу в случае возникновения проблем. Поэтому, вместо того, чтобы расслабляться, необходимо воспользоваться нормальной работой сети и выполнить комплексную проверку. Фактически необходимо сделать пять различных ревизий сети: инвентаризационную, установленного оборудования, эксплуатации, эффективности и средств защиты сети. Все эти пять типов ревизий описываются в данной главе. Инвентаризационную ревизию и ревизию установленного оборудования можно начать сразу. Информация для эксплуатационной ревизии и ревизий эффективности и средств защиты сети может и должна быть получена после начала функционирования сети, поскольку эти ревизии требуют данных, которые могут быть обеспечены только посредством мониторинга и анализа поведения и производительности сети.

Инвентаризационная ревизия

Инвентаризационная ревизия позволяет инвентаризовать все сетевое оборудование и программное обеспечение. В идеале эта информация должна быть получена в момент закупки аппаратуры и программного обеспечения еще до их установки. Это сэкономит время и усилия и снизит количество неудобств, которые будут испытывать пользователи сети.

Инвентаризационная ревизия сетевого оборудования должна включать сбор данных о серийных номерах устройств, их типе и фамилиях лиц, которые используют каждую конкретную единицу оборудования. Она также предусматривает составление перечня установок на различных рабочих станциях и сетевых устройствах. Некоторые администраторы считают полезным держать инвентаризационную информацию непосредственно прикрепленной к каждому сетевому устройству. Другие предпочитают хранить ее в письменном виде или в компьютеризированной базе данных, где она легко доступна для персонала технической поддержки.

Инвентаризационная ревизия прикладного программного обеспечения должна включать сбор данных о типах используемого программного обеспечения, количестве пользователей каждого приложения и эксплуатационных требованиях к каждому из приложений. Во время выполнения инвентаризационной ревизии также необходимо удостовериться, что количество пользователей каждого приложения не превосходит количества лицензий, которым располагает данная рабочая площадка.

Ревизия установленного оборудования

Ревизия установленного оборудования позволяет зафиксировать, где все находится. Она должна включать учет проложенных кабелей, рабочие станции, принтеры и устройства межсетевого взаимодействия (такие как концентраторы, мосты и маршрутизаторы). Короче говоря, она должна в конечном итоге дать подробную информацию о местонахождении всех составляющих элементов сети. В идеале вся эта информация должна быть внесена в рабочую версию документа с названием *карта нарезки* еще во время монтажа сети. После завершения этой ревизии самое время перенести нанесенные на карты нарезки данные на комплект чертежей здания.

Карта сети

После завершения инвентаризационной ревизии и ревизии установленного оборудования необходимо воспользоваться собранной информацией и составить *карту сети*, которая по внешнему виду похожа на чертеж. Карта должна включать данные о физическом местонахождении и схеме размещения всех устройств, включенных в сеть, и выполняемых на них приложениях. Она также должна включать IP- и MAC-адреса каждого устройства. Наконец, карта сети должна содержать сведения о длине каждого отрезка кабеля между узлами сети. Законченная карта сети должна храниться рядом с рабочим местом, выбранным для администрирования и мониторинга сети.

Когда программы мониторинга и устройства сообщают о проблеме с какими-либо физическими компонентами сети, часто они указывают место проблемы, например обрыва или короткого замыкания, путем предоставления информации о расстоянии между точкой возникновения проблемы и местом расположения контролирующего устройства. В других случаях программа мониторинга сообщает адрес устройства (или устройств), где возникла проблема. Совершенно очевидно, что локализация и решение проблемы существенно облегчаются, если информация, показанная на рис. 19.1, готова и находится под рукой.

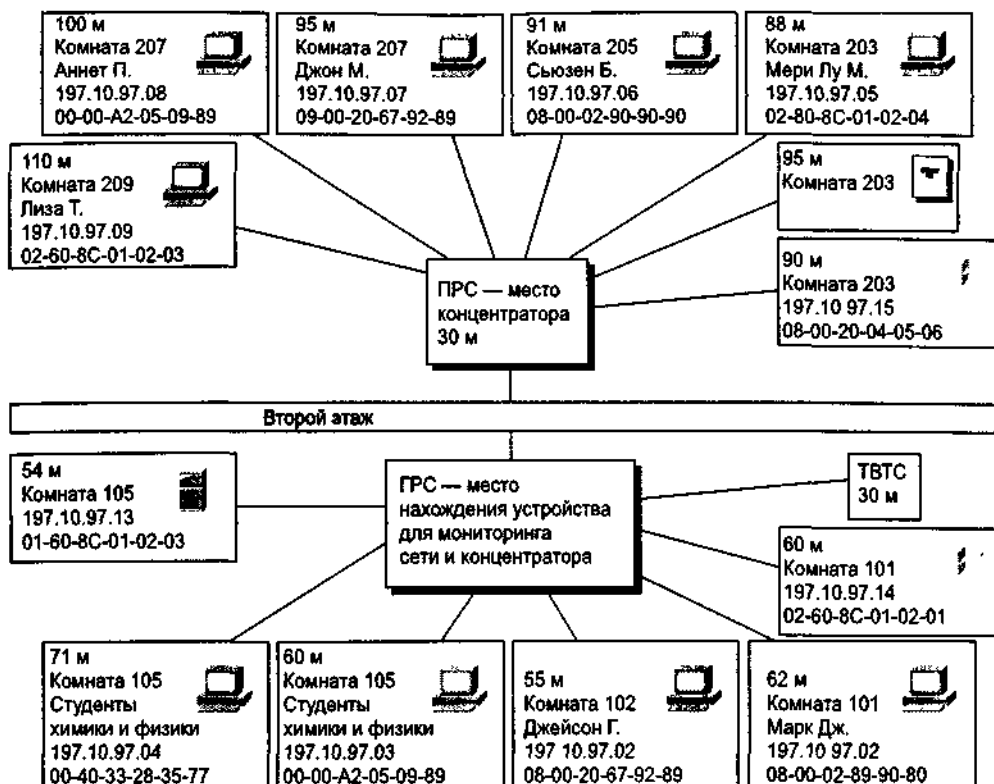


Рис. 19.1. Информация о сети должна включать адрес устройства (или устройств), где может возникнуть проблема

Инвентаризационная ревизия и ревизия установленного оборудования должны быть сделаны как можно быстрее — до того, как сеть начнет предоставлять услуги клиентам. Наличие под рукой предоставляемой этими ревизиями информации позволит при возникновении проблем устранить их быстрее и эффективнее.

Ревизия эксплуатации

Ревизия эксплуатации позволяет наблюдать за повседневной работой сети. Она требует применения специализированного программного обеспечения и аппаратуры. Кроме устройства, осуществляющего мониторинг сети, в ходе ревизии эксплуатации могут потребоваться и такие устройства, как анализатор сети, измеритель отраженного сигнала, разветвительные коробки, измерители мощности и генератор. Устройства, подобные мониторам сети, и анализаторы используют для выполнения своих функций специализированное программное обеспечение.

Все это оборудование и программное обеспечение позволяют администратору сети отслеживать сетевой трафик путем пересчета количества посланных пакетов, повторно переданных пакетов, а также определять размер пакетов и уровень загруженности сети. Проще говоря, эти устройства и программное обеспечение, которым они пользуются, позволяют обнаруживать такие события, как возникновение короткого замыкания и разрывов в кабеле, шум в сетевой среде передачи данных и узкие места в сети.

Из всех упомянутых здесь аппаратных средств управления для получения информации, требующейся при выполнении ревизии эксплуатации, ревизии эффективности и ревизии средств защиты, наиболее часто используются сетевые мониторы и анализаторы. Ниже в данной главе эти два типа устройств будут рассмотрены более подробно. Сейчас же достаточно сказать, что обычно они размещаются на центральной площадке, где легко доступны для персонала службы технической поддержки.

Программные средства для управления сетью

Производители поставляют на рынок большое количество разнообразного программного обеспечения для управления сетями. Эти инструментальные средства позволяют наблюдать за поведением узлов сети, контролировать уровень сетевого трафика, следить за узкими местами в сети, вести записи результатов измерений и собирать диагностическую информацию. Большинство из этих прикладных программ поддерживает специфические для производителя типы информации и работает с использованием одного из двух протоколов управления сетью: простого протокола управления сетью (Simple Network Management Protocol, SNMP) и протокола общей управляющей информации (Common Management Information, CMIP). Оба этих протокола передачи управляющей информации используют концепцию так называемой базы данных информации управления сетью (Management Information Base, MIB). Если говорить проще, то в такой базе данных содержится информация, тесты, уравнения и управляющие воздействия, которым подчиняются все ресурсы, находящиеся в сети. Хотя протоколы SNMP и CMIP выполняют одинаковую задачу и используют концепцию базы данных MIB, их методы получения информации о сети сильно разнятся. В некоторых случаях это даже может определять выбор типа протокола для мониторинга состояния сети.

Протокол SNMP

Протокол SNMP, выпущенный в 1988 году министерством обороны США и разработчиками протокола TCP/IP, является наиболее используемым и хорошо известным программным средством для управления сетью.

Для получения информации о сети протокол SNMP использует методику, называемую

сбором MIB-данных. Это означает, что он, переходя от одного сетевого устройства к другому, опрашивает каждого из них о его состоянии. Затем, как показано на рис. 19.2, выполняется копирование информации о состоянии каждого устройства, а также локальной базы данных MIB каждого устройства.

Одним из преимуществ протокола SNMP является то, что устройства в сети не обязательно должны быть достаточно "интеллектуальными", чтобы сообщать о возникновении проблемы. Об этом заботится за них сам процесс опроса протокола SNMP. Однако в больших сетях, к которым подключено большое количество устройств и ресурсов, метод опроса протокола SNMP может стать недостатком, поскольку дает существенный вклад в трафик. А это может реально замедлить работу сети.

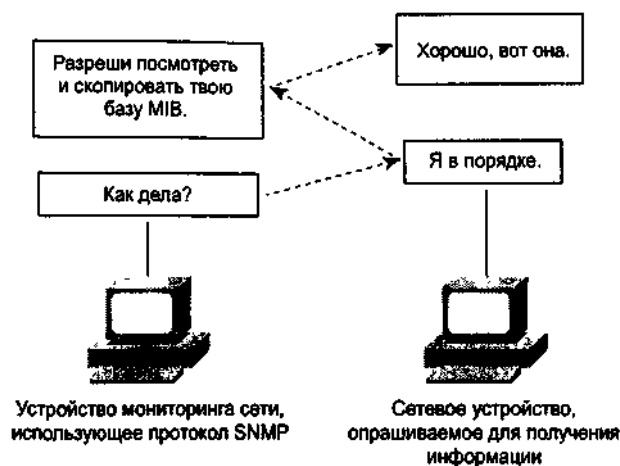


Рис. 19.2. Для получения информации о сети путем опроса сетевых устройств протокол SNMP использует методику сбора MIB-данных

Протокол CMIP

Протокол CMIP был разработан Международной организацией по стандартизации (ISO). В настоящее время этот протокол используется не так широко, как протокол SNMP, особенно во вновь создаваемых сетях. Для получения информации о сети протокол CMIP использует так называемую методику *доклада MIB-данных*. При использовании этой техники, как показано на рис. 19.3, центральная рабочая станция мониторинга ожидает от устройств доклада об их текущем состоянии.

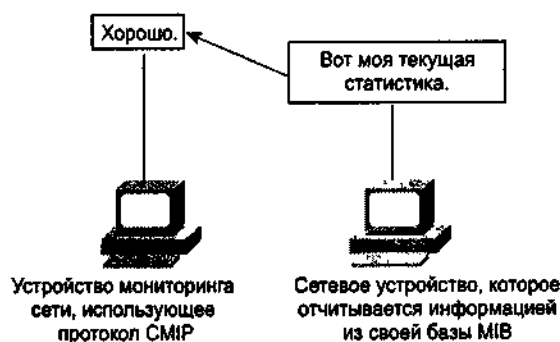


Рис. 19.3. Если объем трафика является предметом беспокойства, то протокол CMIP может быть полезным инструментом для управления в такой сети

Мониторинг сети

Каждодневный контроль работы сети позволяет установить, что для нее является нормальным состоянием. Например, отслеживая информацию за период времени, можно узнать, насколько в среднем загружена сеть. Также администратор может выяснить, в какое время суток, день недели и месяца трафик достигает своего пика. Можно определить наиболее и наименее популярные приложения в сети и как они используются. В некоторых случаях можно даже идентифицировать тех пользователей, которые чаще всего сталкиваются с проблемами при работе в сети. Вся эта информация должна храниться в соответствующих журналах. Позднее, когда администратор заметит что-либо, что, возможно, является проблемой, он сможет сравнить ее с этой информацией базового уровня, которая показывает, какой должна быть нормальная работа сети.

Ревизия эффективности

Ревизия эффективности позволяет определить, работает ли сеть в соответствии со своими потенциальными возможностями. Как и ревизию эксплуатации, эту ревизию лучше всего выполнять после того, как сеть начала предоставлять услуги своим клиентам.

Что до кабельной системы сети, то набор опорных измерений, удовлетворяющих стандартам Института инженеров по электротехнике и электронике (IEEE) и/или Ассоциации электронной промышленности/Ассоциации телекоммуникационной промышленности США (EIA/TIA), должна предоставить та организация, которая выполняла установку сети. Чтобы иметь уверенность в том, что кабельная система продолжает работать эффективно, необходимо периодически проводить соответствующие измерения и сравнивать их результаты с этими базовыми данными.

К другим показателям, которые должны быть включены в ревизию эффективности, относятся стоимостной анализ сети, анализ легкости, с которой сеть способна давать информацию, анализ способности сети обеспечивать целостность данных, а также оценка количества персонала для поддержки сети. Наконец, ревизия эффективности должна включать и оценку того, как клиенты сети умеют пользоваться программными и аппаратными ресурсами сети.

Ревизия средств защиты

Ревизия средств защиты сети предусматривает просмотр требований по защите данных в сети и определение аппаратных и программных защитных систем, которые в наибольшей степени удовлетворяют им. Предоставить информацию, необходимую для выполнения этой ревизии, может только наблюдение и практика того, как сеть и ее клиенты используют данные и обращаются за ними.

Информация, которая должна собираться при выполнении ревизии этого типа, включает список сегментов, требующих ограниченного доступа или шифрования данных, перечень устройств, файлов и каталогов, требующих блокирования или защиты паролями, данные о файлах, архивные резервные копии которых должны создаваться, анализ необходимой частоты выполнения процедур резервного копирования, тип используемой защиты от вирусов и, что наиболее важно, сведения о тех процедурах, которые будут использоваться в сети в случае возникновения аварийных ситуаций и катастрофических отказов.

Если у вас нет точного представления о той информации, которая должна быть собрана в ходе той или иной ревизии, то следует проконсультироваться с другими сетевыми администраторами и узнать у них, как они проводят ревизии своих сетей и какие типы инструментальных средств управления сетью они находят наиболее пригодными для выполнения подобных задач. Можно также связаться с поставщиками сетевой операционной системы, которые смогут порекомендовать подходящее программное обеспечение для аудита сети, которое само проведет по процессу организации адекватной защиты сети и поможет выполнить полный мониторинг и анализ сети.

Сетевые анализаторы

Для выполнения исследований можно включить в сеть сетевой анализатор. Называемое также анализатором протокола, это устройство, во многом так же, как монитор сети, отслеживает статистическую информацию о работе сети. Однако по сравнению с ним обеспечивает более высокий уровень возможностей. Фактически эти устройства настолько сложны и "интеллектуальны", что не только обнаруживают и идентифицируют проблемы, например узкие места, но и решают их.

Решение проблем в сети

Ключом к успешному решению проблем в сети является информация. Есть общее правило: чем больше информации, тем легче решать проблемы. Информация, собранная при проведении ревизий, обеспечит тот набор измерений базового уровня, с которыми можно будет сравнивать текущие данные в процессе детализации проблемы. После возникновения проблемы должна быть собрана дополнительная информация. И точно так же, как в случае информации, полученной во время выполнения ревизий, эта новая информация должна регистрироваться и документироваться, равно как и любое предложенное решение. Наличие подобного журнала очень важно, так как он регистрирует ваш вклад в систему. Позднее он может быть использован для обоснования запросов на дополнительное оборудование, персонал и обучение. Задокументированные в журнале проблемы и решения могут быть полезным инструментом для обучения новых специалистов по поиску и устранению неполадок в сети. Такой журнал также позволит проследить тенденции, что поможет предвидеть проблемы и предлагать решения как в отношении конкретных ситуаций, так и в отношении людей.

Документирование проблем в сети

Некоторые проблемы в сети будут выявляться сетевым администратором с помощью программных и аппаратных средств управления сетью. О других персонал технической поддержки сети будет узнавать из сообщений клиентов сети. Все запросы клиентов о помощи должны документироваться в виде отчета о неисправности. Регистрируемая в каждом отчете о неисправности информация должна быть разделена на пять общих категорий.

В первую категорию входит идентификационный номер, присваиваемый запросу. Он будет полезен для ведения картотеки информации или ввода ее в базу данных.

Вторая категория включает предварительную информацию. Сюда должны входить сведения о фамилии лица, сообщившего о проблеме, времени поступления сообщения о проблеме, методе его поступления, наличии связи этой проблемы с предыдущими сообщениями о неисправностях с указанием их идентификационных номеров, месте, где проблема возникла, может ли быть проблема воспроизведена для персонала технической поддержки, времени первого проявления проблемы, было ли что-либо сделано по-другому или изменено непосредственно перед возникновением проблемы и носит ли проблема периодический или устойчивый характер.

К третьей категории относится информация, собранная персоналом технической поддержки на месте возникновения проблемы. Она должна включать комментарии персонала технической поддержки относительно таких параметров окружающей среды ПК, как качество электропитания, температура, влажность и т.п., замечания персонала технической поддержки о наблюдении проблемы или возникших сложностях, а также перечень действий, предпринятых для исправления проблемы.

Четвертая категория должна включать информацию о том, был ли ПК передан в ремонт для дальнейшего обслуживания, список всех выполненных операций и результат этих действий.

Последняя категория, которая должна быть в отчете о неисправности — это резюме. Резюме должно содержать вывод о том, была ли проблема связана с аппаратурой, программным

обеспечением или пользователем: если проблема была связана с программным обеспечением, то должно быть указано, с каким именно, если проблема была связана с аппаратурой, то должно быть указано, с какой именно.

Анализ и решение проблем в сети

После того как будет собрана вся доступная информация о проблеме, необходимо составить список возможных причин. Основываясь на имеющейся истории работы сети, можно расставить приоритетность этих причин от наиболее вероятных до наименее вероятных. При выполнении такой расстановки приоритетов очень помогает, если держать в уме направления потоков данных в сети. Используя этот перечень возможностей, можно с помощью средств управления сетью идентифицировать причину проблемы.

Успешный поиск и устранение проблем в сети возможны и в том случае, если имеющийся набор типов инструментальных средств для управления сетью ограничен. Хотя в таких обстоятельствах вместо ориентации на такие средства управления сетью, как мониторы и анализаторы, придется воспользоваться *методом замены*.

Чтобы понять, как работает метод замены при возникновении проблемы, предположим, что есть один работоспособный объект и один нефункционирующий. Например, если собранная информация приводит к заключению, что проблема лежит в конкретной рабочей станции, то необходимо иметь другую такую же рабочую станцию, но заведомо работоспособную.

Начинать надо с самого нижнего уровня — с кабельной системы. Перекоммутируйте шнуры с одной машины на другую. Если сбоящая машина начнет работать правильно, а исправная начнет давать сбои, то проблема найдена с первой попытки. Если со сбоящим устройством не произошло никаких изменений, то необходимо восстановить исходное подключение шнуров и перейти на следующий уровень. Продолжайте перекоммутацию компонентов до тех пор, пока сбоящее устройство не начнет работать, а исправное не перестанет функционировать. Но следует быть готовым к тому, что метод замены может потребовать для устранения проблемы значительных затрат времени.

Если перепробовано все, но решения проблемы по-прежнему нет, то не надо упускать из виду очевидного. Частью проблемы может быть нехватка знаний, опыта или отсутствие соответствующих средств управления. Придя к этому заключению, необходимо без колебаний звонить экспертам. В долгосрочной перспективе вооруженные мощными средствами диагностики и управления, обладающие большими знаниями и опытом консультанты сэкономят вам и вашей организации время, деньги и усилия. Кроме того, в процессе своей работы они могут дать вам ценную возможность обучения.

Ключом к успешному устранению проблем в сети является их изоляция путем планомерного следования простой иерархии процедур по устранению неполадок.

Процедуры устранения неполадок

Приобретая опыт в работе с сетью и клиентами, вы со временем разработаете подходящую для себя иерархию процедур по устранению неполадок. А до тех пор может оказаться полезным выполнение следующих рекомендаций.

В большинстве сетей обычно пользователи, а не аппаратура или программное обеспечение, ответственны за так называемые проблемы в сети. Поэтому логичным первым шагом в решении выявленной пользователем проблемы является работа с самим пользователем.

Если определено, что проблема не является результатом действий пользователя, тогда следует перейти к следующему наиболее часто встречающемуся источнику проблем — аппаратуре. Начинать нужно с проверки наличия необходимых для диагностики проблемы инструментальных средств. Затем необходимо определить, является ли проблема локальной по отношению к устройству. При необходимости переставьте ПК на заведомо работающий сетевой вход, а его замените переносным компьютером. Если окажется, что проблема носит не

локальный характер, то следует сосредоточиться на сетевом оборудовании. Определить, связана ли проблема с конкретным сегментом сети, поможет протокол SNMP. Первым делом необходимо посмотреть сетевую разводку. Следует проверить, не было ли недавно сделано каких-либо изменений в кабельном хозяйстве. Тут необходимо воспользоваться средствами диагностики, например измерителем отраженных сигналов. Проверьте все соединения кабелей в отказавшем сегменте, начните с рабочей зоны и двигайтесь к помещению для коммутационного оборудования. Если кабельное хозяйство и все соединения исправны, тогда следует проверить сетевые файл-серверы. Если таких серверов несколько, следует попытаться определить, какой из них является наиболее вероятным источником проблемы. Если вы полагаете, что проблема связана с рабочей станцией, проверьте коммутационную панель, кабель, разъем и память рабочей станции. В процессе диагностирования и решения проблемы не пренебрегайте любыми диагностическими утилитами, встроенными в плату сетевого интерфейса устройства. Если сетевое оборудование исключено как источник проблемы, то тогда, следуя соответствующим процедурам диагностики, переходите к проверке и устранению проблем программного обеспечения.

Оценки производительности сети

Периодическое выполнение оценок работы сети является важным инструментом в техническом сопровождении и профилактике отказов, гарантирующим, что сеть продолжает работать на приемлемом уровне. Первая оценка должна быть сделана после того, как сеть поработает разумный промежуток времени. Она должна основываться на информации, получаемой с помощью системных средств управления сетью. Собранные результаты оценки должны быть оформлены в виде документа, называемого *отчетом о проведении оценки*, который позволит персоналу, ответственному за управление сетью, увидеть, продолжает ли сеть работать так, как прогнозировалось и как требуется для организации. Целью создания отчета о проведении оценки является выявление сильных и слабых сторон сети, которые при необходимости можно будет исправить.

Например, в журналах, которые ведет анализатор сети, может быть отображена тенденция к замедлению трафика в определенных сегментах сети. Проведение новой ревизии аппаратных и программных средств может выявить добавление в этих сегментах нескольких новых сетевых устройств, выполняющих мультимедийные приложения. Если объединить эти оба набора данных в отчете о проведении оценки, то для персонала, отвечающего за управление сетью, такая информация может послужить основой для формулирования изменений в системе и ее работе.

Процедуры выполнения изменений в сети

Администратор сети должен помнить, что все организации изменяются и растут. Как следствие, сеть, которая была установлена всего год назад, может уже не удовлетворять требованиям и потребностям организации. С изменением и развитием организации то же самое должно происходить и с сетью.

Если сетевой администратор полагает, что в сети должны быть сделаны изменения, особенно такие, которые поменяют способ взаимодействия пользователей с сетью, набор услуг, предоставляемых сетью, доступ к информации в приложениях, выполняемых в сети, или такие, которые будут связаны с дополнительными затратами времени, материальных и трудовых ресурсов, то ему необходимо подготовить проект *технических требований на изменения*. Этот документ должен будет пройти круг согласований.

Состав людей, участвующих в согласовании технических требований на изменения, разный в различных организациях. В идеале в состав лиц, участвующих в согласовании, должны входить сотрудники организации, которые не только обладают достаточными техническими знаниями, но и знакомы с типами услуг, приложений и производственными операциями, с которыми имеет дело организация.

В некоторых случаях эти технические требования могут послужить спусковым механизмом появления откликов от рецензентов. Обычно содержание таких откликов лежит в диапазоне от краткого анализа до широкого исследования с глубоким анализом. Иногда подобные исследования могут приводить к возврату в более раннюю точку цикла жизни сети. Другими словами, они могут потребовать полного перепроектирования сети. Если проблемы, которые показаны в отчете по проведению оценки, серьезны и имеют достаточно далеко идущие последствия, то это может даже означать возврат к стадии изучения. Короче говоря, технические требования на изменения могут привести к значительной модификации сети.

Резюме

- Первым шагом в управлении сетью является ее документирование.
- Для документирования сети должны быть проведены следующие ревизии.
- Инвентаризационная ревизия и ревизия установленного оборудования, которые могут помочь при устранении проблем в сети.
- Ревизия эксплуатации, которая путем использования специализированных аппаратных и программных средств позволяет увидеть каждодневные операции, выполняемые в сети.
- Ревизия средств защиты, в ходе которой просматриваются требования к защите сети и определяются типы программных и аппаратных систем защиты, которые наилучшим образом им удовлетворяют.
- Ревизия эффективности, которая позволяет определить, что сеть работает в соответствии со своим потенциалом.
- Ревизии необходимы для установки той базовой линии производительности, с которой можно сравнивать текущие показатели.
- При устранении проблем, особенно выявленных клиентами, может быть полезным использование заранее продуманных процедур и вопросов.
- Периодическое выполнение оценок работы сети является важным инструментом в техническом сопровождении и профилактике отказов, гарантирующим, что сеть продолжает работать на приемлемом уровне.
- Информация, собранная при выполнении оценки производительности сети, используется для подготовки соответствующего отчета, который становится основой технических требований на изменения.

Контрольные вопросы

1. Какова цель инвентаризационной ревизии?
 - A. Идентификация местонахождения каждого элемента сети.
 - B. Мониторинг и анализ работы сети.
 - C. Сбор технических спецификаций поставщиков на каждый элемент сети.
 - D. Составление инвентаризационной описи всего программного и аппаратного обеспечения, используемого в сети.
2. Какова цель ревизии установленного оборудования?
 - A. Идентификация типов оборудования и устройств, сети.
 - B. Идентификация местонахождения каждого элемента сети.
 - C. Мониторинг и анализ работы сети.
 - D. Перенос информации на чертежи здания для создания карты нарезки.
3. Каким образом карта сети помогает локализовать место возникновения проблемы с физическим элементом сети?
 - A. Предоставляет имя пользователя проблемного устройства.
 - B. Предоставляет информацию об установках на проблемном устройстве.
 - C. Предоставляет данные об эксплуатационных требованиях приложений, используемых на проблемном устройстве.
 - D. Предоставляет информацию об адресах проблемного устройства.
4. Что из приведенного ниже правильно описывает протокол SNMP?
 - A. Редко используется во вновь создаваемых сетях.
 - B. Входит в стандарт протокола TCP/IP.
 - C. Использует концепцию, известную под названием MIB.
 - D. Является лучшим выбором для сетей с высоким объемом трафика.
5. Что из приведенного ниже правильно описывает работу протокола CMIP?
 - A. Использует метод опроса баз данных MIB.
 - B. Предусматривает наличие центральной рабочей станции мониторинга, которая ожидает от устройств сообщений об их текущем состоянии.
 - C. Копирует локальную базу данных MIB каждого устройства.
 - D. Способ, которым он получает информацию от устройств, дает значительный вклад в трафик сети.
6. Какова цель ревизии эффективности?
 - A. Мониторинг и анализ работы сети.
 - B. Определение того, работает ли сеть в соответствии со своим потенциалом.
 - C. Идентификация типов оборудования и устройств, сети.
 - D. Обеспечение информации о восстановлении после сбоя или катастрофического отказа.
7. Какова цель ревизии средств защиты сети?
 - A. Согласование требований по защите сети со строительными нормами и нормами секретности.
 - B. Оценка способностей клиентов пользоваться сетевым оборудованием и программным обеспечением.
 - C. Выяснение способности сети гарантировать целостность данных.
 - D. Определение состава аппаратно-программного комплекса, требующегося для обеспечения защиты сети.
8. Какие шаги следует предпринять для анализа и решения проблемы в сети после сбора данных о работе?
 - A. Определить, является ли проблема периодической или устойчивой; составить список возможных причин; расставить приоритеты причин.
 - B. Расставить приоритеты причин; используя средства управления сетью или метод замены, идентифицировать причины; отследить тенденции с целью предвидения возникновения проблем в будущем.
 - C. Составить список возможных причин; расставить приоритеты причин; используя средства

управления сетью или метод замены, идентифицировать причины.

- D. Определить, можно ли воспроизвести проблему; расставить приоритеты возможных причин; используя средства управления сетью или метод замены, идентифицировать причины.
- 9. Что из приведенного ниже должно быть включено в отчет о проведении оценки?
 - A. Состав сетевой аппаратуры и программного обеспечения, которые не удовлетворяют промышленным стандартам.
 - B. Журналы, показывающие тенденцию к уменьшению скорости трафика в определенных сегментах сети.
 - C. Описание случаев и мест несанкционированного доступа к файлам.
 - D. Описание типов пользователей, наиболее часто сталкивающихся с проблемами при использовании сетью.
- 10. Что должно входить в письменную форму документа "Технические требования на изменения", который готовится для достижения более высокой производительности и уровня защиты сети?
 - A. Обоснования каждого запрашиваемого изменения.
 - B. Тип, количество и местонахождение каждого устройства в сети.
 - C. Сравнение текущей работы сети с ее прогнозируемой оптимальной работой.
 - D. Смета стоимости оборудования и трудозатрат.

Приложение Б

Сводные данные о командах

В этом приложении содержатся сводные данные о командах, использованных в книге. Его назначение — дать быструю справку по той или иной команде. Каждая команда приводится опально и сопровождается кратким описанием. Кроме того, в таблице есть перекрестная ссылка на главу в которой впервые упоминалась эта команда. Данное приложение должно помочь в понимании команд, используемых для конфигурирования маршрутизаторов компании Cisco.

Команда	Описание	Глава
access-enable	Разрешает маршрутизатору создавать временную запись о доступе в динамическом списке доступа	12
access-template	Вручную помещает в конфигулируемый маршрутизатор временную запись о доступе	12
appn	Посылает команду в подсистему A ^P N	12
atmsig	Выполняет команды выдачи ATM-сигналов	12
b	Загружает вручную операционную систему	16
bandwidth	Устанавливает значение полосы пропускания для интерфейса	15
banner motd	Задаёт баннер с сообщением дня	15
bfe	Устанавливает ручные аварийные режимы	12
boot system	Задаёт образ системы который маршрутизатор загружает при запуске	16
calendar	Управляет аппаратно реализованной системой календаря	12
cd	Изменяет текущее активное устройство	12
cdp enable	Активизирует выполнение на интерфейсе протокола исследования Cisco Discovery Protocol	13
clear	Сброс функций	12
clear counters	Обнуление счетчиков интерфейса	13
clockrate	Конфигурирует на последовательных интерфейсах, например в модулях сетевых интерфейсов или в интерфейсном процессоре, тактовую частоту аппаратных соединений с целью получения приемлемой скорости передачи в битах	15
cmt	Запускает или останавливает FDDI-функции управления соединением	12
config-register	Изменяет установки регистра конфигурирования	16
configure	Позволяет вводить изменения в существующую конфигурацию, а также поддерживать и хранить информацию о конфигурации на центральной площадке	12, 15, 18
configure memory	Загружает информацию о конфигурации из энергонезависимого ЗУ	15
configure terminal	Конфигурирует вручную терминал с консольного терминала	15, 16
connect	Открывает терминальное соединение	12
copy	Копирует данные конфигурации или образа системы	12
copy flash tftp	Копирует образ системы из флэш-памяти на TFTP-сервер	16

copy running-config startup-config	Сохраняет находящуюся в ОЗУ текущую конфигурацию в энергонезависимом ЗУ	15, 16
copy running-config tftp	Сохраняет находящуюся в ОЗУ текущую конфигурацию на сетевом TFTP-сервере	4
copy tftp flash	Загружает новый образ с TFTP-сервера во флэш-память	16
copy tftp running-config	Загружает конфигурационную информацию с сетевого TFTP-сервера	15
debug	Использует отладочные функции	12
debug ip rip	Выводит содержание пакетов актуализации маршрутной информации протокола RIP в том виде, в котором они посылаются и принимаются	18
delete	Удаляет файл	12
dir	Выводит список файлов на данном устройстве	12
disable	Отключает выполнение привилегированных команд	12
disconnect	Разрывает существующее сетевое соединение	12
enable	Включает выполнение привилегированных команд	12
enable password	Устанавливает локальный пароль для управления доступом к различным привилегированным уровням	15
enable secret	Задаёт дополнительный уровень защиты над командой enable password	15
erase	Стирает содержимое флэш-памяти или памяти конфигурации	12
erase startup-config	Стирает содержимое энергонезависимой памяти	14, 15
exit	Осуществляет выход из любого режима конфигурирования, закрывает активный сеанс терминала и прекращает работу в режиме EXEC	12, 15
format	Форматирует устройство	12
help	Дает описание из интерактивной системы помощи	12
history	Активизирует функцию истории команд	12
interface	Конфигурирует тип интерфейса и осуществляет переход в режим конфигурирования интерфейса	15
ip address	Назначает адрес и маску подсети и запускает на интерфейсе обработку по протоколу IP	17
ip default-network	Устанавливает маршрут по умолчанию	18
ip domain-lookup	Разрешает маршрутизатору выполнять трансляцию имени в адрес	17
ip host	Делает статическую запись о соответствии между именем и адресом в конфигурационном файле маршрутизатора	17
ip name-server	Задаёт адреса до шести серверов имен для использования в процессе преобразования имен и адресов	17
ip route	Устанавливает статические маршруты	18
lat	Открывает LAT-соединение	12
line	Идентифицирует конкретную линию, подлежащую конфигурированию, и запускает режим группирования команд конфигурирования линии	15
lock	Блокирует терминал	12
login	Вход в систему конкретного пользователя. Активизирует проверку пароля при регистрации в системе	12, 15
logout	Осуществляет выход из режима EXEC	12
media-type	Задаёт физическое соединение	15
mbranch	Трассирует по нисходящей ветвь многоадресного дерева для конкретной группы	12
mrbranch	Трассирует по восходящей ветвь многоадресного дерева	12

	для конкретной группы	
mrinfo	Запрашивает информацию о соседях и версии программного обеспечения у маршрутизатора с многоадресной рассылкой	12
mstat	Показывает статистические данные после нескольких трассировок маршрутов	12
mtrace	Трассирует путь от источника до ветви пункта назначения дерева многоадресной рассылки	12
name-connection	Именует существующее сетевое соединение	12
ncia	Запускает/останавливает NCIА-сервер	12
network	Назначает получаемый из Центра информации о сетях адрес, к которому непосредственно подключается маршрутизатор	18
no shutdown	Перезапускает отключенный интерфейс	15
pad	Открывает Х.29 РАО-соединение	12
ping	Посылает эхо-запрос; диагностирует принципиальную возможность взаимодействия в сети	10, 12, 17
PPP	Запускает двухточечный протокол разработки IETF	12
pwd	Показывает текущее активное устройство	12
reload	Останавливает работу и осуществляет холодный перезапуск; перезагружает операционную систему	12, 14, 16
rlogin	Открывает соединение удаленного доступа в систему	12
router	Запускает процесс маршрутизации, вводя определение протокола IP-маршрутизации. Например, команда <code>router rip</code> выбирает RIP в качестве протокола маршрутизации	15, 18
rsh	Выполняет удаленную команду	12
sdlc	Посылает тестовый кадр протокола SDLC	12
send.	Посылает сообщение по tty-каналам (телетайпным)	12
service password-encryption	Активизирует функцию шифрования пароля	15
setup	Осуществляет вход в средства команды <code>setup</code>	12, 14, 18
show	Показывает текущую рабочую системную информацию	2
show buffers	Предоставляет статистические данные о пуле буферов на сетевом сервере	13
show cdp entry	Выводит информацию о соседнем устройстве, запись о котором есть в CDP-таблице	13
show cdp interface	Выводит информацию об интерфейсах, на которых активизирован протокол CDP	13
show cdp neighbors	Выводит результаты CDP-процесса исследования	13
show flash	Выводит распределение и содержание флэш-памяти	13, 16
show hosts	Выводит находящийся в кэше список имен и адресов хост-машин	17
show interfaces	Выводит статистические данные обо всех интерфейсах, сконфигурированных на маршрутизаторе	13
show ip interface	Выводит данные о статусе и глобальные параметры, связанные с интерфейсом	18
show ip protocols	Выводит параметры и текущее состояние активного процесса протокола маршрутизации	18
show ip route	Выводит содержание таблицы IP-маршрутизации	13, 18
show memory	Показывает статистические данные о памяти маршрутизатора, включая статистику свободных пулов памяти	13
show processes	Выводит информацию об активных процессах	13
show protocols	Выводит данные о сконфигурированных протоколах. Эта команда показывает статус любого сконфигурированного	13

	протокола уровня 3 модели OSI	
show running-config	Выводит информацию о текущей конфигурации в ОЗУ	13, 14, 15, 16
show stacks	Контролирует использование стека процессами и прерванными маршрутами, а также указывает причину последней перезагрузки системы	13
show startup-config	Выводит сохраненную конфигурацию, которая содержится в энергонезависимом ЗУ	14, 15, 16
show version	Выводит конфигурацию аппаратной части системы, версию программного обеспечения, имена и источники конфигурационных файлов и образы начальной загрузки	13, 16
shutdown	Отключает интерфейс	15
telnet	Регистрация в хост-машине, поддерживающей протокол Telnet	13, 17
term ip	Задаёт формат сетевых масок в текущем сеансе	17
trace	Определяет путь, по которому будут следовать пакеты, перемещаясь к пункту назначения	13, 17
verify	Верифицирует контрольную сумму файла во флэш-памяти	12
where	Выводит список активных соединений	12
which-route	Выполняет просмотр таблицы OSI-маршрутов и выводит результаты	12
write	Записывает рабочую конфигурацию в память, передает в сеть или на терминал	12
write erase	Заменена командой <code>erase startup-config</code>	15
write memory	Заменена командой <code>copy running-config startup-config</code>	15
x3	Устанавливает X.3-параметры РАО-устройств	12
xr emote	Осуществляет вход в режим удаленной работы XRemote	12

Приложение В

Ответы на контрольные вопросы

В приложении содержатся ответы на контрольные вопросы, приведенные в конце каждой главы.

Глава 1

1. А
2. В
3. В
4. А
5. D
6. А
7. А
8. В
9. С
10. D

Глава 2

1. С
2. D
3. В
4. В
5. В
6. D
7. А
8. С
9. В
10. А

Глава 3

1. А
2. D
3. D
4. А
5. В
6. В
7. А
8. В
9. А
10. В

Глава 4

1. А
2. А
3. С
4. А
5. А
6. А
7. В
8. D
9. С
10. А

Глава 5

1. D
2. A
3. B
4. D
5. C
6. C
7. A
8. D
9. C
10. A

Глава 8

1. D
2. C
3. A
4. D
5. B
6. D
7. C
8. A
9. A
10. B

Глава 6

1. C
2. D
3. D
4. A
5. A
6. B
7. A
8. A
9. C
10. C

Глава 9

1. A
2. A
3. C
4. C
5. C
6. B
7. B
8. D
9. A
10. C

Глава 7

1. B
2. C
3. C
4. D
5. B
6. C
7. A
8. D
9. B
10. C

Глава 10

1. A
2. B
3. B
4. A
5. A
6. C
7. B
8. A
9. C
10. B

Глава 11

1. C
2. B
3. A
4. A
5. A
6. A
7. D
8. A
9. A
10. A

Глава 12

1. A
2. B
3. C
4. A
5. D
6. A
7. D
8. B
9. C
10. D

Глава 13

1. A
2. C
3. C
4. B
5. C
6. B
7. A
8. C
9. A
10. A

Глава 14

1. B
2. C
3. A
4. D
5. A
6. C
7. D
8. B
9. C
10. B

Глава 15

1. B
2. A
3. C
4. D
5. D
6. B
7. A
8. C
9. C
10. A

Глава 16

1. C
2. D
3. A
4. B
5. A
6. B
7. A
8. D
9. A
10. B

Глава 17

1. C
2. D
3. A
4. A
5. D
6. C
7. A
8. B
9. D
10. A

Глава 18

1. A
2. B
3. A
4. C
5. D
6. B
7. B
8. C
9. B
10. D

Глава 19

1. D
2. B
3. D
4. C
5. B
6. B
7. D
8. C
9. B
10. A

Приложение Г

Основы компьютерной техники

В данном приложении рассматриваются компоненты компьютера и роль компьютеров в сети, излагаются основы организации взаимодействия в сети, начиная с главного элемента сети — компьютера. Чем больше вы будете знать о компьютерах, тем легче вам будет понять принципы создания сети.

Чтобы разобраться с ролью компьютеров, можно представить себе Internet в виде живого организма, а компьютеры — в виде его клеток. Они являются источниками и приемниками информации, одновременно отдавая и получая ее из сети Internet. Хотя часто клетки способны жить независимо от организма, частью которого они являются, сам организм не может жить без клеток, его составляющих. В выживании компьютеры и Internet до некоторой степени зависят друг от друга. Конечно, компьютеры могут существовать без сети Internet, но с течением времени они становятся все более и более от нее зависимыми.

Компьютеры также играют жизненно важную роль в мире производства. Компании используют компьютеры и компьютерное программное обеспечение разными способами, но некоторое их применение является общим во всех компаниях. Серверы, например, используются для хранения важных данных и начисления заработной платы работникам. Программное обеспечение для работы с электронными таблицами используется для организации финансовой информации. Текстовые процессоры применяются для создания различных служебных записок и других текстовых документов. Базы данных используются для ведения подробных записей о клиентах. А для доступа к Web-серверу компании используются браузеры. Другими словами, сегодня компьютеры абсолютно необходимы для успешной работы компании.

В настоящем приложении будет рассказано о базовых процессах, происходящих внутри компьютера, знание которых необходимо до начала изучения организации взаимодействия в сети.

Составляющие компьютера

Поскольку компьютеры являются важными строительными блоками сети, важно знать основные элементы персонального компьютера (ПК). Многие из сетевых устройств сами представляют собой специализированные компьютеры, которые во многом состоят из тех же составных частей, что и обычный ПК. Чтобы компьютер стал надежным средством получения информации, например, для доступа к учебному курсу по Internet, он должен быть в нормальном рабочем состоянии, а это, в свою очередь, означает, что у вас иногда может возникнуть необходимость в устранении мелких неполадок в программном обеспечении и аппаратной части вашего компьютера. Поэтому необходимо знать названия и назначение следующих составляющих компьютера.

Мелкие дискретные компоненты

Транзистор — прибор, который усиливает (увеличивает) сигнал или замыкает и размыкает цепь.

Интегральная схема — электронный прибор, изготовленный из полупроводникового материала (который может управлять проводимым им количеством электричества).

Резистор — прибор, который оказывает сопротивление прохождению электрического тока.

Конденсатор — электронный компонент, который хранит энергию в виде электростатического поля (электрического поля, не изменяющегося во времени); он состоит из двух проводящих

металлических пластин, разделенных изолирующим материалом (рис. Г.1).



Рис. Г.1. Конденсаторы

Разъем — часть кабеля, которая вставляется в порт или интерфейс (рис. Г.2).

Светодиод (СИД) — прибор, который светится при прохождении через него электрического тока.

Припой — легкоплавкий сплав (смесь металлов), используемый для соединения металлов.

Подсистемы персонального компьютера

Печатная плата — тонкая пластина, на которой размещаются чипы и другие электронные компоненты.

Привод для компакт-дисков (CD-ROM) — привод устройства постоянной памяти на компакт-дисках, который представляет собой устройство, способное считывать информацию с компакт-дисков (рис. Г.3).

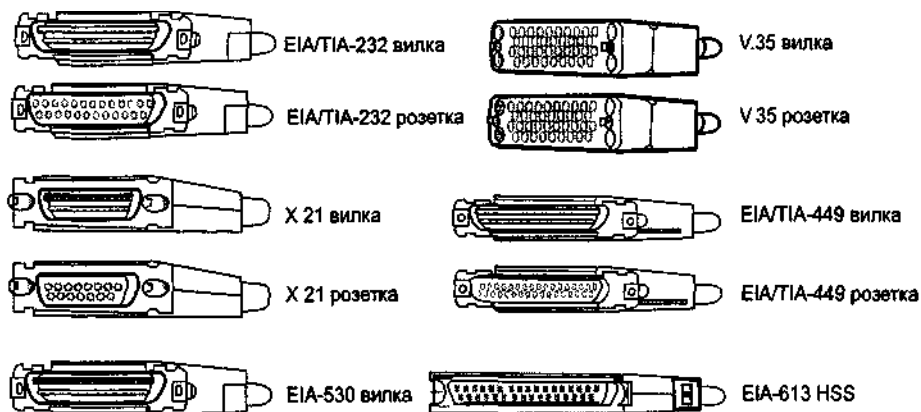


Рис. Г.2. Разъемы



Рис. Г.3. Привод для компакт-дисков

Центральный процессор — мозг компьютера, где выполняется большая часть вычислений

(рис. Г.4).

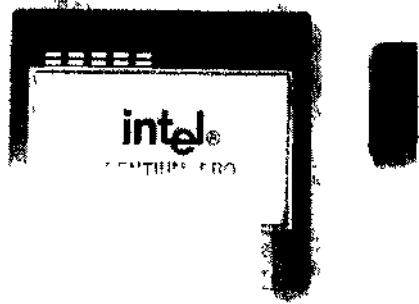


Рис. Г.4. Центральные процессорные устройства

Накопитель на гибких дисках — дисковый накопитель, способный считывать и записывать данные с использованием гибких магнитных дисков (рис Г.5).

Накопитель на жестких дисках — устройство, которое может считывать и записывать данные на жестком диске (рис. Г.6).

Микропроцессор — кремниевый чип, содержащий центральное процессорное устройство. В мире ПК термины *микропроцессор* и *центральное процессорное устройство* взаимозаменяемы.



Рис. Г.6. Накопитель на жестком диске

Материнская плата — основная печатная плата персонального компьютера (рис. Г.7).

Шина — группа проводников, по которым данные передаются из одной части компьютера в другую. Она соединяет все внутренние компоненты компьютера с центральным процессором (рис. Г.8).

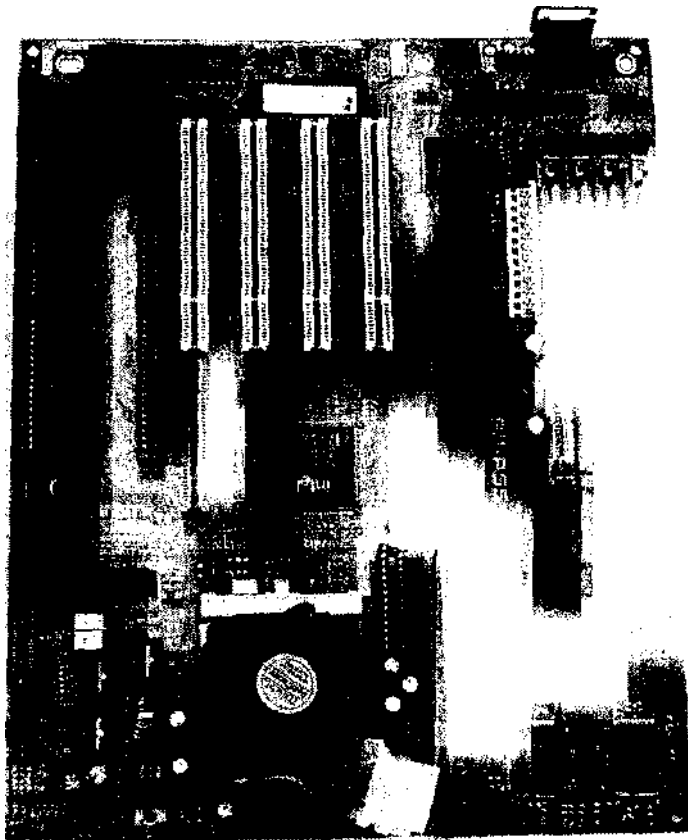


Рис. Г.7. Материнская плата

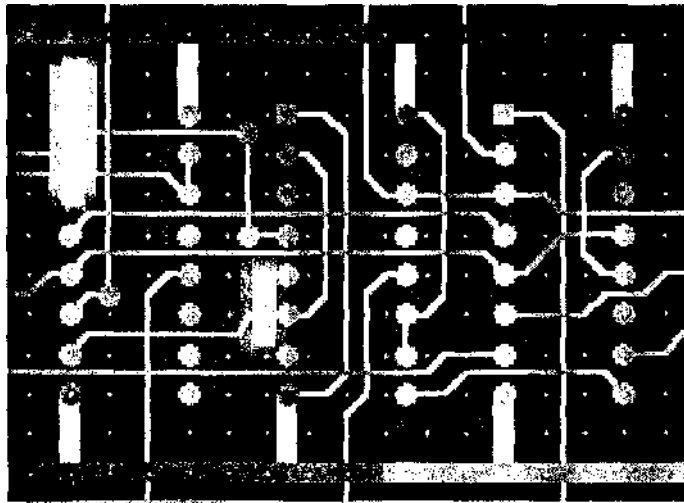


Рис. Г.8. Темно-серые линии являются частью шины

Оперативное запоминающее устройство (ОЗУ) — тип памяти компьютера, в которой можно обращаться к любому байту памяти, не затрагивая предыдущие байты (рис. Г.9).

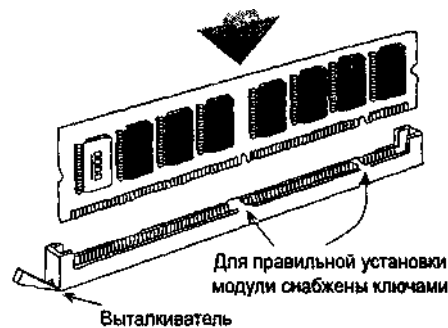


Рис Г9 Модуль оперативной памяти

Постоянное запоминающее устройство (ПЗУ) — память компьютера, в которую данные записываются заранее; после того как данные записаны на чипе ПЗУ, они не могут быть удалены и могут только считываться (рис. Г. 10).

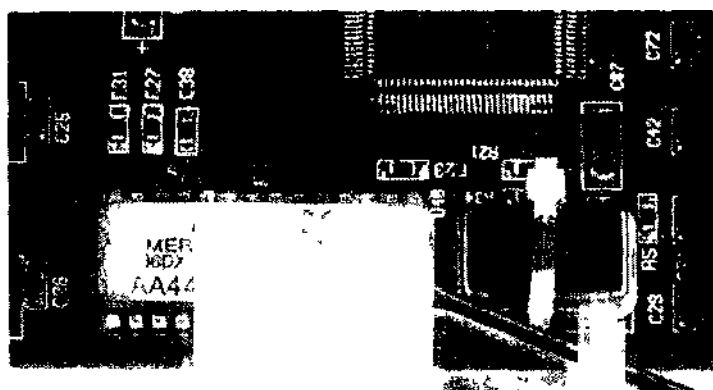


Рис Г 10 Чип ПЗУ

Системный блок — основная часть ПК. Он содержит шасси, микропроцессор, основную память, шину и порты, но в него не входят клавиатура, монитор или любое другое внешнее устройство, подключаемое к компьютеру.

Слот расширения — место в компьютере, куда вставляется печатная плата, добавляющая компьютеру новые функциональные возможности (рис. Г.И).

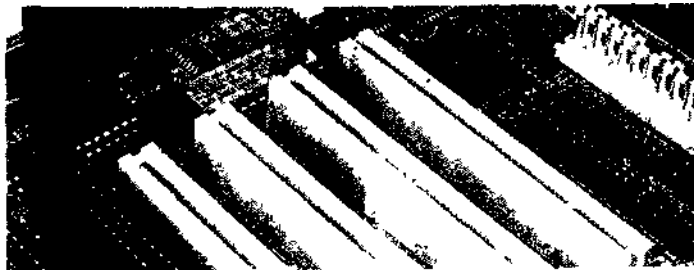


Рис Г 11 Слоты расширения

Блок питания — компонент компьютера, обеспечивающий ему подачу электропитания (рис. Г. 12).

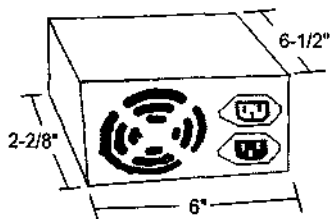


Рис Г 12 Блок питания

Элементы задней стенки

Плата расширения — печатная плата, которая может быть вставлена в компьютер для добавления ему новых функциональных возможностей (рис. Г. 13).

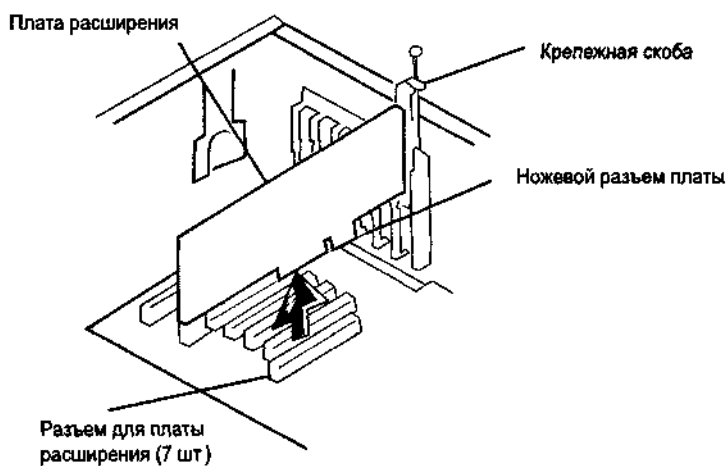


Рис Г 13 Плата расширения

Задняя стенка — большая печатная плата, на которой установлены гнезда для плат расширения. Задняя стенка отличается от материнской платы тем, что на ней могут не находиться логические схемы для выполнения вычислительных функций

Сетевая карта — плата расширения, вставляемая в компьютер для того, чтобы он мог подключиться к сети

Модем (модулятор/демодулятор) — устройство, которое позволяет компьютеру передавать данные по телефонным линиям, существуют внутренние (вставляемые в виде плат расширения) и внешние (подключаемые к порту) модемы

Видеокарта — плата расширения, которая позволяет выводить информацию на экран монитора (рис. Г 14)

Звуковая карта — плата расширения, которая позволяет компьютеру обрабатывать и выводить звук

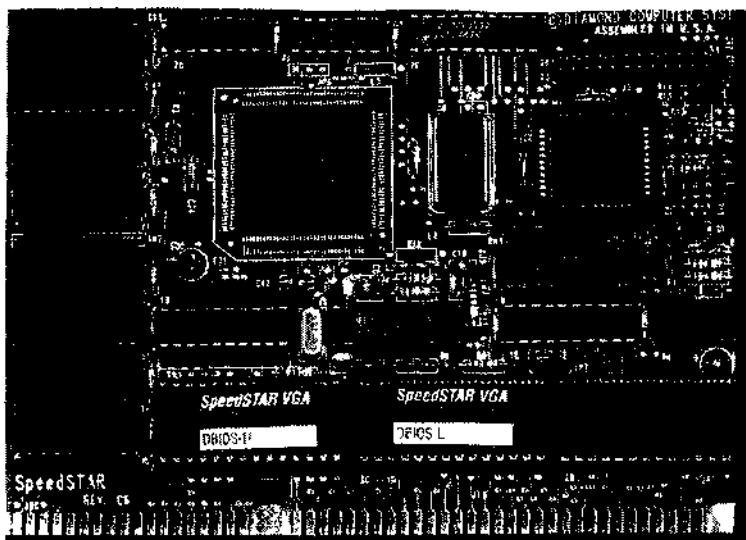


Рис. Г.14. Видеокарта

Интерфейс — элемент аппаратуры, например электрический разъем, который позволяет соединять два устройства (рис. Г. 15).

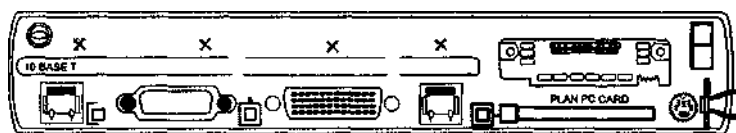


Рис. Г.15. Интерфейсы маршрутизатора Cisco 1601

Порт — интерфейс компьютера, к которому можно подключить электронное устройство (рис. Г. 16).

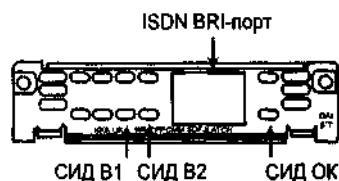


Рис. Г.16. ISDN-порт маршрутизатора Cisco 1603

Параллельный порт — интерфейс, способный передавать одновременно больше одного бита. Используется для подключения таких внешних устройств, как, например, принтеры (рис. Г. 17).

Последовательный порт — интерфейс, который может использоваться для последовательного обмена данными (при котором одновременно передается только один бит) (рис. Г. 18).

Порт мыши — предназначен для подключения к ПК мыши.

Шнур электропитания — используется для подключения электрического устройства к розетке с целью подачи на него электрического питания.

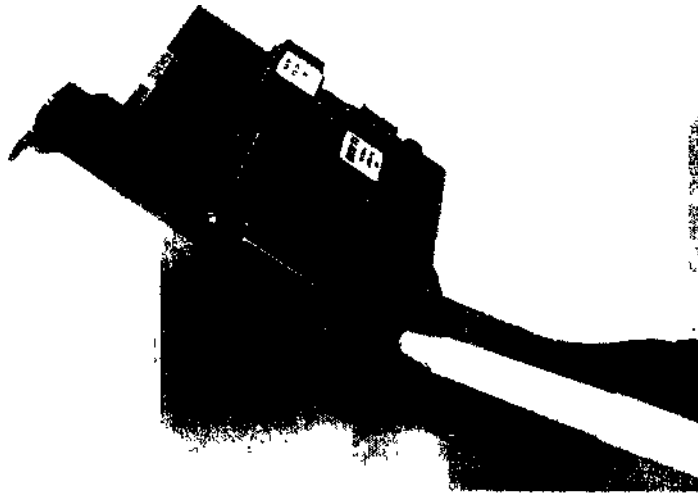


Рис. Г.17. Плата расширения параллельного порта

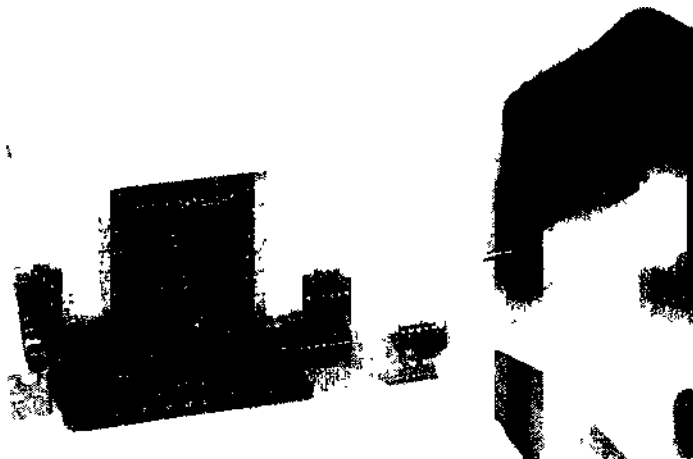


Рис. Г.18. Плата расширения последовательного порта

На рис. Г.19 показаны основные компоненты идеализированного компьютера. Внутренние составляющие компьютера можно представить себе в виде сети устройств, подключенных к системной шине. В некотором смысле ПК и есть небольшая компьютерная сеть.

В компьютер постоянно поступают информационные потоки и электрический ток. Чтобы понять принципы организации взаимодействия в сети — проектирование, создание и техническое сопровождение сетей, — можно представить себе компьютер в виде миниатюрной сети, в которой различные устройства, входящие в состав системного блока, соединены и обмениваются информацией друг с другом. Ниже приведены некоторые из наиболее важных информационных потоков (почти все из них проходят по шине).

- *Команды начальной загрузки* — хранятся и посылаются из ПЗУ.
- *Прикладное программное обеспечение* — после загрузки находится ОЗУ.

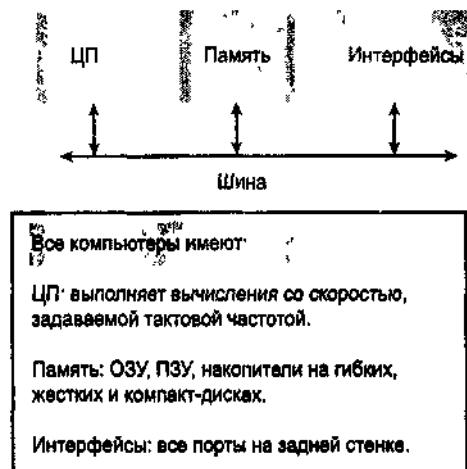


Рис. Г.19. Основными компонентами компьютера являются центральный процессор, память и интерфейсы

- *ОЗУ и ПЗУ*— постоянно общаются с центральным процессором по шине.
- *Информация прикладных программ* — хранится в ОЗУ, пока используется прикладное программное обеспечение.
- *Запоминаемая информация* — поступает из ОЗУ в какое-либо устройство хранения.
- *Экспортируемая информация* — поступает из ОЗУ и центрального процессора через шину и слот расширения на последовательный и параллельный (обычно для принтеров) порты, видеокарту, звуковую или сетевую карту.

Платы сетевого интерфейса

Плата сетевого интерфейса представляет собой печатную плату, которая обеспечивает возможность сетевого обмена данными, поток которых может идти в персональный компьютер, так и из него. Также называемая *сетевым адаптером*, она вставляется в материнскую плату и имеет порт для соединения с сетью.

Сетевая карта взаимодействует с сетью по последовательному соединению (одновременно передается один бит информации) и с компьютером — по параллельному соединению (одновременно передается больше одного бита). Каждая карта требует наличия канала IRQ, адреса ввода/вывода и адреса верхней памяти для ОС DOS или Windows 95/98. Канал IRQ или канал запросов на прерывание представляет собой физические линии связи, по которым устройства могут посылать микропроцессору сигналы прерывания. Сигналы прерывания информируют микропроцессор о наступлении того или иного события, например о выходе за пределы памяти. Адрес ввода/вывода — это участок памяти, используемый для ввода или извлечения данных из компьютера. В системах, работающих под управлением операционной системы DOS, верхней памятью называют область памяти, лежащую между первыми 640 Кбайт и 1 Мбайт.

При выборе сетевой карты следует учитывать следующие три фактора.

- Тип сети (например, Ethernet, Token Ring или FDDI).
- Тип кабеля (например, витая пара, коаксиальный или оптоволоконный).
- Тип системной шины, например, PCI или ISA (рис. Г.20).

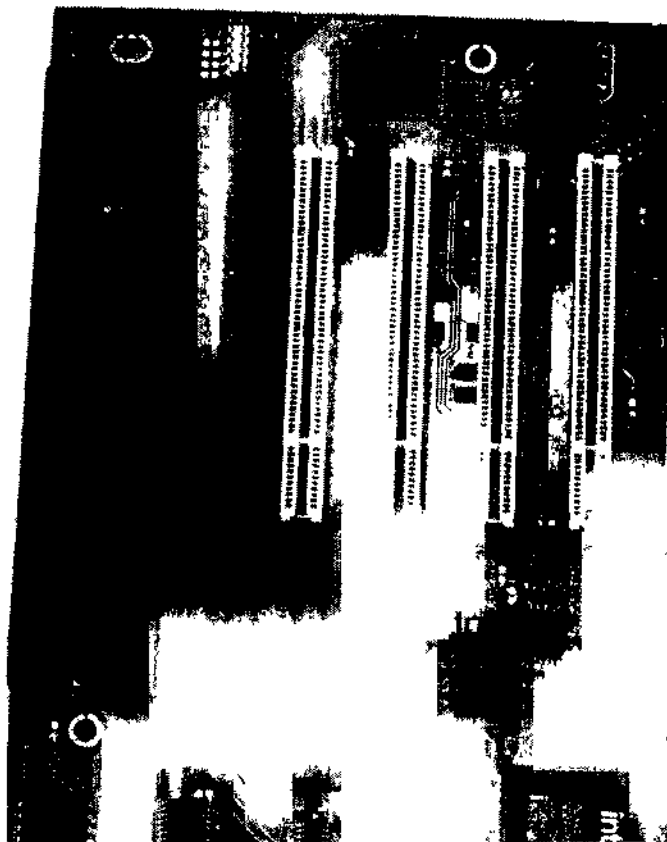


Рис. Г.20 Слоты шины PCI на фотографии находятся справа, а шины ISA — слева

Плата сетевого интерфейса позволяет функционировать сети и потому считается ключевым компонентом. Иногда может возникнуть необходимость в ее установке в компьютер. К некоторым возможным ситуациям, которые приводят к необходимости делать это, относятся следующие.

- Добавление платы сетевого интерфейса в ПК, который ее не имеет.
- Замена плохой или поврежденной платы
- Переход с платы, работающей со скоростью 10 Мбит/с (мегабит или миллион бит в секунду) на плату, работающую со скоростями 10/100 Мбит/с.

Изменение на плате сетевого интерфейса установок перемычек. Перемычка представляет собой металлический мостик, который замыкает электрическую цепь; обычно перемычка состоит из пластмассовой вставки, одеваемой на два штырька. Перемычки переставляются для того, чтобы изменить такие установки, как, например, IRQ (особенно в более старых платах сетевого интерфейса).

Для установки платы вам необходимо следующее.

- Знать, как конфигурируется сетевая карта, включая установку перемычек, программного обеспечения автоматического конфигурирования (plug-and-play software) и стираемого программируемого постоянного запоминающего устройства. (СППЗУ — это тип памяти, которая хранит содержимое до тех пор, пока не подвергнется воздействию ультрафиолетового света.)
- Уметь пользоваться средствами диагностики сетевой карты, включая средства диагностики изготовителя и проверку по методу петли. (Тестовый сигнал посылается в такой пункт назначения в сети, который после приема возвращает его в исходную точку; в случае работы с сетевой картой тестовый сигнал проходит между ПК и сетевой картой, при этом не важно, имеется или подключение внешнего кабеля.)

Способностью разрешать конфликты аппаратных ресурсов. К таким ресурсам относятся сигналы

IRQ и базовый адрес ввода/вывода или *адрес прямого доступа к памяти*. (Адрес прямого доступа к памяти используется для передачи данных из ОЗУ в устройство минуя процессор.)

Компоненты портативных компьютеров

Сейчас все более популярными становятся малогабаритные портативные компьютеры типа лэптоп и ноутбук, а также миниатюрные типа палмтоп, персональные цифровые ассистенты и другие маленькие вычислительные устройства. Материал, приведенный в предыдущих разделах, относится и к портативным компьютерам. Основное отличие состоит только в том, что их компоненты имеют меньшие размеры. Слоты расширения в таких компьютерах выполняются в стандарте Международной ассоциации карт памяти для персональных компьютеров (PCMCIA), когда сетевые карты, модемы, накопители на жестких дисках и другие устройства имеют обычно размер кредитной карточки и могут вставляться в различных местах по периметру корпуса компьютера.

Программное обеспечение

Теперь, когда вы имеете неплохое представление об аппаратной части компьютера, перейдем к рассмотрению компьютерного программного обеспечения. Цель программного обеспечения состоит в том, чтобы позволить вам взаимодействовать с компьютером или сетевым устройством и заставить его делать то, что от него хотят.

Таким образом, после настройки аппаратной части ПК необходимо сконфигурировать программное обеспечение. Например, до получения возможности просмотра учебного курса в сети Internet необходимо выполнить следующее.

1. Выбрать плату сетевого интерфейса.
2. Ввести правильные установки протокола TCP/IP, включая установки сетевого адреса (о протоколе TCP/IP см. в главе 10).
3. Отрегулировать монитор (если необходимо).
4. Инсталлировать и настроить браузер.
5. Выполнить несколько других задач (если необходимо).

Браузеры

Web-сервер представляет собой прикладное программное обеспечение, использующееся для определения местонахождения и отображения Web-страниц. Web-браузер играет роль интерфейса пользователя, последовательно контактируя с Web-сервером, запрашивая информацию, принимая ее и затем выводя результаты на экран. Программное обеспечение браузера интерпретирует язык гипертекстовой разметки (HTML) — язык, который используется для создания Web-страниц. Этот язык способен выводить графические изображения и воспроизводить звук и видеофильмы, а также работать с другими мультимедийными файлами. Гиперсвязи, являясь элементами электронного документа, которые указывают другое место в том же или совершенно другом документе, позволяют пользователю связываться с другими Web-страницами и файлами, которые могут загружаться в компьютер.

Двумя наиболее популярными браузерами являются Netscape Communicator и Internet Explorer (IE). Ниже приведены некоторые их сходные черты и отличия.

Netscape

- Первый популярный браузер.

- Занимает меньший объем дискового пространства.
- Многими считается простым.
- Выводит HTML-файлы.
- Пересылает электронную почту, файлы и выполняет другие функции.

Internet Explorer (IE)

- Сильно связан с другими продуктами компании Microsoft.
- Занимает больший объем дискового пространства.
- Считается более трудным в использовании.
- Выводит HTML-файлы.
- Пересылает электронную почту, файлы и выполняет другие функции.

Интегрируемые программные модули

Также существует много специфических типов файлов (авторство которых принадлежит частным компаниям), с которыми стандартные Web-браузеры работать не могут. Чтобы иметь возможность просматривать подобные файлы, необходимо сконфигурировать браузер на использование интегрируемых прикладных программных модулей. Эти приложения работают совместно с браузером и запускают программы, требующиеся для просмотра специальных файлов.

- Shockwave — воспроизводит мультимедийные файлы (с интегрированным текстом, графикой, видеоматериалами, анимацией и/или звуком); программа создана компанией Macromedia Authorware, Director and Flash programs.
- QuickTime — воспроизводит видеофильмы и звуковые файлы в формате Apple QuickTime.
- RealAudio — воспроизводит звуковые файлы в формате RealAudio
- RealPlayer G2 — воспроизводит файлы видеофильмов с высоким разрешением в формате RealPlayer.

Офисные прикладные программы

Кроме конфигурирования компьютера для просмотра через Internet учебных курсов, пользователь использует его для выполнения многих других полезных задач. В бизнесе регулярно применяют набор приложений, которые поступают в виде пакета офисных программ. Примером такого пакета является Microsoft Office. Обычно офисные приложения включают электронные таблицы, текстовый процессор, систему управления базой данных, программное обеспечение для подготовки презентаций и менеджер персональной информации, включающий электронную почту. Программное обеспечение для работы с электронными таблицами включает таблицы, состоящие из столбцов и строк, и часто используется с формулами для обработки и анализа данных. Текстовый процессор является приложением, которое используется для создания и редактирования текстовых документов; современные программы текстовых процессоров позволяют пользователю создавать сложные документы, включающие графику и многоформатный текст. Базы данных используются для хранения, ведения, организации, сортировки и фильтрации записей (запись — это некий

набор информации, идентифицируемый общей темой, например именем заказчика). Программное обеспечение для подготовки презентаций используется для создания презентационных материалов, показываемых на совещаниях, в учебных классах или на торговых презентациях. Менеджеры персональной информации включают электронную почту, список контактов, календарь и многое другое. Сегодня офисные приложения являются в той же степени частью повседневной работы, в какой до появления ПК были печатные машинки.

Сети

Сеть представляет собой сложную соединенную систему объектов или людей. Ее везде вокруг и даже внутри нас. Нервная и кровеносная системы — это тоже сети. Изображенная на рис. Г. 21 кластерная диаграмма показывает несколько типов сетей. Вы можете придумать и другие.

Отметим выделенные группы:

- транспорт;
- социальная сфера;
- биология;
- коммунальные службы

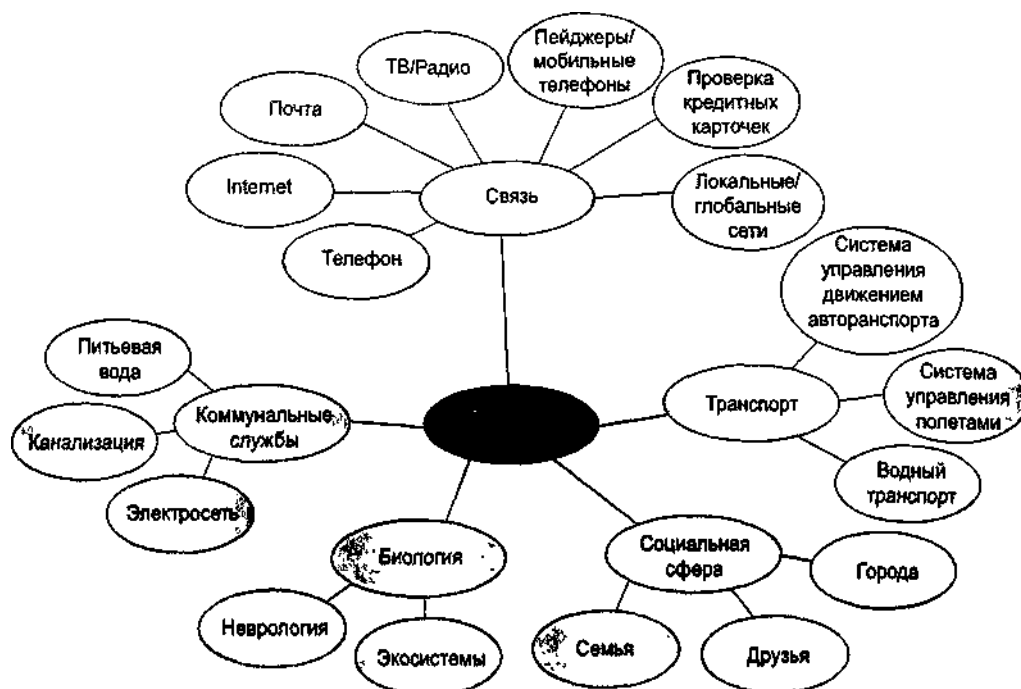


Рис. Г.21. Термин «сеть» используется в разных случаях, но в каждом из них его смысл подобен тому, что вкладывается и в понятие «компьютерная сеть»

Сети обмена данными проектируются для того, чтобы позволить двум компьютерам, расположенным в любой точке земного шара, общаться друг с другом. Сети также обеспечивают возможность обмена данными между компьютерами различных типов, будь то Macintosh, IBM-совместимый ПК или мэйнфрейм. Главное, чтобы все компьютеры и устройства понимали языки других, называемые протоколами.

Протокол представляет собой формальное описание набора правил, определяющих порядок, в соответствии с которым устройства обмениваются информацией. Большинство сетей обмена данными классифицируется по следующим категориям: локальные, региональные и глобальные. Локальные сети обычно расположены в отдельных зданиях или небольших комплексах зданий и обеспечивают связь между офисами. Региональные сети спроектированы для города или

деловой его части. Глобальные сети охватывают большие географические области и связывают города и страны. Соединение локальных, региональных и глобальных сетей называется организацией межсетевое взаимодействие.

Первые компьютеры были автономными устройствами. Каждый работал сам по себе независимо от какого-либо другого компьютера. Со временем стало очевидным, что это не эффективный, в том числе и в стоимостном плане, способ ведения бизнеса. Необходимо было найти решение, которое бы помогло найти ответ два вопроса.

1. Как избежать дублирования оборудования и ресурсов (например, требования наличия отдельного принтера на каждую пару ПК)⁷
2. Как эффективно организовать коллективное использование и обмен информацией?

Одним из первых решений этих проблем было создание локальных сетей. Поскольку локальные сети позволили объединить все рабочие станции, периферийное оборудование (внешние устройства, подключаемые к компьютеру), терминалы и другие устройства, находящиеся в одном здании, они сделали возможным для предприятий, использующих компьютерные технологии, обеспечить коллективное пользование файлов и принтеров.

Повсеместное использование компьютеров в производстве сделало очевидным, что и локальных сетей недостаточно. Использование систем на основе локальных сетей приводило к тому, что каждое подразделение или предприятие превращалось в своего рода электронный остров.

Необходим был способ эффективного и быстрого перемещения информации из одного предприятия в другое. Тогда и появилось решение о создании региональных и глобальных сетей. Так как глобальные сети могли соединять сети пользователей, находящиеся в географически большой области, они обеспечили производствам возможность общения друг с другом на больших расстояниях.

Ранние разработки локальных, региональных и глобальных сетей носили во многом хаотический характер. В начале 1980-х годов наблюдался огромный рост количества сетей. Компании поняли, сколько денег они могут сберечь и насколько могут повысить производительность за счет применения сетевой технологии. Например, служебные записки могли быть доведены по сети до всех сотрудников мгновенно, и для этого не надо было иметь кого-то, кто бы распечатал документ, сделал достаточное количество копий и доставил бы всем сотрудникам. Компании начали добавлять сети и расширять существующие почти с такой же скоростью, с какой появлялись новые сетевые технологии и продукты.

К середине 1980-х проявилась болезнь роста. Многие из появившихся сетевых технологий были созданы с использованием аппаратного и программного обеспечения от разных производителей и разработчиков. Как следствие, многие новые сетевые технологии оказались несовместимыми. Сетям, использующим различные спецификации, например Ethernet и Token Ring, становилось все труднее обмениваться данными друг с другом. Не удивительно, что начиная с середины 1980-х годов большая часть работ была связана с созданием и реализацией сетевых технологий и стандартов, которые позволяли работать вместе в одной сети сетевым устройствам или технологиям от различных производителей. Например, тогда появились *мосты* (устройства, соединяющие две локальных сети или два сегмента одной сети), которые позволили обмениваться информацией сетям Ethernet и Token Ring.

С появлением множества технологий возникла необходимость каким-то способом измерять характеристики локальных и глобальных сетей с целью определения их полезности для компаний и конечных пользователей. Основным способом описания возможностей сети является применение такой меры, как *полоса пропускания*. Этот термин может быть сложным для понимания, но он представляет собой важную концепцию техники создания сетей. Это и является темой следующего раздела.

Полоса пропускания

Полоса пропускания является мерой того объема информации, который может быть передан из

одного места в другое за заданный промежуток времени. Существуют два общеупотребительных случая использования термина *полоса пропускания*: один относится к аналоговым сигналам, а другой — к цифровым (сигналы рассматриваются в приложении Д, "Основы электроники и сигналы"). Во всем остальном материале данной книги имеется в виду цифровая полоса пропускания, или просто полоса пропускания.

Вы уже знаете, что основной единицей измерения, используемой для описания потока цифровой информации из одного места в другое, является бит, а основной единицей измерения времени — секунда. Теперь понятно, откуда возникает термин бит в секунду (бит/с).

Бит в секунду — это единица измерения полосы пропускания. Конечно, если обмен происходит со скоростью 1 бит в секунду, то это очень медленно. Американский стандартный код для обмена информацией (ASCII) представляет символы английского языка в виде чисел, при этом каждой букве назначается номер от 0 до 127. Теперь представьте передачу ASCII-кода своей фамилии и адреса со скоростью 1 бит в секунду — это займет минуты! К счастью, сейчас возможен значительно более быстрый обмен данными. В табл. Г. 1 представлены различные единицы измерения полосы пропускания.

Таблица Г.1. Единицы измерения полосы пропускания

Единица измерения	Сокращенное название	Эквивалентность
Бит в секунду	бит/с	1 бит/с — основная единица измерения полосы пропускания
Килобит в секунду	Кбит/с	1 Кбит/с = 1024 бит/с = 2^{10} бит/с
Мегабит в секунду	Мбит/с	1 Мбит/с = 1 048 576 бит/с = 2^{20} бит/с
Гигабит в секунду	Гбит/с	1 Гбит/с = 1 073 741 824 бит/с = 2^{30} бит/с

Полоса пропускания является очень важным элементом в создании сетей, хотя, может быть, довольно абстрактным и трудным для понимания. Ниже приведены три аналогии, которые, возможно, помогут вам лучше представить себе полосу пропускания.

1. Полосу пропускания можно сравнить с диаметром трубы (рис. Г.22). Представьте себе систему трубопроводов, через которые в ваш дом поступает питьевая вода и уходят сточные воды. Эти трубы имеют различные диаметры: магистральная труба городского водопровода может иметь диаметр 2 метра, тогда как диаметр крана на кухне может быть всего 2 сантиметра. Диаметр трубы служит мерой пропускной способности трубы. По этой аналогии вода подобна информации, а диаметр трубы — полосе пропускания. Фактически многие специалисты по сетям используют в разговорах между собой как раз подобные аналогии, говоря, что, мол, надо бы установить "трубы побольше", имея под этим в виду более широкую полосу пропускания, т.е. более высокую пропускную способность передачи информации.
2. Полоса пропускания похожа на количество полос дорожной магистрали (рис. Г.23). Представьте себе сеть дорог, которые имеются в вашем городе. Это могут быть скоростные восьмиполосные магистрали с выездами на двух- и трехполосные дороги, которые затем могут переходить в двухполосные отдельные улицы и заканчиваться подъездными дорожками к вашему дому. В соответствии с этой аналогией количество полос магистрали представляет собой полосу пропускания, а количество автомобилей подобно объему информации, который может передаваться.

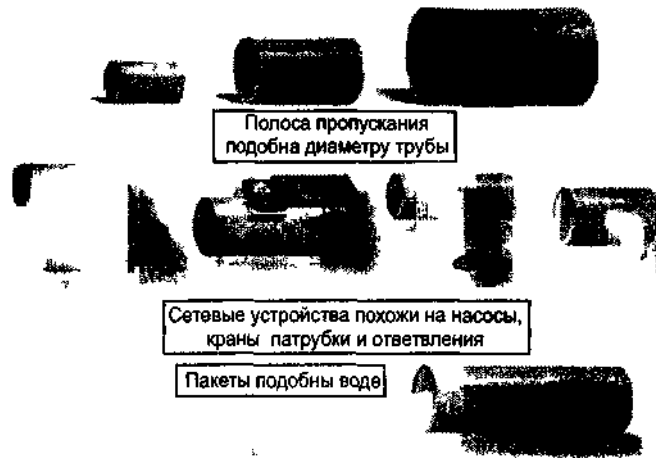


Рис Г 22 Чем больше диаметр трубы, тем с большей удельной скоростью по ней может течь жидкость

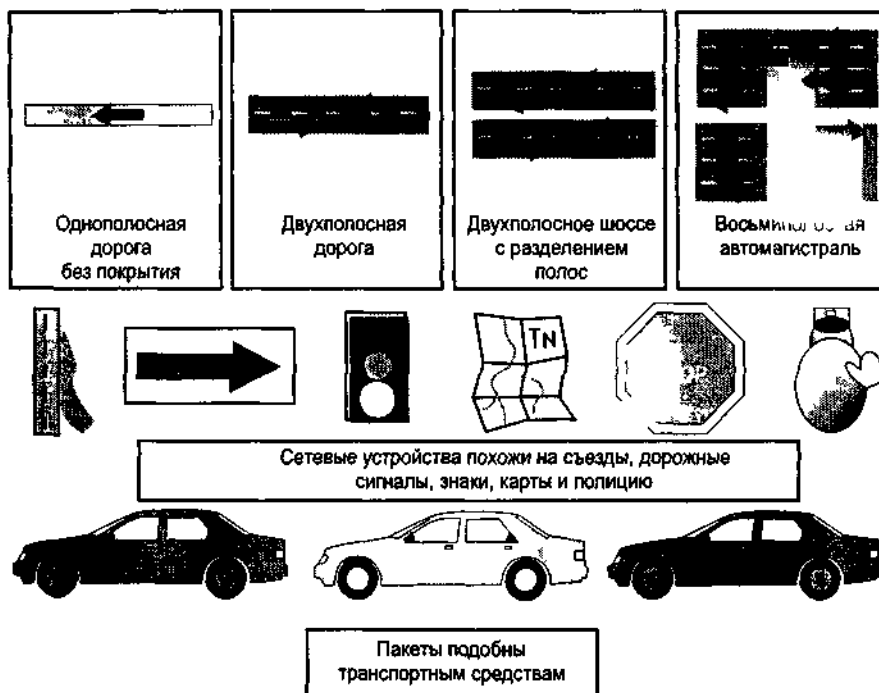


Рис Г 23 Чем больше полос имеет магистраль, тем больший поток машин она способна пропустить

- Полоса пропускания подобна качеству звука вашей аудиосистемы Звук — это информация, а качество звука — полоса пропускания, т.е. звук — это данные, а мера частоты звука — полоса пропускания Если бы вы попытались оттранжировать предпочитаемый способ прослушивания любимой песни по телефону, через АМ- и FM-радиопремник или с помощью проигрывателя компакт-дисков, то, вероятно, поставили бы компакт-диск на первое место, затем — FM-радиоприемник, потом — АМ-радиоприемник и на последнее место — телефон Реальные значения полосы пропускания для всех этих случаев равны соответственно 20, 15, 5 и 3 КГц.

Однако все-таки следует помнить, что истинным и действительным значением термина "полоса пропускания" в контексте данной книги является максимальное количество бит, которое теоретически может пройти через заданную область пространства за определенное количество времени при заданных условиях Используемые выше аналогии приведены только для того, чтобы облегчить понимание концепции полосы пропускания

Полоса пропускания — это чрезвычайно полезная концепция. Однако она имеет свои

ограничения Независимо от того, как посылаются сообщения и какой тип кабеля используется, величина полосы пропускания ограничена Это объясняется как законами физики, так и современным уровнем технологии

В табл Г 2 представлены максимально возможные значения цифровой полосы пропускания (включая ограничения по длине) для нескольких широко распространенных типов кабеля Всегда следует помнить, что ограничения носят как физический, так и технологический характер (технология определяет качество изготовления кабеля, что, в свою очередь определяет границы полосы пропускания)

Таблица Г.2. Максимальные значения полосы пропускания и ограничения подлине

Тип среды	Теоретически максимальное значение полосы пропускания, Мбит/с	Максимальное физическое расстояние, м
50-омный коаксиальный кабель (Ethernet 10-1000 10Base2 ThinNet)		200
75-омный коаксиальный кабель (Ethernet 10-100 10Base5 ThickNet)		500
Неэкранированная витая пара категории 5 (UTP) (Ethernet 100BaseTX Fast Ethernet)	100	100
Многомодовое (62 5/125 мкм) оптоволокно (100BaseFX)	100	200
Одномодовое (центральная жила 10 мкм) оптоволокно (1000BaseLX)	1000	3000
Другие технологии находящиеся на стадии исследования	2400	40000
Беспроводная передача	2	100

Полоса пропускания также ограничивается возможностями конкретной сетевой технологии, например ISDN (цифровая сеть с интегрированными службами), которую использует провайдер услуг

В табл Г 3 приведены различные службы глобальных сетей и соответствующие им значения полосы пропускания Какой из них вы пользуетесь дома? В школе?

Таблица Г.3. Службы глобальных сетей и значения полосы пропускания

Тип службы глобальной сети	Типовой пользователь	Полоса пропускания
Модем	Физические лица	0,033 Мбит/с
Frame Relay	Небольшие учреждения (школы), надежные глобальные сети	0,056 Мбит/с
ISDN	Сотрудники, работающие на дому, небольшие предприятия	0,128 Мбит/с
T1	Более крупные предприятия и организации	1,544 Мбит/с
T3	Более крупные предприятия и организации	44,736 Мбит/с
STS-1 (OC-1)	Телефонные компании, магистральные каналы компаний, занимающихся передачей данных (datascomm-компания)	51,840 Мбит/с
STS-3 (OC-3)	Телефонные компании, магистральные каналы компаний, занимающихся передачей данных (datascomm-компания)	155,251 Мбит/с
STS-48 (OC-48)	Телефонные компании, магистральные каналы компаний, занимающихся передачей данных (datascomm-компания)	2,488320 Гбит/с

Представим, что вам повезло и что у вас есть новый фирменный кабельный модем (предназначенный для работы с использованием каналов кабельного телевидения), ваш местный магазин только что установил у себя линию сети ISDN или ваше учебное заведение как раз получило локальную 10-мегабитовую сеть Ethernet. Представим также, что просмотр фильма, который вы давно хотели посмотреть, загрузка Web-страницы или программного обеспечения занимают целую вечность. А вы, вероятно, полагали, что получаете всю полосу пропускания, о которой шла речь в рекламе. Но есть другой важный момент, который следует учитывать, — пропускная способность.

Пропускной способностью называется фактическое значение полосы пропускания, измеренное в конкретное время дня при загрузке конкретного файла, поступающего по конкретным маршрутам сети Internet (путям, по которым будут следовать данные в Internet). К сожалению, по многим причинам пропускная способность часто значительно меньше максимально возможной цифровой полосы пропускания используемой среды передачи данных. Некоторые факторы, которые определяют величину пропускной способности и полосы пропускания, приведены ниже.

- Устройства межсетевого взаимодействия (например, маршрутизаторы и коммутаторы).
- Тип передаваемых данных.
- Топология (конфигурация сети, например, "кольцо" или "звезда").
- Количество пользователей.
- Компьютер, используемый пользователем.
- Компьютер, используемый в качестве сервера.
- Сбои, вызываемые электропитанием и погодой.

Проектируя сеть, важно учитывать теоретическую величину полосы пропускания (напомним, что это теоретически максимальное количество бит, которое может пройти через заданную область пространства за определенное количество времени). Сеть не будет быстрее, чем позволит среда передачи данных. Реально работая с сетями, вероятно, надо будет измерить пропускную способность и принять решение о ее адекватности для пользователя (рис Г 24).

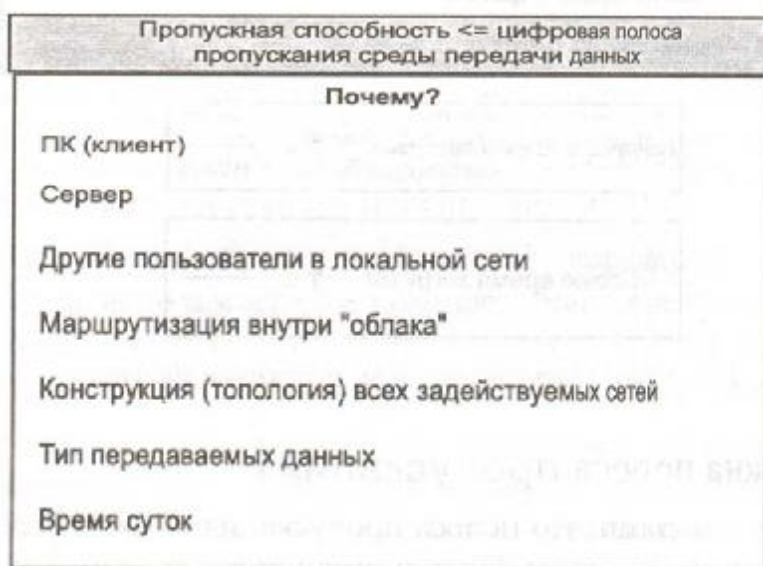


Рис. Г.24. Пропускной способностью называется реальный объем данных, проходящий через заданную область пространства за определенный промежуток времени

Важным моментом при проектировании сети является решение о том, какую среду

передачи данных использовать. Это часто приводит к вопросам, связанным с величиной полосы пропускания, требующейся для приложений пользователя. На рис. Г.25 показана простая формула, которая поможет при принятии таких решений. Выглядит она следующим образом: оценочное время = размер файла/полоса пропускания. Получившийся в результате ответ представляет собой самое быстрое время, за которое могут быть переданы данные. Он, конечно, не принимает во внимание все те ранее рассмотренные моменты, которые оказывают влияние на полосу пропускания, но все же дает приблизительную оценку времени, которое займет пересылка информации при использовании данной конкретной среды/приложения.

Теперь, зная единицы измерения цифровой полосы пропускания, попытайтесь решить следующую задачу.

Задача

Сокращение Гбайт означает гигабайт, один гигабайт примерно равен одному миллиарду байтов. Аналогично, 1 Гбайт/с — это один миллиард байтов в секунду. SONET — это аббревиатура от слов *synchronous optical network* (синхронная оптическая сеть) и стандарт, описывающий соединение оптоволоконных передающих систем. Название OC-48 означает сеть с *оптической несущей* с полосой пропускания 2,488 Гбайт/с, удовлетворяющую стандарту SONET. Держа в уме эти определения, определите, что будет быстрее' переслать полностью заполненный гибкий диск по ISDN-каналу или полностью заполненный жесткий диск объемом 10 Гбайт по каналу OC-48?

BW — теоретически максимальная полоса пропускания "самого медленного" канала между хост-машиной отправителя и хост-машиной получателя.

P — Фактическая пропускная способность на момент передачи

T — Время на передачу файла

S — Размер файла в битах

Наилучшее время загрузки $T = \frac{S}{BW}$

Типовое время загрузки $T = \frac{S}{P}$

Рис. Г.25. Формула расчета времени перекачки файла

Почему так важна полоса пропускания?

1. Прежде всего, надо сказать, что полоса пропускания не бесконечна. Независимо от среды передачи данных, законы физики ограничивают величину полосы пропускания. Например, именно ограничения полосы пропускания (из-за физических свойств телефонных кабелей типа "витая пара", которые проложены во многих домах) определяют

верхнюю границу пропускной способности стандартных телефонных модемов на уровне примерно 56 Кбит/с. Полоса электромагнитного спектра (полный диапазон длин волн электромагнитного излучения) — тоже конечна. Сюда входят только те частоты, которые принадлежат радио-, микроволновому и инфракрасному спектрам. Вследствие этого Федеральная комиссия связи США имеет целое подразделение, которое контролирует, кто и какую полосу использует. В принципе оптоволоконный кабель позволяет иметь настолько широкую полосу пропускания, что она может считаться практически бесконечной. Однако технологии, применяемые для создания сверхширокополосных сетей, которые бы полностью использовали потенциальные возможности оптоволокна, в настоящее время только разрабатываются и реализуются.

2. Зная то, как работает полоса пропускания, и то, что она конечна, можно сберечь большие деньги. Например, стоимость различных вариантов подключения к провайдерам Internet-услуг частично зависит от того, какую полосу пропускания необходимо иметь (в среднем и при пиковых, т.е. максимально возможных, нагрузках).
3. Как от профессионала в области сетей от вас будут ожидать, что вы знакомы с понятиями полосы пропускания и пропускной способности. Они являются главными факторами при анализе производительности сети. Кроме того, если вы — проектировщик новых сетей, то полоса пропускания всегда будет главным вопросом при проектировании.
4. Вполне естественно, что человек или организация, начав пользоваться сетью, в конечном итоге хотят иметь все большую и большую полосу пропускания. Новые мультимедийные программы требуют значительно большей полосы пропускания, чем те, которые использовались в середине 1990-х годов. Программисты и пользователи энергично проектируют сети, которые способны выполнять более сложные задачи и, следовательно, требуют наличия более высокой полосы пропускания.

Резюме

- Компьютеры являются жизненно важными компонентами любой сети. Чем больше вы знаете о компьютерах, тем легче вам понять работу сетей.
- Важно знать составляющие элементы компьютера и уметь устанавливать платы сетевого интерфейса. Также необходимым условием для тех, кто работает с сетями, является умение устранять неисправности в ПК.
- Программное обеспечение позволяет пользователю взаимодействовать (подключаться и использовать) с компьютером. Чаще всего для работы в сетях используют Web-браузеры и системы электронной почты. Для ведения бизнеса используются офисные приложения, браузеры и электронная почта.
- Существуют два основных типа сетей: локальные и глобальные. Глобальные соединяют локальные сети. В качестве средства взаимодействия компьютеров и сетевых устройств локальные и глобальные сети используют протоколы.
- Полоса пропускания и пропускная способность являются мерой быстродействия или технических возможностей сети.

Приложение Д

Основы электроники и сигналы

Функцией физического уровня модели OSI является передача данных за счет введения электрических спецификаций, которые должны выполняться в промежутке между отправителем и получателем. Достигая здания, электрический ток поступает в рабочие станции, серверы и сетевые устройства по проводам, проложенным в стенах, полу и потолках. Данные, которые могут содержать текст, картинки, звуковое сопровождение и видеоматериалы, тоже поступают по системе кабелей и в медных проводниках представлены в виде электрических импульсов или в виде импульсов света в оптоволокне.

В данном приложении будут изложены основы электричества, которые являются основой для понимания взаимодействия в сетях на физическом уровне модели OSI. Рассматриваемые здесь концепции помогут понять процесс передачи данных в физической среде, например с использованием кабелей и разъемов, а также факторы, которые оказывают влияние на передачу данных (см главу 2, "Физический и канальный уровни")

Основы электричества

Все вещества состоят из атомов. В *Периодической таблице элементов* (рис Д 1) приведены все известные типы атомов и их свойства. Атом состоит из следующих частей:

- *Ядро* — центральная часть атома, образуемая протонами и нейтронами.
- *Протоны* — частицы с положительным зарядом, которые вместе с нейтронами образуют ядро.
- *Нейтроны* — частицы без заряда (нейтральные), которые вместе с протонами образуют ядро.
- *Электроны* — частицы с отрицательным зарядом, вращающиеся по орбитам вокруг ядра.

Чтобы разобраться в электрических свойствах элементов и материалов, давайте найдем в периодической таблице элементов гелий. Его *атомный номер* 2, и это означает, что у него два протона и два электрона. *Атомный вес* гелия равен 4. Вычитая атомный номер (2) из атомного веса (4), определяем, что гелий также имеет два нейтрона.

Периодическая таблица элементов

1A		2A		Переходные металлы										3A						4A	5A	6A	7A	8A
1	H													5	6	7	8	9	10	2	He			
3	Li	4	Be											13	14	15	16	17	18					
11	Na	12	Mg	3B	4B	5B	6B	7B	8B	1B	2B	31	32	33	34	35	36							
19	K	20	Ca	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36					
37	Rb	38	Sr	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54					
55	Cs	56	Ba	57	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86					
87	Li	88	Ra	89	104	105	106	107	108	109	110	111	112		114		116		118					

Ряд лантаноидов	
58	Ce
59	Pr
60	Nd
61	Pm
62	Sm
63	Eu
64	Gd
65	Td
66	Dy
67	Ho
68	Er
69	Tm
70	Yb
71	Lu

Ряд актиноидов	
90	Th
91	Pa
92	U
93	Np
94	Pu
95	Am
96	Cm
97	Bk
98	Cf
99	Es
100	Fm
101	Md
102	No
103	Lr

Рис. Д.1. Периодическая таблица элементов

Пример:

- атомный номер гелия — 2
- 2 протона + 2 электрона
- 4 (атомный вес) - 2 (атомный номер)
- 2 нейтрона

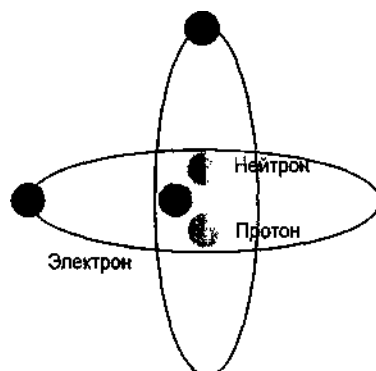


Рис. Д.2 Атом гелия имеет два протона, два нейтрона и два электрона

Датский физик Нильс Бор разработал упрощенную модель, иллюстрирующую строение атомов. На рис. Д.2 показана модель атома гелия. Отметим относительный масштаб составных частей атома. Если бы протоны и нейтроны этого атома имели размер футбольного мяча, который находится в центре поля, то тогда электроны имели бы размер вишни и вращались бы по орбитам, проходящим где-то в районе последних кресел трибун стадиона. Пространство внутри атома имело бы размер футбольного поля.

Эта модель дает установки, полезные для обсуждения концепции сил, действующих в атоме. Закон Кулона (закон о действии электрических сил) гласит, что *противоположные заряды* действуют друг на друга с силой, которая заставляет их притягиваться, а *одинаковые заряды* действуют друг на друга с силой, которая заставляет их отталкиваться. Сила представляет собой толкающее или тянущее действие — в случае противоположных и одинаковых зарядов сила увеличивается при приближении зарядов друг к другу.

Обратимся к модели атома гелия по Бору, показанной на рис. Д.2. Если закон Кулона верен и если модель Бора описывает атом гелия как стабильный, то тогда должны выполняться другие

законы природы. Иначе как эти две концепции могут быть совместимыми?

Вопрос 1: почему электроны не летят в направлении протонов?

1. Закон Кулона — одинаковые заряды отталкиваются.

2. Модель Бора — протоны имеют положительный заряд. В ядре находится несколько протонов.

Вопрос 2: почему протоны не разлетаются?

Ответы на эти вопросы состоят в том, что существуют другие законы природы, которые необходимо учитывать. Ниже даны ответы на каждый из предыдущих вопросов.

Ответ 1: электроны остаются на орбите, хотя и притягиваются протонами, благодаря тому, что они обладают достаточной скоростью, чтобы продолжать вращаться по орбите и не дать ядру притянуть себя.

Ответ 2: протоны не разлетаются благодаря наличию ядерных сил, связанных с нейтронами. Ядерные силы чрезвычайно велики и действуют в качестве своего рода клея, который удерживает протоны вместе.

Протоны и нейтроны связаны очень мощной силой. Однако сила, которая удерживает электроны на орбите вокруг ядра, значительно слабее. На рис. Д.3 проиллюстрированы эти силы. Как раз в результате того, что эта сила "более слабая", в атомах определенного типа электроны могут отрываться от своих атомов и создавать *поток*. Это и есть электрический ток — поток свободных электронов.

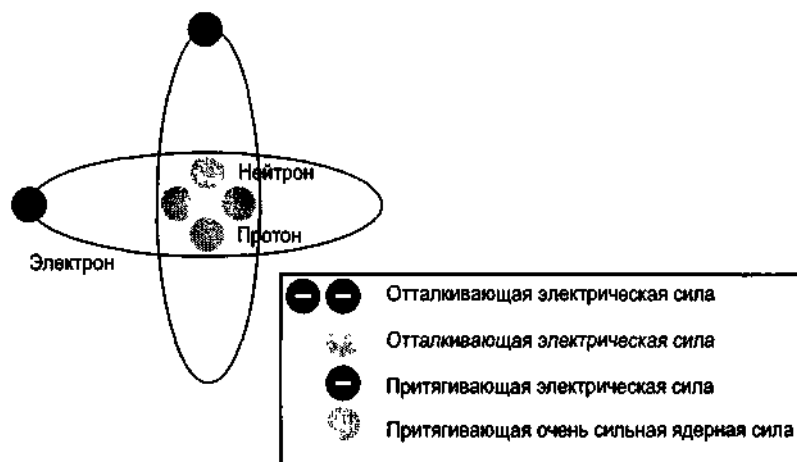


Рис. Д.3. Силы внутри атома

Типы электрических материалов

Группы атомов образуют *молекулы*. В свою очередь *материалы* состоят из молекул. В зависимости от того, с какой легкостью в них может протекать электрический ток (свободные электроны), материалы могут принадлежать к одной из трех групп. Эти три типа материалов называются: *изоляторы*, *проводники* и *полупроводники*.

Изоляторы

Электрические изоляторы, или просто изоляторы, — это материалы, которые позволяют течь электронам с большим трудом или не позволяют течь совсем. Электрические изоляторы не похожи на термоизоляторы или теплоизоляцию, которая удерживает зимой тепло в домах. Примерами электрических изоляторов могут быть пластмасса, стекло, воздух, сухое дерево, бумага, резина и определенные атомы, например гелий. Эти материалы обладают очень стабильной химической структурой с электронами на орбитах, которые сильно связаны с атомами.

Хорошим примером изолятора является стекло. Из стекла изготавливается оптоволоконный кабель, и оно служит в качестве среды для переноса световых импульсов. Поскольку стекло не

передает электрические сигналы, оно нечувствительно к наведенным электрическим сигналам и импульсам. Также вследствие того, что стекло является изолятором, использование в сети оптоволоконных каналов снимает проблему контура заземления сети.

Проводники

Электрические проводники, или *проводники*, — это материалы, в которых электроны могут течь совершенно свободно. Эта легкость объясняется тем, что внешние электроны атомов очень слабо связаны с ядром и легко могут становиться свободными. Уже при комнатной температуре в этих материалах имеется большое количество свободных электронов, которые могут обеспечивать проводимость. Подача напряжения (обсуждается подробно в следующем разделе) вызывает движение свободных электронов, т. е. электрический ток.

В периодической таблице некоторые группы атомов выделяются в категории по столбцам. Атомы в каждом столбце принадлежат конкретному химическому семейству. Хотя все они могут иметь различное количество протонов, нейтронов и электронов, их внешние электроны обладают сходными орбитами и при взаимодействии с другими атомами и молекулами ведут себя похожим образом. Наилучшими проводниками являются такие металлы, как медь (Cu), серебро (Ag) и золото (Au). Все эти металлы размещаются в одном столбце периодической таблицы и имеют электроны, которые легко освобождаются, делая их прекрасными материалами для переноса *тока*.

К другим проводникам также относятся припой (смесь свинца (Pb) и олова (Sn)) и вода. Вода является проводником из-за наличия ионов. Ионом называется атом, у которого больше или меньше электронов, чем у нейтрального атома. Человеческое тело приблизительно на 70% состоит из ионизированной воды, что означает, что наше тело тоже является проводником.

Несомненно, проводники широко распространены в мире сетей. Именно они позволяют передавать электрические сигналы в компьютере и по сети.

Полупроводники

Полупроводниками называются материалы, которые могут управлять проводимым количеством электричества. Эти материалы в периодической таблице находятся в одном столбце. Их примерами являются углерод (C), германий (Ge) и сплав арсенид галлия (GaAs). Однако наиболее важным полупроводником и полупроводником, из которого изготавливаются наилучшие электронные микросхемы, является кремний (Si).

Кремний распространен очень широко: его можно обнаружить в песке, стекле и во многих горных породах. Район возле Сан-Хосе в Калифорнии известен под названием "Кремниевая долина" благодаря получившей здесь развитие полупроводниковой промышленности, которая всецело зависит от кремниевых микрочипов. *Переключатели* или *вентили* внутри микропроцессора делаются на основе полупроводников.

Таблица Д.1. Сводная таблица трех основных типов электрических материалов

Изоляторы	Электроны текут плохо	Пластмасса Резина Воздух	Бумага Сухое дерево Стекло
Проводники	Электроны текут хорошо	Медь (Cu) Серебро (Ag) Золото (Au) Припой Вода с ионами Человеческое тело	
Полупроводники	Поток электронов может точно контролироваться	Углерод (C) Германий (Ge)	

Не важно, относится материал к изоляторам, проводникам или полупроводникам, но именно знание того, как каждый из них управляет потоком электронов и как они взаимодействуют в разных комбинациях, является основой понимания работы всех электронных приборов.

Измерение электричества

Как и в случае любого другого процесса или теории, для того, чтобы пользоваться электричеством, его надо уметь измерять. Существует большое количество способов измерения электричества, но в этой книге основное внимание будет уделено рассмотрению таких величин, как *напряжение, ток, сопротивление* и *импеданс*.

Напряжение

Напряжение, иногда называемое *электродвижущей силой* (э.д.с.), представляет собой электрическую силу или давление, которое возникает при разделении электронов и протонов. Возникающая сила толкает в направлении разноименных зарядов и в противоположную сторону от одноименных. Подобный процесс имеет место в электрической батарее, когда химическая реакция вызывает высвобождение электронов на отрицательном полюсе и их перемещение к противоположному положительному полюсу. Разделение зарядов приводит к возникновению напряжения. Напряжение также может создаваться трением (статическое электричество), магнитным полем (электрический генератор) или светом (солнечная батарея).

Напряжение обозначается буквой "V" и иногда буквой "E" (от английского *electromotive force* — электродвижущая сила). Единицей измерения напряжения является вольт (V), который определяется как количество работы на единицу заряда, затрачиваемой на разделение зарядов.

Ток

Электрический ток, или *ток*, представляет собой поток зарядов, который возникает при движении электронов. В электрических цепях ток вызывается потоком свободных электронов. При подаче напряжения и наличии пути для тока электроны двигаются по пути от отрицательного полюса (который отталкивает их) к положительному полюсу (который притягивает их).

Ток обозначается буквой "I". Единицей измерения тока является ампер (A), определяемый как количество зарядов в секунду, проходящих через точку, принадлежащую пути. Электрический ток может быть двух видов: *переменный* и *постоянный*.

Переменный ток

Переменный ток изменяется во времени, меняя свою *полярность* или направление приблизительно 60 раз в секунду. Переменный ток течет в одном направлении, а затем меняет его на противоположное и повторяет процесс. Переменное напряжение положительно на одном полюсе и отрицательно на другом; затем оно меняет свою полярность, и положительный полюс становится отрицательным, а отрицательный — положительным. Этот процесс повторяется непрерывно.

Переменный ток относится к тому типу электричества, которое мы наиболее часто используем в повседневной жизни. Электричество поступает в дом, школу и офис по линиям электроснабжения,

которые передают электричество в форме переменного тока. Электропитание переменного тока подходит для многих типов устройств, но совершенно непригодно для использования внутри таких низковольтных устройств, как компьютеры.

Постоянный ток

Постоянный ток всегда течет в одном направлении, а его напряжение всегда имеет одну и ту же полярность. Один полюс — всегда положительный, а другой — всегда отрицательный. Напряжение на них не изменяется и не меняется на противоположное.

Постоянный ток течет в батарейках карманных фонариков, автомобильных аккумуляторах, питает микрочипы на материнской плате компьютера. Источник питания системы преобразует переменное напряжение сети электропитания в напряжение постоянного тока, которое требуется компьютеру для работы. Многие внешние периферийные устройства (например, принтеры, внешние модемы и внешние накопители) поставляются вместе с адаптером переменного тока, который выглядит как небольшой тяжелый черный ящичек, вставляющийся в настенную розетку. Он также представляет собой преобразователь, изменяющий переменное напряжение, поступающее из стенной розетки, в напряжение постоянного тока, используемое компьютером. Обычно электрические спецификации входного и выходного напряжения обозначены прямо на нем.

Важно понимать, в чем различие между переменным и постоянным током и когда каждый из них используется.

Способность материалов к пропусканию тока можно описать количественно. Это возможно благодаря понятиям *сопротивление* и *импеданс*.

Сопротивление

Материалы, через которые протекает ток, оказывают различное противодействие, или *сопротивление*, движению электронов. Те материалы, которые имеют небольшое сопротивление или вообще его не имеют, называются *проводниками*. Те же, которые не дают току течь или серьезно ограничивают его протекание, называются изоляторами. Величина сопротивления зависит от химического состава материалов.

Сопротивление обозначается буквой "R". Единицей измерения сопротивления является ом (co). Этот символ произносится как "омега" и представляет собой прописную букву греческого алфавита. (Греческие буквы широко используются в математике и физике.)

В электрических системах переменного и постоянного тока поток электронов всегда направлен от отрицательно заряженного источника к положительно заряженному источнику. Однако, для того, чтобы имел место управляемый поток электронов, требуется наличие замкнутой цепи. Вообще говоря, электрический ток течет по пути наименьшего сопротивления. Поскольку металлы, например медь, обеспечивают маленькое сопротивление, то они часто используются в качестве проводников электрического тока. И наоборот, такие материалы, как стекло, резина и пластмасса, имеют более высокое сопротивление. Поэтому они не относятся к хорошим проводникам и часто используются в качестве изоляторов. Они наносятся на проводники для предотвращения ударов током, возгорания и закорачивания цепей.

Импеданс

Импеданс — это общее противодействие протеканию тока (вызываемого как переменным напряжением, так и постоянным). Термин *сопротивление* обычно используется, когда речь идет о напряжениях постоянного тока. Импеданс же является общим термином и определяет, какое сопротивление, или противодействие, оказывается потоку электронов.

Импеданс обозначается буквой "Z". Единицей его измерения, как и для сопротивления, является ом (co). От техников и инженеров часто можно слышать о *согласовании* импедансов; это просто

означает, что для каждого типа среды передачи данных в сети необходимо использовать правильное оборудование. Например, кабель UTP (неэкранированная витая пара) имеет величину характеристического импеданса 100 Ом, а кабель STP (экранированная витая пара) — 150 Ом. Поэтому плата сетевого интерфейса должна обеспечивать наличие соответствующих импедансов, чтобы не допустить отражения (приводящего к нарушению сигналов).

Понятия напряжения тока и сопротивления связаны. Токи текут только в замкнутых контурах, называемых цепями. Эти цепи должны включать проводящие материалы и иметь источник напряжения. Напряжение является причиной протекания тока, тогда как сопротивление и импеданс противодействуют ему.

Формулы $P = PR$ и $V = IR$ связывают мощность (P), сопротивление (R) и напряжение (V). Например, при фиксированном сопротивлении, как у кабеля неэкранированная витая пара, увеличение напряжения в 5 раз приведет к увеличению мощности в 25 раз (квадрат множителя 5)!

Поток воды (рис. Д 4) помогает объяснить понятия напряжения, тока и сопротивления. Чем выше уровень воды (и больше давление), тем сильнее течет вода. Ток воды зависит от того, насколько открыт кран. Аналогично, чем выше напряжение (чем больше электрическое давление), тем больший ток производится. Но потом электрический ток сталкивается с сопротивлением, которое, как кран, уменьшает его. Если рассматривать случай переменного тока, то тогда сила тока зависит от величины импеданса. Роль насоса играет электрическая батарея: она обеспечивает давление для поддержания движения потока.

Ниже приведен список, сводящий воедино все электрические понятия, которые упоминались в предыдущем материале. Эти понятия являются основой для объяснения процессов формирования сигналов и передачи данных. Понимание этих концепций делает относительно легким и понимание процессов, имеющих место на физическом уровне модели OSI.

- Электроны текут в замкнутых контурах, называемых цепями.
- *Напряжение* — электрическое давление, возникающее из-за разделения электрических зарядов (+ и —).

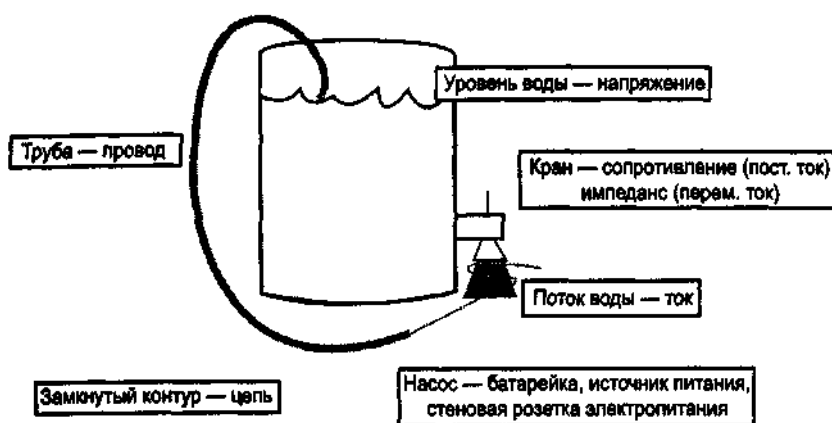


Рис. Д.4. Можно провести полезные аналогии между потоком воды и электричеством

- *Ток* — поток заряженных частиц, обычно электронов.
- *Сопротивление* — свойство материала, которое оказывает противодействие протеканию тока и может управлять величиной электрического тока.
- *Импеданс* — эквивалент сопротивления, но для цепей переменного тока и импульсных цепей.
- *Замкнутая цепь* — проводящий путь. *Разомкнутая цепь* — разрыв в проводящем пути.
- Напряжение вызывает электрический ток; сопротивление и импеданс ограничивают величину тока.

Электрическая земля

Другим связанным с электричеством понятием, которое часто встречается при работе с сетями, является понятие электрической земли. Понимание термина земля может быть затруднено, поскольку люди часто используют его в различных целях.

Землей называется место на земельном участке, примыкающем к дому (обычно в виде закопанных труб водоснабжения), которое в конечном итоге обеспечивает не прямое соединение с розетками электрической сети. Когда вы используете бытовой электроприбор с вилкой, имеющей три штырька, то третий штырь является землей. Он обеспечивает электронам в случае короткого замыкания дополнительный проводящий путь на землю, а не через ваше тело.

Земля также может обозначать точку отсчета или уровень нулевого напряжения при выполнении электрических измерений. Напряжение создается разделением зарядов, а это означает, что измерять напряжение необходимо между двумя точками. По этой причине мультиметр (прибор, который измеряет напряжение, ток и сопротивление) имеет два провода. Черный провод называют землей или опорной землей. Отрицательный полюс батареи также называют нулевым или опорной землей.

На рис. Д. 5 показан знакомый объект: точка подвода электричества через стенную розетку. Два верхних соединителя подводят электропитание, круглый соединитель внизу защищает людей и оборудование от ударов током и коротких замыканий цепи. Этот соединитель называется *защитным заземлением*. В электрическом оборудовании, в котором используется защитное заземление, провод защитного заземления соединяется со всеми его открытыми металлическими частями. Материнская плата и вычислительные цепи в вычислительном оборудовании электрически соединены с шасси компьютера. Это одновременно также подсоединяет их к проводу защитного заземления, который используется для рассеивания статического электричества. Целью соединения открытых металлических частей компьютерного оборудования с проводом защитного заземления является предотвращение возникновения на таких металлических частях опасного для здоровья напряжения, которое может попасть туда в результате какой-либо неисправности в разводке внутри устройства.

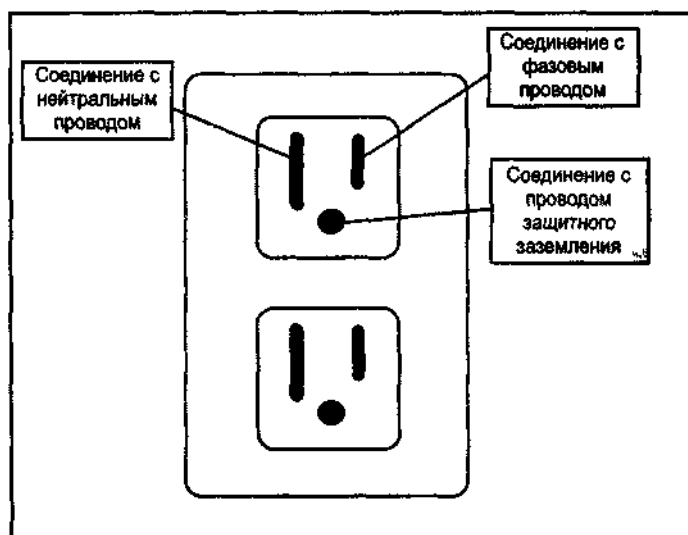


Рис. Д. 5. Знакомые нейтральный и фазовый провода, а также провод защитного заземления стенной розетки электропитания

Примером неисправности, которая может возникнуть внутри сетевого устройства, является случайное соединение провода под напряжением с шасси. Если случается такая неисправность, то провод защитного заземления, соединенный с устройством, послужит в качестве низкоомного пути к земле. Соединение с защитным заземлением обеспечивает путь с меньшим сопротивлением, чем сопротивление вашего тела.

При правильной установке низкоомный путь, обеспечиваемый проводом защитного

заземления, имеет достаточно низкое сопротивление и пропускает достаточно невысокий ток, чтобы не допустить возникновения опасно высоких напряжений. Эта цепь напрямую соединяет провод под напряжением с землей.

Протекание электрического тока по этому пути на землю приводит к срабатыванию защитных устройств (например, пакетных выключателей или автоматических выключателей с реле утечки на землю). Разрывая цепь, эти выключатели прекращают поток электронов и снижают опасность электрического удара. Однако выключатели защищают людей и электропроводку в доме, но для защиты вычислительного и сетевого оборудования требуются дополнительные средства защиты, которые часто представлены подавителями всплесков напряжения и источниками бесперебойного питания.

Потребляемая компьютерами и сетевым оборудованием электрическая мощность подается с трансформатора, который обычно устанавливается на опоре линии электропередачи (рис. Д.6). Трансформатор, который также подсоединен к земле, понижает высокое напряжение, поступающее с электростанции, до напряжения 120 или 240 вольт, которое используется обычными бытовыми электроприборами.

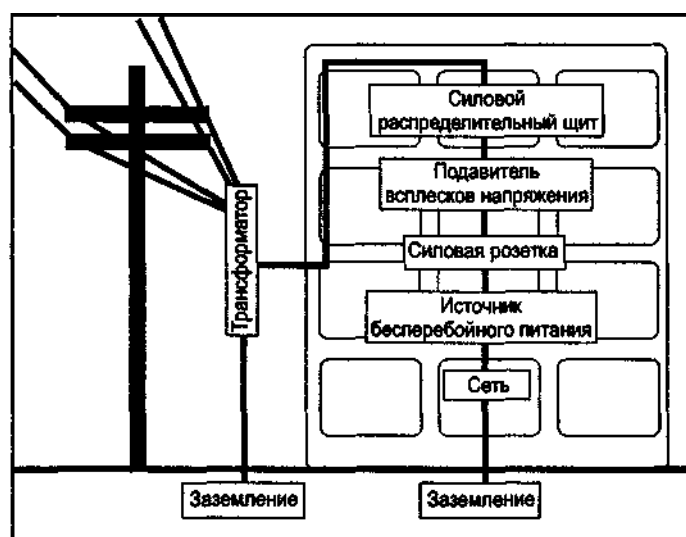


Рис. Д.6. Подавители всплесков напряжения, источники бесперебойного питания и стенные розетки соединены с трансформатором и заземлением

Теперь вы знаете, как электричество с электростанции попадает в дома, школы и на рабочие места. Все рассмотренные нами соображения играют свою роль в главных строительных блоках электронных устройств — цепях, из которых состоит все используемое нами электронное оборудование.

Простая цепь

Электроны текут только в цепях, которые представляют собой замкнутые или полные контуры. Схема, приведенная на рис.Д.7., является примером простой цепи, обычной для карманного фонарика. Химический процесс в батарейке вызывает разделение зарядов, что приводит к возникновению напряжения или электрического давления, позволяющего электронам течь через различные приборы. Линии представляют собой проводник, обычно - это медный провод.

Переключатель можно представить в виде двух концов одного провода, которые могут разъединиться (или разрываться) и соединиться (тогда их называют связанными или закороченными), тем самым запрещая или позволяя течь электронам. Лампочка обеспечивает сопротивление потоку электронов, заставляя тех высвободить свою энергию в виде света. Применяемые в сетях цепи используют те же принципы, что и эта очень простая цепь, но они значительно сложнее.

Цепи лежат в основе работы сетевого оборудования, включая компьютеры. Все электронные устройства в конечном итоге состоят из цепей и переключателей. В используемых нами электронных устройствах показанный на рис Д.7 простой пример повторяется миллионы раз.

Как правило, микрочип содержит на четверти квадратного дюйма (1,6 см²) от трех до пяти миллионов таких переключателей

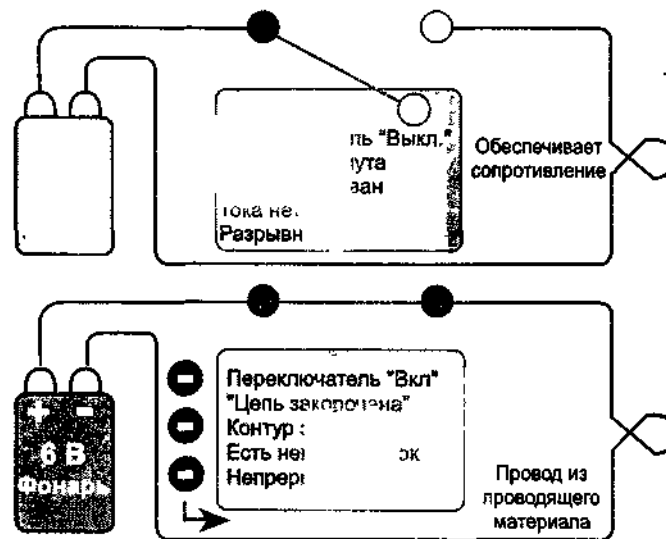


Рис. Д.7. Простая цепь 6-вольтового карманного фонарика

Резюме

- Электричество основано на способности электронов атомов определенных типов отделяться или течь за пределами этих атомов.
- Противоположные заряды притягиваются, а одноименные — отталкиваются. В электрических цепях ток течет от отрицательного полюса к положительному.
- В зависимости от способности допускать протекание электронов материалы могут подразделяться на изоляторы, проводники и полупроводники.
- Понятия напряжения, тока, сопротивления и импеданса являются теми средствами измерения электричества, которые необходимы, чтобы иметь возможность проектировать и изготавливать электронные устройства.
- Переменный и постоянный ток — это два типа электрического тока. Переменный ток используется для подачи электроэнергии в наши дома, школы и на рабочие места. Постоянный ток используется в устройствах, функционирование которых зависит от электрических батарей.
- Электрическое заземление обеспечивает опорный уровень, относительно которого измеряется напряжение. Оно также используется в механизме защиты от опасных для жизни ударов электрического тока.
- Все электронное оборудование состоит из электрических цепей, которые управляют потоком электронов посредством переключателей.

Приложение Е

Формирование сигналов и передача данных

В приложении Д, "Основы электроники и сигналы", были изложены основополагающие физические принципы, управляющие взаимодействием компьютеров в сети. Физический уровень модели OSI представляет собой определенное окружение, в котором необходимое физическое явление подчиняется целям формирования сигналов. *Формирование сигналов* — это способы, с помощью которых становится возможной передача данных. *Передача данных* — это средства, с помощью которых сетевые устройства могут работать в рамках остальных уровней модели OSI.

Интересно понять, как работает подход на основе движения снизу вверх, который, собственно, и делает возможным мир сетевых взаимодействий. Все, что известно и делается в области организации работы компьютеров в сети, в конечном счете, зависит от основополагающих физических принципов электричества. И точно так же, как легче освоить принципы IP-адресации и назначения подсетей, если есть четкое представление о двоичных числах и соответствующих преобразованиях, значительно легче понять организацию взаимодействия в сети на физическом и канальном уровнях, если есть четкое представление о физике электричества.

В данном приложении подробно объяснены различные концепции, связанные с формированием сигналов и передачей данных. Излагаемый материал завершается описанием формирования кадров из битов на физическом уровне модели OSI, чем и заканчивается рассмотрение физического уровня в данной книге.

Сигналы и шумы в коммуникационных системах

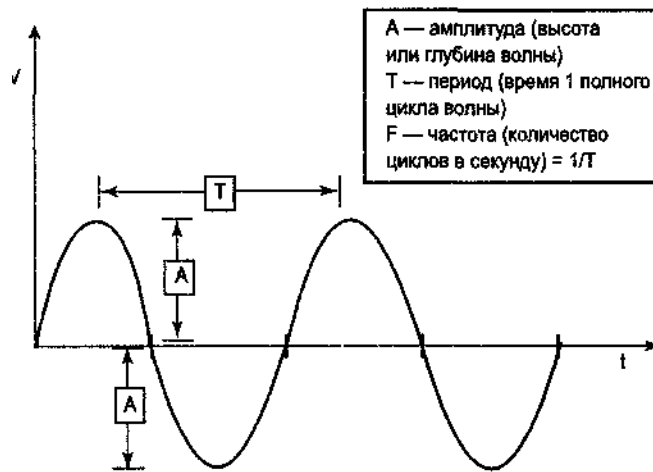
Термином *сигнал* называют напряжение требуемой формы, картину распределения света или модулированную электромагнитную волну. Каждый из этих объектов может переносить данные в сети. Существуют два основных типа сигналов: *аналоговые* и *цифровые*. Рассмотрим специфические свойства каждого из этих типов сигналов.

Сравнение аналоговых и цифровых сигналов

Как уже говорилось, одним из типов сигналов являются аналоговые сигналы, которые имеют следующие характеристики

- Они волновые.
- Непрерывно меняющийся график зависимости напряжения от времени.
- Типичны в природе.
- Широко использовались в телекоммуникациях более 100 лет.

На рис. Е1 показана *синусоидальная волна*, имеющая две важные характеристики: *амплитуду* (A), т.е. высота и глубина волны, и *период* (T), т.е. продолжительность одного полного цикла (в нашем случае это временной параметр). Можно вычислить частоту волны (f), измеряемую количеством циклов в секунду, для чего необходимо воспользоваться формулой $f = 1/T$.



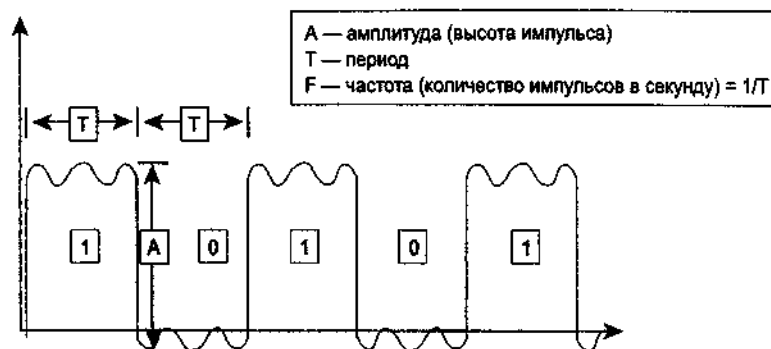
- Непрерывное напряжение
- Может иметь любое значение напряжения
- "Волнистый" характер напряжения во времени
- Возможно множество способов кодирования

Рис. Е.1. Пример аналогового сигнала, имеющего вид синусоидальной волны

Другой тип сигналов — цифровые. Эти сигналы обладают следующими характеристиками.

- Дискретный (меняется скачкообразно) график зависимости напряжения от времени.
- Типичность скорее для техногенных (вызванных человеком) явлений, чем для природных.

На рис. Е.2 показан цифровой сетевой сигнал. Он имеет фиксированную амплитуду, но его амплитуда, период и частота могут меняться. Цифровые сигналы можно приблизительно представить прямоугольными волнами (рис. Е.3) с мгновенными переходами от состояния с низким уровнем напряжения в состояние с высоким уровнем. Хотя это и приблизительное представление, оно вполне разумно и дальше часто используется.



- Не непрерывные (дискретные) импульсы
- Может иметь только один из двух уровней напряжения
- Напряжение меняется скачком между уровнями
- Состоит из множества определенных синусоидальных волн

Рис. Е.2. Пример цифрового сигнала

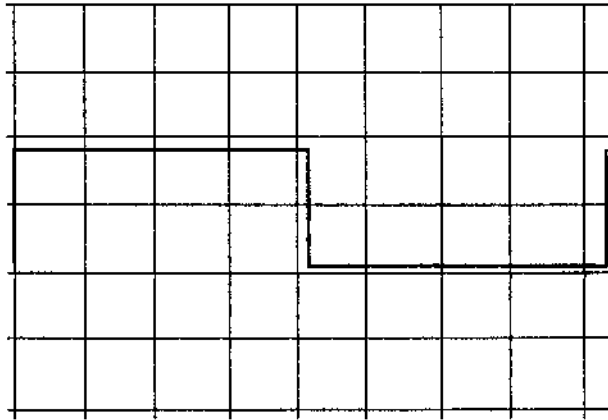


Рис. Е.3. Прямоугольная волна. Такие волны могут быть аппроксимированы синусоидальными волнами

Использование цифровых сигналов для построения аналоговых сигналов

Французский физик Жан Батист Фурье (1768-1830) математически доказал, что волновой процесс любой формы можно представить специальной суммой синусоидальных волн с гармонически связанными частотами, кратными некоей базовой частоте. Фундаментальность принципа состоит в том, что сложные волны можно строить из простых волн. Именно так работают устройства по распознаванию голоса и электронные кардиостимуляторы.

Прямоугольную волну или прямоугольный импульс можно построить с использованием правильной комбинации синусоидальных волн. На рис. Е.4 показано, как прямоугольную волну (цифровой сигнал) можно построить с помощью синусоидальных волн (аналоговых сигналов). Это важно помнить при рассмотрении того, что происходит с цифровым импульсом в процессе его прохождения по сетевой среде передачи данных. Бесконечная сумма синусоид, которая "итого" равна прямоугольной волне, называется *рядом Фурье* (эта тема изучается в курсе высшей математики).

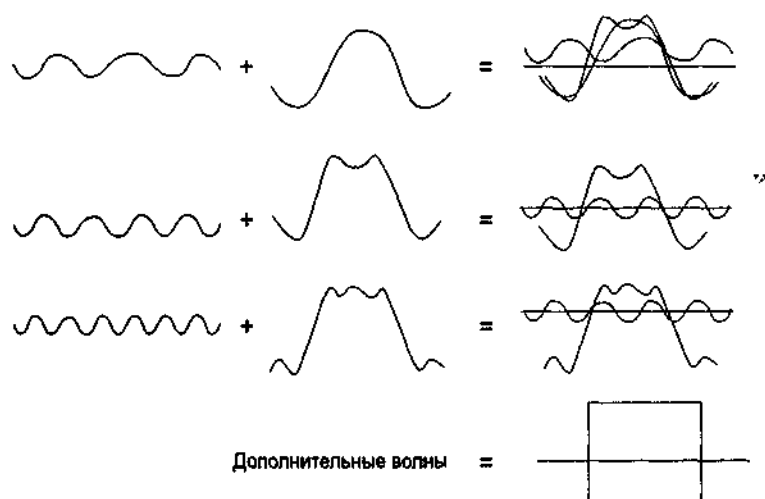


Рис. Е.4. Прямоугольная волна, аппроксимируемая рядом синусоид

Теперь мы знаем, что цифровые волны могут аппроксимироваться суммами синусоидальных волн. Поэтому цифровые сигналы могут строиться из аналоговых. А сейчас мы рассмотрим, как электрические сигналы представляют бит.

Представление одного бита в физической среде

Сети передачи данных стали все более зависимыми от цифровых (двоичных, с двумя устойчивыми состояниями). Основным строительным блоком информации является двоичная цифра, известная под названием бит, или импульс. Один бит в проводящей электричество среде представляет собой электрический сигнал, соответствующий двоичному 0 или двоичной 1. Это может быть реализовано просто как 0 вольт — для двоичного нуля и +5 вольт — для двоичной единицы (или может использоваться более сложное кодирование). Во всех сетевых средах, использующих для передачи сообщений напряжение, важной является концепция опорной земли сигналов.

Для правильного функционирования опорная земля сигналов должна располагаться как можно ближе к цифровым цепям компьютера. Инженеры добиваются этого, проектируя печатные платы, в которых формируются плоскости земли. В свою очередь, корпуса компьютеров используются в качестве общей точки соединения плоскостей земли печатных плат, чем и формируется опорная земля сигналов. На диаграммах, подобных приведенной на рис. Е.5, опорная земля сигналов определяет положение линии 0 вольт.

В случае применения оптических сигналов двоичный 0 обычно кодируется низким уровнем света или отсутствием света вообще (темнотой), а двоичная единица — светом с более высокой интенсивностью (яркостью). Могут использоваться и другие более сложные способы кодирования.

При беспроводной передаче сигналов двоичный 0 может представляться короткой пачкой электромагнитных волн, а двоичная 1 — более длинной пачкой электромагнитных волн или другой более сложной картиной распределения волн. Бит со значением 0 обычно изображается горизонтальной линией, идущей по оси времени (ось t) (на рис. Е.5 — это черная линия). Для показа бита со значением 1 также обычно используется линия, соответствующая уровню напряжения +5 В (верхняя горизонтальная линия на графике зависимости напряжения от времени слева).

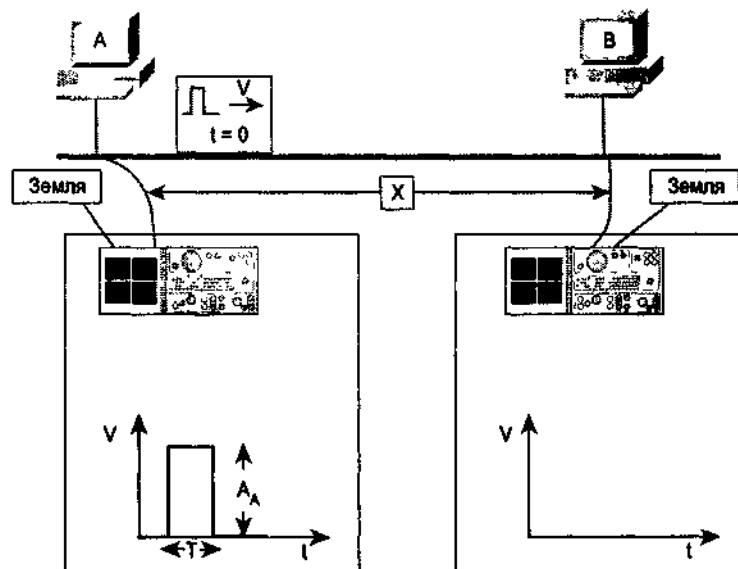


Рис. Е.5. Для установки базовой линии отсчета используется опорная земля сигналов

На сигнал бита могут оказывать влияние шесть следующих факторов.

- Распространение.
- Атенюация.
- Отражение.
- Шум.
- Проблемы синхронизации.

- Конфликты.

Распространение

Под *распространением* понимают движение в среде. Когда плата сетевого интерфейса вводит в физическую среду импульс напряжения или света, то этот прямоугольный импульс, состоящий из волн, начинает двигаться (распространяться) в среде. Распространение означает, что порция энергии, соответствующая биту со значением 1, движется из одного места в другое. Скорость, с которой происходит это движение, зависит от реального материала, используемого в среде, геометрии (структуры) среды и частоты импульсов. Время, которое занимает движение бита от одного конца среды до другого и назад, называется *временем кругового обхода* (round trip time, RTT). Если предположить, что отсутствуют другие задержки, то время движения бита до противоположного конца среды равно $RTT/2$ (рис. Е 6).

Тот факт, что бит перемещается с некоторой скоростью, не создает проблемы для сети. Сигналы двигаются настолько быстро, что для человека это иногда выглядит как мгновенная передача. Но в любом случае важно учитывать различные временные интервалы, связанные с распространением сигналов в сети.

Можно рассмотреть два крайних случая: либо время перемещения бита равно 0, т.е. он перемещается мгновенно, либо он перемещается бесконечно долго. Согласно теории относительности Альберта Эйнштейна, первый случай не может соответствовать действительности, ибо никакая информация не может перемещаться со скоростью большей скорости света в вакууме. Это означает, что перемещение бита занимает по крайней мере некоторое, хотя и малое, время. Второй случай тоже не соответствует действительности, так как при правильном выборе оборудования всегда можно определить время прихода импульса. Незнание времени распространения представляет проблему, поскольку бит может приходиться в некоторый пункт назначения либо слишком рано, либо слишком поздно.

Эта проблема решаема. Как уже говорилось, наличие времени распространения (см. рис Е.6) само по себе не создает каких-либо сложностей; это просто факт, который надо себе четко представлять. Если время распространения слишком велико, необходимо пересмотреть способ учета такой задержки в остальной части сети. Если задержка распространения слишком мала, то, возможно, биты надо замедлить или ввести их временное хранение (этот метод называется *буферизацией*), чтобы остальное сетевое оборудование успевало их улавливать.

Аттенюация

Аттенюацией называется потеря силы сигнала при его движении в физической среде, в частности, когда длина кабеля превышает максимально рекомендуемую величину. Это означает, что сигнал напряжения бита со значением 1 уменьшает свою амплитуду за счет передачи энергии от собственно сигнала кабелю (рис. Е.7). Хотя электрическая аттенюация может быть уменьшена благодаря тщательному подбору материалов (например, использование меди вместо углерода) и учету геометрии (формы и расположения проводов), все же из-за наличия электрического сопротивления некоторые потери неизбежны. Аттенюация имеет место и в случае оптических сигналов: оптическое волокно поглощает и рассеивает некоторую часть световой энергии по мере продвижения по нему импульса света, или бита со значением 1. Этот эффект может быть минимизирован путем подбора длины волны или цвета света. Он также зависит от того, используется ли одномодовое или многомодовое оптоволокно, и от типа конкретного стекла, применяемого для изготовления самого оптического волокна. Но даже при оптимальном выборе некоторые потери сигнала неизбежны.

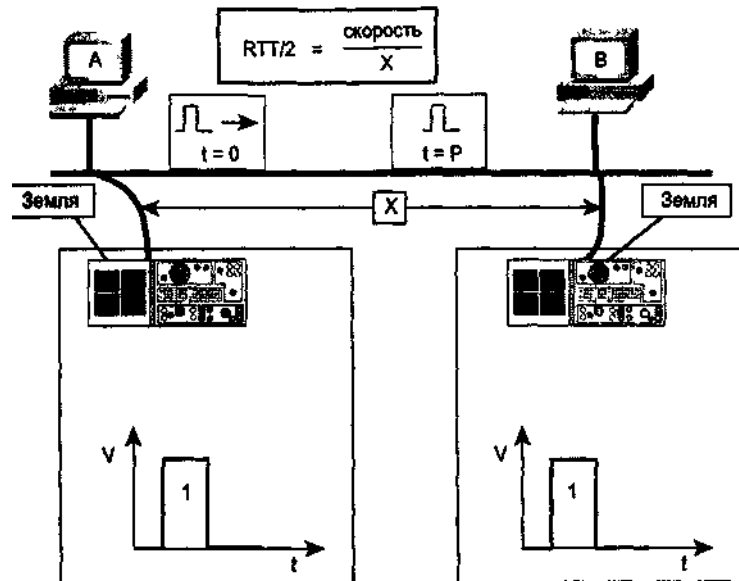


Рис. Е 6. Знакомая формула — расстояние = скорость × время — иногда очень кстати при организации работы сети. На рисунке показано одно из применений этой формулы: расчет задержки распространения (половина времени кругового обхода) бита, движущегося от хост-машины А к хост-машине В

Радиоволны и микроволны также подвержены аттенюации, поскольку они поглощаются и рассеиваются молекулами атмосферы.

Аттенюация может воздействовать на сеть, поскольку она ограничивает длину кабелей сети, по которым посылаются сообщения. Если кабель слишком длинен, то единичный бит, посланный отправителем, к моменту прихода получателю может выглядеть как бит со значением 0.

Эту проблему можно решить путем выбора соответствующей среды передачи данных для конкретного сценария проектирования. Другой путь решения проблемы заключается в использовании повторителей, если требуемая длина кабеля превышает имеющиеся ограничения на его максимальную протяженность. Существуют повторители для электрических, оптических и радиоканалов передачи битов.

Отражение

Чтобы понять, что такое отражение, представим, что у вас в руках есть резинка или скакалка, другой конец которой держит натянутым ваш друг. Теперь представим, что вы посылаете своему другу импульс или сообщение в виде единичного бита. Если наблюдать внимательно, то можно увидеть небольшую волну (импульс), которая возвращается (отражается) к вам назад.

Отражение имеет место и в электрических сигналах. Если импульсы напряжения или биты сталкиваются с неоднородностью, то некоторая часть энергии может быть отражена. Это может произойти в месте соединения различных или даже одинаковых материалов. Если эту энергию тщательно не контролировать, она может повредить другие биты. Необходимо помнить, что хотя сейчас мы рассматриваем случай передачи одного бита, в реальных сетях каждую секунду посылаются миллионы или даже миллиарды бит в секунду, что требует отслеживания этой энергии отраженных импульсов. В зависимости от качества кабельной системы и соединений отражения могут быть или не быть проблемой. Комплексная электрическая характеристика, которая связана с сопротивлением (противодействием потоку электронов) и реактивностью (противодействием изменению напряжения и тока), и называется импедансом.

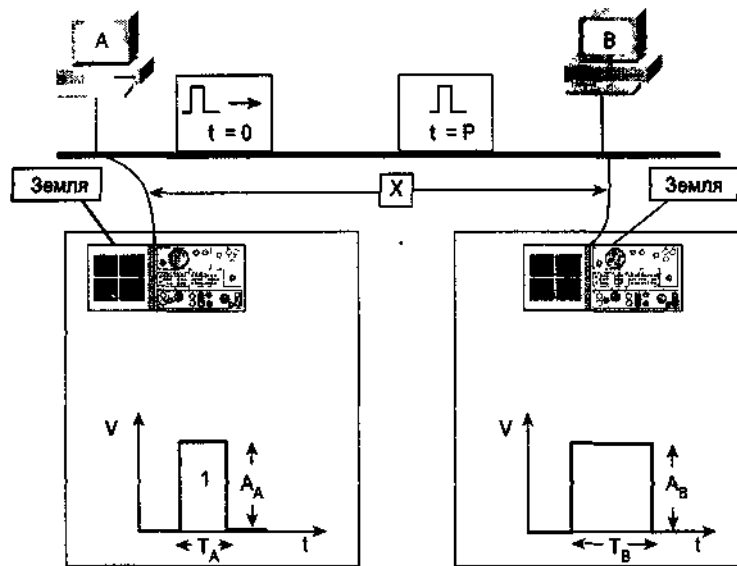


Рис. Е.7 *Аттенуация — это потеря сигналом энергии по мере увеличения расстояния, проходимого битом по кабелю. Это явление заметно на примере прямоугольной волны, изображенной на рисунке справа, у которой по сравнению с исходными условиями, показанными слева, уменьшается амплитуда и увеличивается длина основания*

Оптические сигналы отражаются там, где они наталкиваются на неоднородность в оптическом волокне, например в том месте, где разъем вставляется в устройство. Этот эффект можно наблюдать ночью, когда вы выглядываете в окно. Вам видно ваше отражение в окне, хотя оно и не является зеркалом. Некоторая часть света, отражаемая вашим телом, отражается окном. То же самое происходит с радио- и микроволнами, когда они сталкиваются с различными слоями атмосферы.

Подобное явление может стать причиной проблем в сети (рис. Е.8). Для оптимальной производительности сети важно, чтобы ее среда передачи данных имела конкретное значение импеданса, чтобы согласовываться по этому параметру с электрическими компонентами платы сетевого интерфейса. Если среда не имеет нужного импеданса, то сигналы подвержены отражению и возникает интерференция. Кроме того, может иметь место несколько отраженных импульсов. Независимо от того, является ли система электрической, оптической или беспроводной, рассогласование импедансов вызывает отражения. Если количество отражаемой энергии достаточно велико, то двоичная система с двумя устойчивыми состояниями может запутаться во всей этой рикошетирующей туда-сюда энергии. Решение этой проблемы состоит в обеспечении точного согласования импедансов всех элементов сети. Множество технологий позволяют избежать рассогласования импедансов.

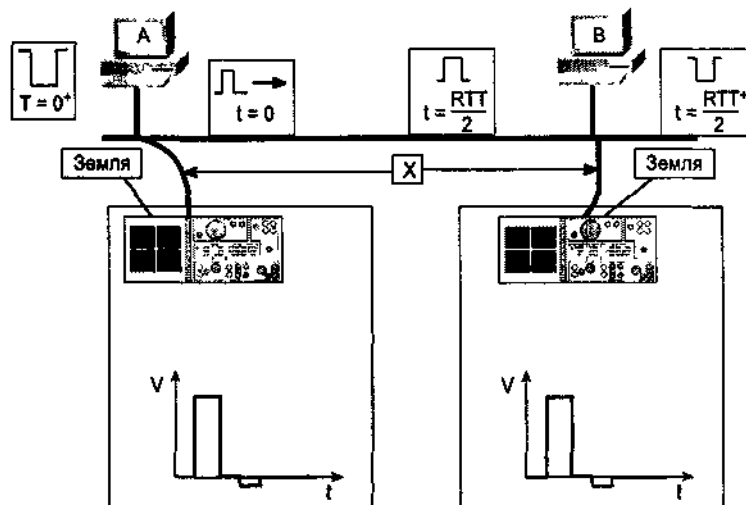


Рис. Е 8 Отражение вызывается неоднородностью среды и может быть результатом перегиба кабеля или плохой заделки его конца

Шум

Шумом в процессе обмена данными называется нежелательное суммирование с сигналом в виде напряжения, оптическим или электромагнитным сигналом дополнительных сигналов. Другими словами, каждый бит получает дополнительные нежелательные сигналы от различных источников. Слишком высокий уровень шума может разрушить сигнал бита со значением 1, превратив его в двоичный 0 и, таким образом, уничтожив сообщение, состоящее из одного бита с единичным значением. Или из-за шума сообщение в виде бита со значением 0 может быть ошибочно принято за сообщение, содержащее бит со значением 1. Не бывает электрических сигналов без шума, однако величину отношения сигнал/шум необходимо поддерживать как можно более высокой. На рис. Е.9 показаны пять источников шума, которые могут оказывать влияние на бит в проводе.

Приконцевые перекрестные помехи (NEXT)

Если электрический шум в кабеле возникает от сигналов в соседних проводах кабеля, то такой шум называют перекрестными помехами. Аббревиатура NEXT (near-end crosstalk) обозначает приконцевые перекрестные помехи. Если два провода кабеля находятся рядом друг с другом и не свиты, то энергия из одного провода может наводить сигнал в другом. Это вызывает шум на обоих концах заделываемого в разъем кабеля. Существует много видов перекрестных помех, которые следует принимать во внимание при создании сетей.

С приконцевыми перекрестными помехами можно справиться с помощью технологии заделки, строгого следования стандартным процедурам заделки и использования качественных кабелей типа "витая пара".

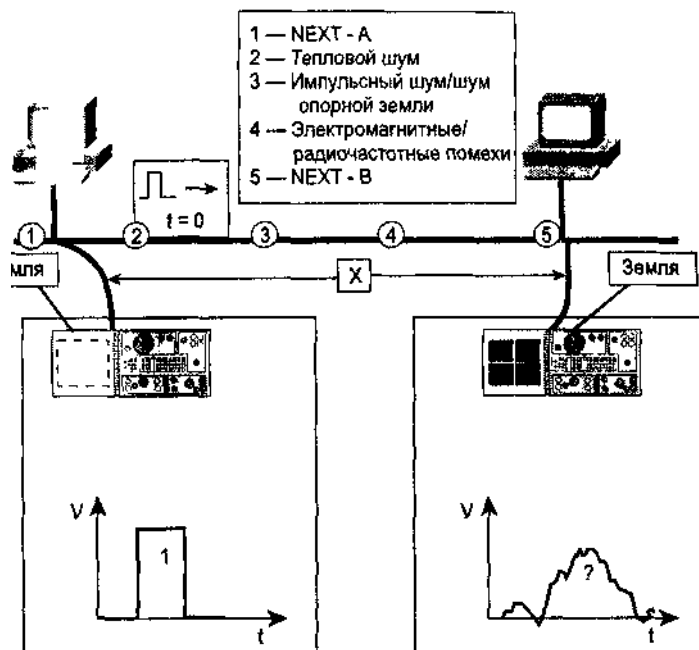


Рис. Е 9. Пять источников шума в кабеле

Тепловой шум

Тепловой шум представляет собой случайное движение электронов, вызываемое температурными флуктуациями в среде, и обычно оказывает относительно небольшое влияние на сигналы. С тепловым шумом поделать ничего нельзя. Можно только обеспечить сигналам достаточную амплитуду, чтобы влияние теплового шума оставалось незаметным.

Сетевой шум и шум опорной земли

Сетевой шум и шум опорной земли представляют серьезную проблему при организации взаимодействия в сети. Сетевой шум является источником проблем в домах, школах и офисах. Электроэнергия подводится к бытовым электроприборам и машинам по проводам, спрятанным в стенах, полу и потолках. Следовательно, внутри зданий шум от силовой электропроводки — повсюду. Если не принять соответствующих мер, то этот шум может быть причиной проблем в сети.

В идеале опорная земля сигналов должна быть полностью изолированной от заземления. Такая изоляция будет удерживать попадание утечек электропитания и всплесков напряжения на опорную землю сигналов. Но проблема в том, что шасси (корпус) вычислительного устройства играет роль как опорной земли сигналов, так и земли линий силового электропитания. Поскольку существует связь между опорной землей сигналов и землей электропитания, то проблемы с землей электропитания могут привести к помехам в системе обработки данных. Такие помехи могут быть трудно обнаруживаемыми и плохо поддающимися прослеживанию. Обычно проблемы возникают из-за того, что служба главного энергетика и монтажники не заботятся о длине проводов нейтрали и земли, подходящих к каждой розетке электропитания. К сожалению, если эти провода длинные, то они могут действовать для электрического шума в качестве антенны. Этот шум накладывается на цифровые сигналы (биты), которые компьютеры должны иметь возможность распознавать и обрабатывать.

Шума, поступающего от стоящего рядом видеомонитора или привода накопителя на жестких дисках, может оказаться достаточно, чтобы привести к возникновению ошибок в компьютерной системе. Происходит это из-за того, что он взаимодействует с полезными сигналами (изменяя форму и уровень напряжения), не давая компьютеру идентифицировать передние и задние фронты прямоугольной волны. Эта проблема может усугубляться еще больше, если компьютер имеет плохое заземление.

Чтобы избежать возникновения проблем из-за описанных выше шумов электропитания и опорной земли, важно работать в тесном сотрудничестве со службой главного энергетика и энергокомпаниями. Это позволит иметь высококачественный и самый короткий контур электрического заземления. Один из способов добиться этого состоит в том, чтобы определить стоимость получения отдельного силового трансформатора, выделенного под область установки локальной сети. Если такой вариант приемлем, то можно контролировать подключение к вашей электросети других устройств. Накладывая ограничение на то, как и где подключаются такие устройства, как моторы и сильноточные электрические нагреватели, можно во многом исключить влияние генерируемого ими электрического шума.

В службе главного энергетика можно попросить об установке отдельных силовых распределительных панелей для каждого офиса. Эти панели известны под названием щитов пакетных выключателей. Так как провода нейтрали и заземления от каждой розетки сходятся вместе в щите пакетных выключателей, такой шаг увеличивает шансы на укорочение длины земли сигналов. Хотя установка отдельных силовых распределительных панелей для каждого кластера компьютеров увеличивает предварительные расходы на прокладку электросетевой разводки, это уменьшает длину проводов заземления и ограничивает влияние некоторых типов шумов, маскирующих электрические сигналы.

Электромагнитные и радиочастотные помехи

Внешние источники электрических импульсов, способных атаковать качество электрических сигналов в кабеле, включают молнии, электрические моторы и радиосистемы. Такие типы помех называются электромагнитными и радиочастотными помехами. Каждый провод в кабеле может действовать в качестве антенны. Когда такое происходит, провод фактически поглощает электрические сигналы от других проводов кабеля и от внешних электрических источников. Если возникающий в результате электрический шум достигает достаточно высокого уровня, то для платы сетевого интерфейса становится сложным отделять шум от сигналов данных. Проблема еще и в том, что в большинстве локальных сетей используются частоты, лежащие в диапазоне от 1 до 100 МГц, а так получается, что именно в этом диапазоне лежат сигналы ЧМ-радио и телевизионные сигналы. Кроме того, в этом же диапазоне лежат рабочие частоты многих бытовых приборов.

Чтобы понять, как электрический шум, независимо от типа источника, воздействует на цифровые сигналы, представим, что по сети необходимо переслать данные, представляемые двоичным числом 1011001001101. Компьютер преобразовывает двоичное число в цифровой сигнал. На рис. ЕЛО показано, как выглядит цифровой сигнал для числа 1011001001101. Цифровой сигнал начинает двигаться по среде к пункту назначения. Как оказалось, получатель стоит рядом с розеткой электропитания, которая имеет длинные провода как нейтрали, так и заземления. Эти провода действуют для электрического шума как антенны. На рис. ЕЛО также показано, как выглядит электрический шум. Поскольку шасси компьютера получателя используется и как заземление, и как опорная земля сигналов, то сгенерированный шум накладывается на цифровой сигнал, который принимает компьютер. Внизу на рис. ЕЛО показано, что происходит с сигналом, когда он складывается с этим электрическим шумом. В результате вместо считывания сигнала как число 1011001001101 компьютер читает его как 1011000101101, делая данные ненадежными (поврежденными).

Существует много способов ограничения электромагнитных и радиочастотных помех. Одним из них является увеличение диаметра проводников. Другой путь заключается в улучшении типа используемого изолирующего материала. Однако такие изменения увеличивают диаметр и стоимость кабеля быстрее, чем они улучшают его качество. Поэтому для проектировщиков сетей более типична закладка в проект кабеля хорошего качества и задание требований на максимально рекомендуемую длину кабеля между узлами.

Для нейтрализации электромагнитных и радиочастотных помех разработчики кабелей успешно используют два метода: *экранирование* и *подавление*. В кабеле, использующем метод экранирования, каждую пару проводов или группу пар проводов окружает металлическая оплетка или фольга. Подобный экран выступает в качестве барьера для любых сигналов помех.

Однако увеличение диаметра проводника и использование покрывала из оплетки или фольги увеличивает диаметр кабеля и его стоимость. Поэтому для защиты провода от нежелательных помех чаще используется метод подавления.

Когда электрический ток течет по проводнику, он создает вокруг проводника слабое круговое магнитное поле (рис. Е.11). Направление силовых магнитных линий определяется направлением тока, протекающего по проводнику. Если два провода являются частью одной и той же электрической цепи, то электроны от отрицательного полюса источника напряжения текут к пункту назначения по одному проводу. Затем электроны текут от пункта назначения к положительному полюсу источника напряжения по другому проводу. Теперь, если два этих провода электрической цепи разместить близко друг к другу, то их магнитные поля будут точно противоположны друг другу. Таким образом, два магнитных поля подавят одно другое. Более того, они также будут подавлять и некоторые внешние магнитные поля. Свивка проводов может еще усилить этот эффект. Используя метод подавления совместно с перевивкой проводов, разработчики кабелей могут обеспечить эффективный способ самоэкранирования пар проводов среды передачи данных в сети.

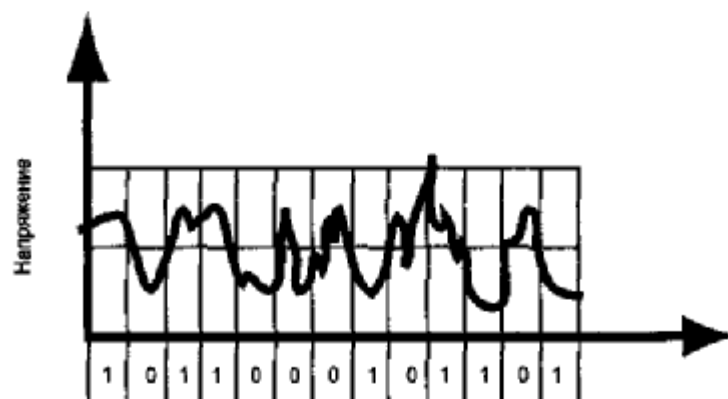
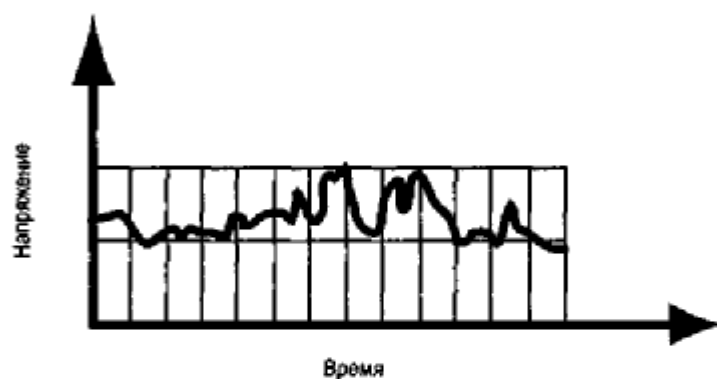
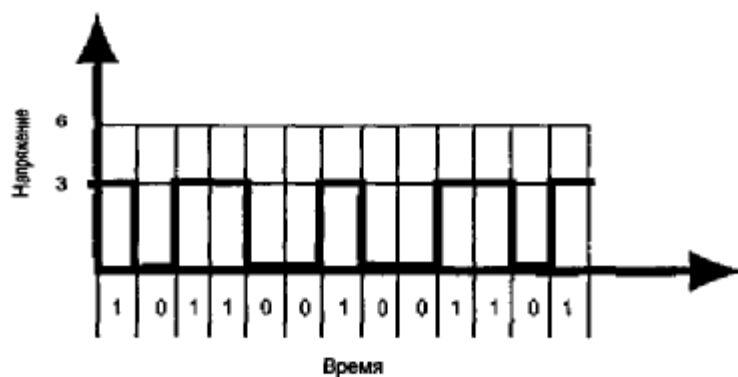


Рис. Е.10 Первый график представляет собой цифровой сигнал, второй — электрический шум, а на третьем показан суммарный результат. Заметим, что выделенные красным цветом 0 и 1 поменялись местами относительно оригинала

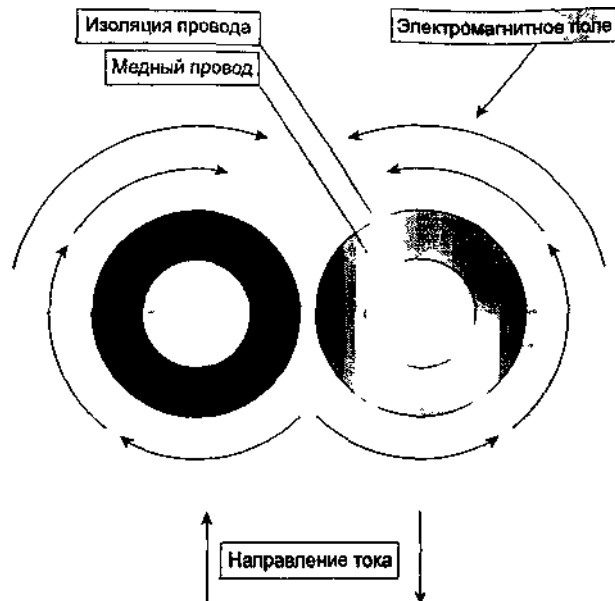


Рис. Е 11. Электрический ток в проводе индуцирует вокруг него магнитное поле

Дисперсия, неустойчивая синхронизация и запаздывание (проблемы синхронизации)

Хотя дисперсия, неустойчивая синхронизация и запаздывание фактически представляют собой три разные проблемы, которые могут произойти с битом, они сгруппированы вместе, поскольку каждая из них оказывает влияние на одно и то же — на временную синхронизацию бита. Так как мы здесь пытаемся разобраться в том, какие проблемы могут иметь место, когда в среде передачи данных путешествуют миллионы и миллиарды битов в секунду, то синхронизация играет весьма существенную роль.

Дисперсией называется явление расширения сигнала во времени (рис. ЕЛ 2). Степень дисперсии зависит от типа среды передачи данных. Если она достаточно серьезна, то один бит может начать накладываться на следующий бит, затрудняя определение, где заканчивается один бит и начинается другой. Поскольку надо посылать миллионы или миллиарды бит в секунду, необходимо быть особенно внимательным, чтобы не допустить расширение сигналов. Дисперсия может быть минимизирована за счет соответствующего проектирования кабеля, ограничения его длины и нахождения подходящего значения импеданса. В оптическом волокне дисперсией можно управлять путем использования света лазера с точно заданной длиной волны. При беспроводной связи дисперсию можно минимизировать выбором частот, используемых для передачи.

Все цифровые системы тактируются. Это означает, что тактовые импульсы управляют работой электроники. Именно тактовые импульсы заставляют центральный процессор вычислять, данные — записываться в память и плату сетевого интерфейса — посылать биты. Если генератор тактовых импульсов на машине-отправителе не синхронизирован с машиной-получателем, то в результате получаем *неустойчивую синхронизацию*. Это означает, что биты прибывают немного раньше или немного позже, чем ожидается. Справиться с неустойчивой синхронизацией можно с помощью ряда сложных механизмов синхронизации тактовых импульсов, включая аппаратную и программную или протокольную синхронизации.

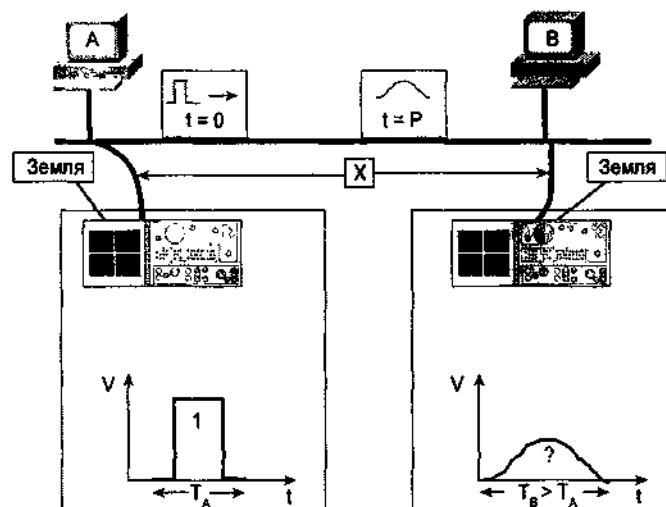


Рис. Е.12. Дисперсия приводит к удлинению цифровых сигналов иногда до такой степени, что сетевые устройства не могут различить, где заканчивается один бит и начинается другой

Запаздывание, известное и под названием задержка, вызывается двумя основными причинами. Во-первых, согласно теории относительности Эйнштейна, ничто не может перемещаться быстрее скорости света в вакууме ($3,0 \times 10^8$ м/с). Сигналы в беспроводной сети двигаются со скоростью, несколько меньшей скорости света ($2,9 \times 10^8$ м/с). В медных проводах они двигаются со скоростью $2,3 \times 10^8$ м/с, а в оптоволоконных — $2,0 \times 10^8$ м/с. Так что для прохода расстояния до пункта назначения бит затрачивает какое-то, пусть небольшое, время. Во-вторых, если бит проходит через какие-нибудь устройства, то транзисторы и другая электроника вносят дополнительное запаздывание. Некоторые решения вопроса запаздывания заключаются во внимательном пользовании устройствами межсетевое взаимодействия, в применении различных стратегий кодирования и в реализации подходящих протоколов на каждом уровне модели OSI.

Современные сети обычно работают на скоростях от 1 до 155 Мбит/с или больше. Вскоре они будут работать со скоростью 1 Гбит/с или 1 миллиард бит в секунду. Если в результате дисперсии биты расширяются, то тогда единицы могут приниматься за нули, нули — за единицы. Если группы битов маршрутизируются по-разному и синхронизации не уделяется должного внимания, то неустойчивость синхронизации может привести к ошибкам в принимающем компьютере, который пытается собрать пакеты в сообщение. Если группы битов задерживаются, то промежуточные сетевые устройства и компьютеры в пунктах назначения могут оказаться безнадежно забитыми миллиардом бит в секунду.

Конфликты

Конфликт имеет место в том случае, если два бита от двух различных обменивающихся данными компьютеров одновременно распространяются в коллективно используемой среде. В случае применения среды коллективного использования, напряжения двух двоичных сигналов складываются, что приводит к появлению третьего уровня напряжения. В двоичной системе такая вариация напряжения недопустима, так как они понимают только два уровня напряжений. Биты уничтожаются. На рис. Е.13 проиллюстрирована ситуация конфликта.

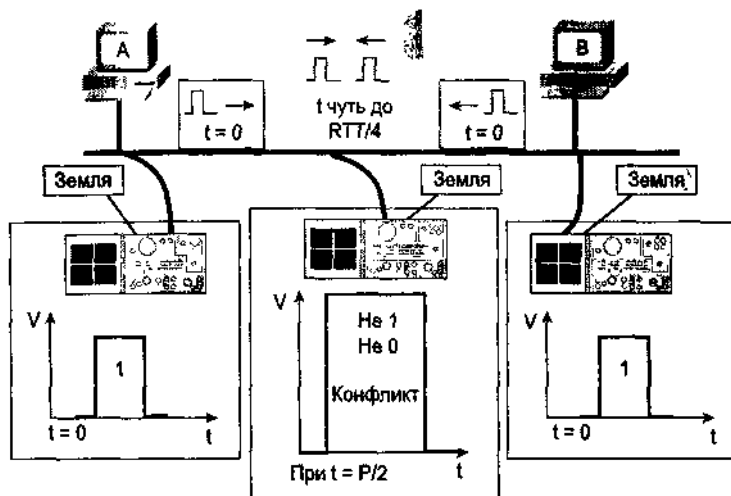


Рис. Е.13. В сетях Ethernet конфликты — обычное явление

Некоторые технологии, например Ethernet, предусматривают наличие механизма переговоров между хост-машинами, пытающимися обменяться данными, о том, чья очередь передавать в среду коллективного пользования. В некоторых случаях конфликты являются естественной частью функционирования сети. Однако чрезмерное количество конфликтов может замедлить или даже остановить работу сети. Поэтому при проектировании сетей большой кусок работы связан с минимизацией и локализацией конфликтов.

С конфликтами можно справляться многими способами. Один из способов заключается в их обнаружении и установлении набора правил их обработки в случае возникновения. Такой подход реализован в сетях Ethernet. Другой метод заключается в том, чтобы попытаться не допустить конфликты, разрешая передавать в среду коллективного пользования одновременно только одному компьютеру. Для этого вводится требование, чтобы компьютер захватывал специальную комбинацию битов, называемую меткой, которая разрешает начало передачи. Такая технология используется в сетях Token Ring и FDDI.

Сообщения в терминах битов

Теперь мы знаем, что в среде передачи данных на бит могут оказывать воздействие аттенюация, отражение, шум, дисперсия и конфликты. Конечно, в действительности передается не один бит, а значительно больше. Фактически передаются миллиарды бит в секунду. Все описанные ранее эффекты, которые могут иметь место для одного бита, косвенным образом работают и в отношении различных блоков данных протоколов в модели OSI: 8 бит эквивалентны 1 байту, несколько байт составляют один кадр (рис. Е.14), кадры содержат пакеты, а пакеты — сегменты. Сегменты несут сообщение, которое вы хотите передать. Это приводит нас к полному циклу назад по уровням модели OSI, обслуживаемым физическим уровнем: канальному, сетевому, транспортному, сеансовому, уровню представлений и уровню приложений.

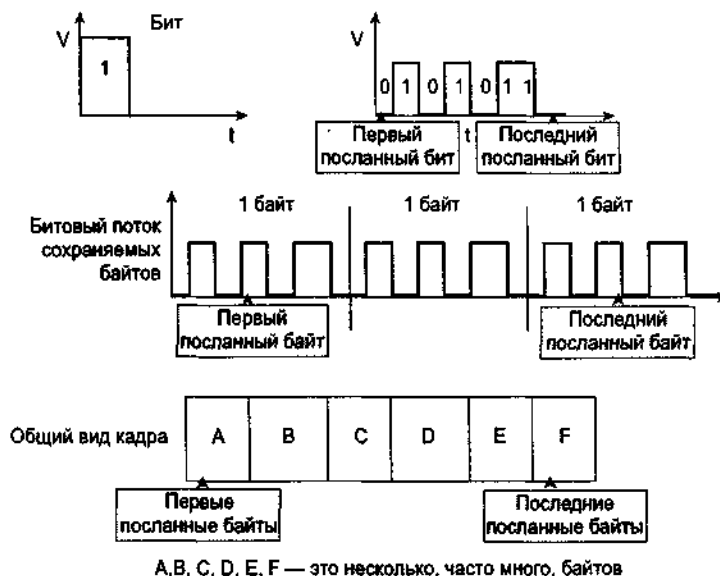


Рис. Е.14. Биты объединяются в цепочки, образуя байты, а байты связываются в кадры

Кодирование сетевых сигналов

Если вы хотите послать сообщение на большое расстояние, то необходимо решить две проблемы: как выразить сообщение (*кодирование* или *модуляция*) и какой метод использовать для его транспортировки (*несущая*).

История знает множество способов решения проблемы связи на большие расстояния: скороходы, наздники, лошади, оптические телескопы, почтовые голуби и сигнальные дымы (рис. Е.15). Каждый метод доставки требует кодирования в той или иной форме. Например, сигнальные дымы, сообщающие о том, что только что были обнаружены богатые охотничьи угодья, могут представлять собой три коротких клуба дыма, а переносимые почтовыми голубями сообщения, что кто-то благополучно добрался до места, могут иметь вид улыбающегося лица.

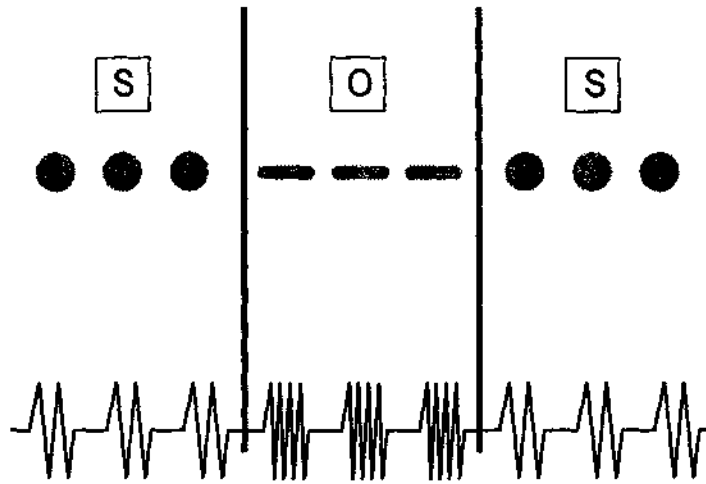
Кодирование представляет собой процесс преобразования двоичных данных в форму, которая может перемещаться по физической линии связи. *Модуляция* означает использование двоичных данных для манипулирования волной. Компьютеры используют три технологии, каждая

из которых имеет свой аналог в истории. Эти технологии включают: кодирование сообщений напряжениями в медных проводах различных форм, кодирование сообщений импульсами управляемого света в оптическом волокне и кодирование сообщений с помощью модулированных излучаемых электромагнитных волн.

Создание азбуки Морзе стало революцией в средствах связи. Всего два символа, точка и тире, позволяют закодировать весь алфавит. Например, символы ...----- означают SOS — международный сигнал бедствия. Современные телефоны, факсы, АМ, ЧМ и коротковолновые радиопередатчики, а также телевидение — все они кодируют свои сигналы электронным образом, обычно с использованием модуляции различных волн из различных участков электромагнитного спектра.

Дымовые сигналы
Телеграфный/Код Морзе
Телефон
ТВ/Радио
Почтовая служба на перекладных
Почтовый голубь

Рис. Е.15. Исторические варианты передачи сигналов с кодированием



Код Морзе был первым широким использованием напряжения для кодирования сообщений

Рис. Е.16. Исторические варианты передачи сигналов с кодированием

Кодирование и модуляция

В процессе кодирования единицы и нули преобразуются в нечто реальное и физическое, например:

- электрический импульс в проводе;
- импульс света в оптическом волокне;
- импульс электромагнитных волн в пространстве.

Для выполнения кодирования существуют два метода: *кодирование без возврата к нулю* и *манчестерское кодирование* (рис. Е.17).

Кодирование по методу без возврата к нулю является самым простым и характеризуется наличием высокого и низкого сигналов (часто это +5 В или +3,3 В — для двоичной 1 и 0 В — для двоичного 0). В оптическом волокне двоичная 1 может представляться ярким светом СИДа или лазера, а двоичный 0 — темнотой или отсутствием света. В беспроводных сетях двоичная 1 может означать наличие несущей, а двоичный 0 — ее отсутствие.

Манчестерское кодирование более сложное, но и более устойчивое к шуму и лучше держит синхронизацию. При использовании манчестерского кодирования напряжение в медном проводе, яркость СИДа или лазера в оптическом волокне или мощность электромагнитной волны содержат биты, закодированные переходами. В частности, при манчестерском кодировании переходы сигнала от низкого уровня к высокому означают двоичную 1, а переходы от высокого уровня к низкому — двоичный 0.

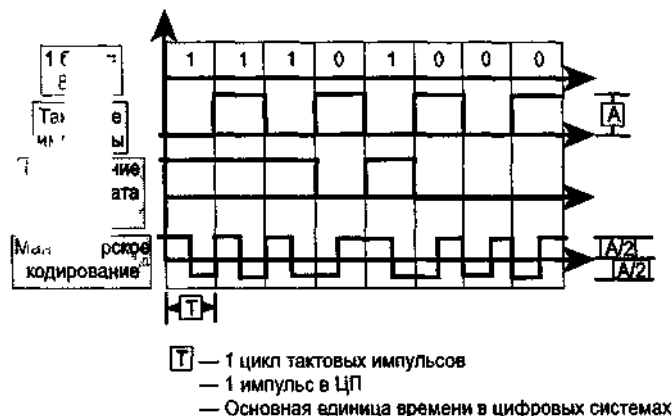


Рис. Е.17 Основными методами кодирования являются кодирование без возврата к нулю и манчестерское кодирование

Тесно связан с кодированием процесс модуляции, когда волна изменяется (модулируется) таким образом, что начинает нести информацию. Чтобы иметь представление о том, что такое модуляция, рассмотрим следующие три формы модификации или модулирования несущей с целью кодирования битов.

- *АМ (амплитудная модуляция)* — для переноса сообщения изменяется амплитуда несущей синусоидальной волны.
- *ЧМ (частотная модуляция)* — для переноса сообщения изменяется частота несущей волны.
- *ФМ (фазовая модуляция)* — для переноса сообщения изменяется фаза (начальные и конечные точки цикла) несущей волны.

Существуют и другие более сложные формы модуляции. На рис. Е.18 показаны три способа кодирования двоичных данных в несущей волне с помощью процесса модулирования. Двоичное число 11 (читается как "один, один", а не как "одиннадцать"!) может переноситься волной с использованием АМ (волна есть или волны нет), ЧМ (волна резко увеличивает количество колебаний при передаче единиц и совсем чуть-чуть при передаче нулей) или ФМ (один тип изменения фазы для нулей и другой для единиц).

Сообщения могут кодироваться разными способами.

- Уровнем напряжения в медном проводе; в сетях, основанных на медных проводниках, популярны манчестерское кодирование и без возврата к нулю.
- Управляемым светом; в оптоволоконных сетях популярны манчестерское кодирование и кодирование по методу 4В/5В
- Излучаемыми электромагнитными волнами; в беспроводных сетях используются разнообразные схемы кодирования (вариации АМ, ЧМ и ФМ).

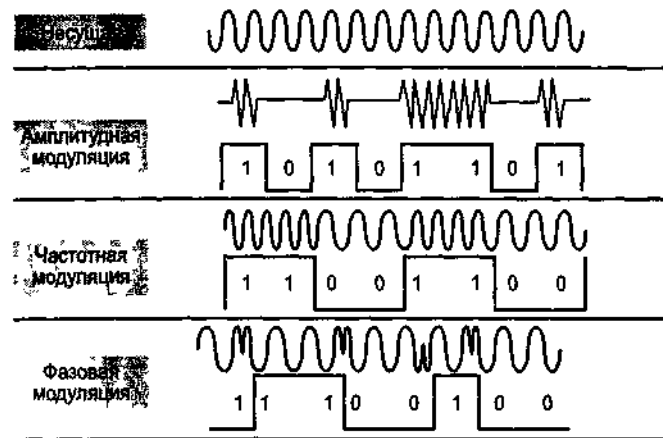


Рис. Е 18 Три способа кодирования двоичных данных в несущей волне

Резюме

- Компьютер преобразовывает двоичные числа в цифровые сигналы.
- Когда подключенный к сети компьютер принимает данные в виде цифровых сигналов, он распознает данные путем измерения и сравнения напряжения сигналов относительно определенной точки отсчета, называемой опорной землей сигналов.
- В идеале опорная земля сигналов должна быть полностью изолирована от электрического заземления. Такое изолирование не допустит попадание на опорную землю сигналов утечек цепей питания переменного тока и выбросов напряжения
- Если не принимать соответствующих мер, то шум от разводки электропитания может представлять серьезную проблему для сети.
- Существуют пять типов шумов: приконцевые перекрестные помехи, тепловой шум, шум электросети или опорной земли и электромагнитные/радиочастотные помехи.
- Проблемы синхронизации включают дисперсию, неустойчивость синхронизации и запаздывание.
- Конфликты возникают в том случае, когда два бита от двух различных компьютеров, участвующих в обмене данными, одновременно распространяются в среде коллективного пользования.
- Существуют два основных метода кодирования битов: без возврата к нулю и манчестерское.
- Существуют три основных типа модуляции несущей: амплитудная, частотная и фазовая.

Приложение Ж

Преобразование в двоичную и шестнадцатеричную систему счисления

Компьютеры представляют собой электронные устройства, состоящие из электронных переключателей. На самых нижних уровнях вычисления компьютеры зависят в принятии решения от этих переключателей. Компьютеры реагируют только на электрические импульсы, которые понимаются либо как состояние "включено", либо как "выключено", либо как 1 и 0. Поскольку компьютеры не умеют разговаривать на человеческом языке, необходимо научиться разговаривать на их языке. Этим языком является *двоичная арифметика*.

Двоичная система счисления, или *счисление с основанием 2*, полностью основана на нулях и единицах. Компьютеры используют основание 2, выражая IP-адреса. Одна из целей данного приложения — помочь в понимании процесса преобразования двоичных чисел (используемых для обозначения IP-адресов) в эквивалентные им десятичные значения.

На более высоких уровнях вычислений компьютеры иногда используют *шестнадцатеричную систему счисления*, или *счисление с основанием 16*. В системе счисления с основанием 16 используется 16 символов 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E и F. Компьютерщики используют основание 16, поскольку оно позволяет выражать байты более управляемым образом. Это объясняется тем, что число 16 является степенью 2: $16 = 2 \times 2 \times 2 \times 2$. Для представления одного 8-битового байта достаточно двух шестнадцатеричных цифр. Конечно, применение оснований 15 или 20 уже не работало бы так же хорошо, поскольку ни 15, ни 20 не являются степенью 2.

Компьютеры не "думают" в десятичной системе счисления или в системе с основанием 10, как это делают люди. Электронные устройства структурированы таким образом, что для них естественны двоичные и шестнадцатеричные числа. Чтобы использовать десятичные числа, им необходимо осуществлять перевод. Это похоже на человека, разговаривающего на двух языках, один из которых является родным языком, а другой — вторым, естественно, что быстрее и лучше он общается на родном языке.

Материал данного приложения поможет научиться думать в двоичной и шестнадцатеричной системе счисления, чтобы затем иметь возможность выполнять необходимые преобразования, решая определенные задачи, связанные с работой в сети, например проектировать схемы IP-адресации сети (двоичная) или работать с адресами памяти или MAC адресами в маршрутизаторе (шестнадцатеричные).

Как известно, для изучения новой концепции в математике необходимы время и практика. Невозможно освоить двоичные и шестнадцатеричные числа, читая о них первый раз. Поэтому, изучая двоичную и шестнадцатеричную системы счисления, следует помнить, что это процесс постепенный.

Предварительные сведения

Как узнать, какое основание имеется в виду?

Двоичная система счисления использует два символа: 0 и 1. Любое десятичное число, какое только можно себе представить, может быть выражено в двоичной системе. В десятичной системе используются символы от 0 до 9. Поскольку обе системы используют символы 0 и 1, то здесь существует потенциальная возможность запутаться. Например, что означает число 10110? Вообще-то, это зависит от того, имеется ли в виду число 10110 с основанием 10 или число 10110 с основанием 2. Из-за этой потенциальной возможной путаницы математики иногда пишут 10110_{10} , если имеют в виду число 10110 с основанием 10, и 10110_2 , если имеют в виду число 10110 с

основанием 2. Однако написание подстрочных символов каждый раз, особенно если вы пишете быстро, становится утомительным, поэтому обычно делают так, чтобы из самого контекста было понятно, какое основание имеется в виду, даже без его явной записи. Поэтому прежде всего удостоверьтесь, что при взгляде на цепочку символов, например 10110, вам ясно, какое основание имел в виду человек, писавший число 10110. Если для вас это непонятно, то тогда тот, кто писал, плохо прояснил это или вообще не имел в виду никакого конкретного основания (такую запись ученые-компьютерщики называют *цепочкой*: абстрактный список символов, выстроенный в линию).

Некоторые факты

Существует одна важная *условность* (неписаное правило), которую следует пояснить и которая почти всегда принимается без слов. После многих лет работы с десятичными числами она считается сама собой разумеющейся и заключается в том, что цепочки, подобные 10110, читаются, пишутся и произносятся слева направо. Например, 10110 читается как "один, нуль, один, один, нуль".

Если приходится сталкиваться с цепочкой типа 10110, то обычно она является каким-либо результатом, выводимым компьютером. Существуют специальные обозначения, которые используются определенными программами, например анализаторами протоколов, для обеспечения отличий между двоичными, десятичными и шестнадцатеричными числами. Например, знак % ставится перед двоичной цепочкой. Таким образом, %10110 означает число 10110 с основанием 2. Кроме того, знак 0x ставится перед шестнадцатеричной цепочкой, так что 0x10110 означает число 10110 с основанием 16.

Используя различные основания, следует держать в уме одно практическое соображение: чем больше основание, тем меньше символов, используемых для обозначения конкретного числа. Например, десятичное число 16 в системе с основанием 2 имеет вид 10000, а десятичное число 16 в системе с основанием 16 — это 10. В дополнение следует сказать, что хотя здесь основное внимание уделяется основаниям 2 и 16, в принципе нет числовых ограничений на основание, которым можно пользоваться. Хотя это и непрактично в работах, связанных с компьютерной техникой, но можно работать с основанием 23 037 или 1 002 395. Например, десятичное число 15 в шестнадцатеричной системе представляется буквой F, в системе счисления с основанием 21 десятичное число 20 представляется буквой K, а десятичное число 29 в системе счисления с основанием 30 — буквой T. Определите, каким символом будет представлено десятичное число 35 в системе счисления с основанием 36 (в предположении, что используется алфавит английского языка)?

Другой важный факт, о котором следует помнить, состоит в том, что каждая система счисления, с которой вы работаете, использует фиксированный набор символов. Например, система с основанием 2 имеет два символа, система с основанием 10—10 символов и система с основанием 16—16 символов. Заметьте, что в системе счисления с основанием 2 нет символа 2 (только 0 и 1 — понятно, что нельзя работать в двоичной системе, если в ней есть еще и символ 2!). Нет символа 3 в системе счисления с основанием 3 (только 0, 1 и 2). Нет символа 9 в системе счисления с основанием 9 (только 0, 1, 2, 3, 4, 5, 6, 7 и 8). В десятичной системе нет символа A (только 0, 1, 2, 3, 4, 5, 6, 7, 8 и 9), а шестнадцатеричной системе нет символа G (только 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E и F). Читатель уже, вероятно, понял идею. Заметим также, что количество символов, используемых в системе счисления с каким-либо основанием, равно десятичной величине основания. Вот два глупых примера: 0 — это единственный символ в системе счисления с основанием 1 (поэтому в системе с основанием 1 нельзя выразить ни одного числа, большего 0), а в системе с основанием 0 вообще нет символов.

Работаете ли вы с основанием 2, 10, 16 или каким-либо другим, числа выражаются в виде цепочки символов, например, 101011 — если используется основание 2, 14932 — если используется основание 10, и A2E7 — если используется основание 16. И это в действительности удобно. А знаете ли вы, что запись числа 124 на самом деле является сокращенной формой записи чисел? Это сокращение от $1 \times 100 + 2 \times 10 + 4 \times 1$, что было бы писать крайне утомительно. Представьте, если бы каждый раз при записи десятичного числа его надо

было записывать подобным образом! Каждое число в цепочке символов представляет значение, которое зависит от его *места* в цепочке. Например, символ 7 в десятичном числе 23761 представляет значение 7×100 или 700. Чтобы подчеркнуть важность значащего места при преобразовании оснований, можно воспользоваться таблицами с соответствующими столбцами. Среди прочего, таблицы помогают проиллюстрировать тот факт, что при чтении цепочки символов слева направо символы представляют уменьшающиеся значения места. Например, в десятичном числе 234 2 представляет 2 сотни, 3 — 3 десятка и 4 — 4 единицы. Если подвести итог, то для каждой цепочки символов существенно понимать две вещи: символы стоят в цепочке и их значение зависит от места в этой цепочке.

Принятые способы указания на величину основания

Слова *десять, одиннадцать, двенадцать, тринадцать, ..., двадцать, двадцать один* и т.д. используются только при работе с десятичными числами. Они и есть десятичные (с основанием 10) числа. Когда мы говорим "тридцать", то это всего лишь короткая форма произношения слов "три десятка". Когда же речь идет о цепочке 23 с основанием 5, то не говорят "двадцать три с основанием 5", а произносят "два три с основанием 5". Говоря "двадцать три", тем самым подразумевают "два десятка и три", т.е. если вы говорите "двадцать три", то тем самым говорите о системе счисления с основанием 10. При работе с основанием, отличающимся от десяти, названия чисел произносятся по-другому. Приведем другой пример: число 101 с основанием 2 произносится как "один нуль один с основанием 2" или просто как "один нуль один", если понятно, что речь идет о счислении с основанием 2. Никто никогда не скажет "сто двадцать один с основанием 2" или "сто двадцать один". Причина этого заключается в том, чтобы не запутать людей, называя цепочку символов в системе счисления с основанием 10, когда на самом деле она представляет число с основанием 2.

Следует отметить, что цепочка "21" в названии числа "3A2 с основанием 21" произносится как "двадцать один", и это точно означает, что 21 — число десятичное. Чтобы подчеркнуть это, иногда так и пишут: "3A2 с основанием двадцать один". Другой пример: цепочка "16" в словосочетании "основание 16" — это шестнадцать, т.е. подразумевается, что 16 является десятичным числом (в противоположность 16 с другим основанием). И в качестве последнего примера возьмем фразу "847 с основанием 20", которая произносится как "восемь четыре семь с основанием двадцать". Просто принято думать, читать, писать и произносить числа в десятичной форме, когда называется цепочка символов, стоящая после слова "основание".

Еще один момент, о котором стоит всегда помнить, — это роль символа 0. Системы счисления с любым основанием используют символ 0. *Где бы ни стоял символ 0 слева от цепочки символов, его можно отбросить, и при этом значение цепочки символов не изменится.* Например, в десятичной системе счисления 02947 эквивалентно 2947. В двоичной системе 0001001101 равно 1001101. Иногда люди ставят нули слева от числа, чтобы подчеркнуть наличие знаковых битов, которые бы в противоположном случае не были бы представлены. Поскольку состоящий из 8 битов байт иногда рассматривают в качестве единичного блока, то двоичные цепочки часто *дополняют* в длину до восьми символов. Например, при организации подсетей десятичное число 6 в двоичной форме более удобно выражать в виде 00000110. Вообще при работе с IP-адресами вполне обычно выражать двоичные числа с нулями впереди, так как, работая с IP-адресами вы работаете с *октетами* (цепочками, состоящими из восьми символов). Например, нет ничего необычного в выражении двоичного числа 10000 в виде 00010000.

Работа с показателями степени

Наконец, работая с различными системами счисления, необходимо уметь работать со *степенями* чисел, называемыми *показателями степени*. Напомним из математики, что степени чисел используются для представления повторяющегося умножения числа на самого себя. Пример, приведенный ниже, иллюстрирует, как показатели степени работают с числом 2, но это правило справедливо также и в отношении всех других чисел. Во-первых, $2^0 = 1$, что произносится как "два

в степени 0 равно единице" (2 называется *основанием*, а 0 — *показателем степени*). Этот факт не следует из предыдущих сведений, а вытекает из определения числа 2^p , где p — *целое число*. Во-вторых, $2^1 = 2$ ("два в степени один равно двум") в соответствии с математическим определением. В-третьих, $2^2 = 2 \times 2 = 4$: "два в степени два равно два умножить на два равно четырем". Продолжая, $2^3 = 2 \times 2 \times 2 = 8$: "два в степени три равно два умножить на два умножить на два равно восьми". Это дает картину, которая может быть использована для любой степени 2. Общая ошибка, когда путают взятие степени с умножением, так что следует быть внимательным: $2^4 \neq 2 \times 4 = 8$, $2^4 = 2 \times 2 \times 2 \times 2 = 16$.

Показатели степени очень удобны при работе с двоичными числами. К примеру, количество объектов, которое может быть представлено p битами, вычисляется с использованием формулы 2^p . Если для описания или именованя объекта выделяется 8 бит, то при присвоении двоичного номера этому объекту возможны $2^8 = 256$ вариантов. Этот факт важно усвоить: если есть 8 бит, то это означает, что двоичное число имеет восемь *разрядов* или *знакомест* и существует 256 различных двоичных чисел, которые могут быть выражены с помощью 8 бит, и есть 256 различных цепочек, состоящих 0 и 1, которые могут быть образованы с использованием 8 разрядов или *знакомест*.

Таким образом, мы рассмотрели множество концепций, связанных с различными основаниями, и узнали, как с ними работать. Так что теперь читатель лучше представляет себе те основы, которые необходимы, чтобы пользоваться различными системами счисления.

Двоичные числа

Теперь мы научимся использовать таблицы для представления чисел в системе счисления с конкретным основанием. Затем рассмотрим два представляющих интерес вопроса: преобразование двоичных чисел в десятичные и преобразование десятичных чисел в двоичные. После этого речь пойдет о том, как *считать* в двоичной системе, что полезно при задании *адресов подсетей*.

В системе счисления с основанием 10 работают со степенями 10. Например, 23 605 означает $2 \times 10000 + 3 \times 1000 + 6 \times 100 + 0 \times 10 + 5$. Заметим, что $10^0 = 1$, $10^1 = 10$, $10^2 = 100$, $10^3 = 1\ 000$ и $10^4 = 10\ 000$. Кроме того, даже если $0 \times 10 = 0$, этот 0 не выбрасывается, так как, если это сделать, будем иметь $2\ 365 = 2 \times 1000 + 3 \times 100 + 6 \times 10 + 5$, что совсем не то, что выражается записью 23605: 0 в данном случае выступает в роли *заполнителя разряда*. С другой стороны, если бы по какой-либо причине необходимо было обратить внимание на знакоместо сотен тысяч и знакоместо миллионов, то тогда число 23 605 выражалось бы в виде 0 023 605.

Как было продемонстрировано в предыдущих абзацах, если необходимо буквально выразить десятичное число, то используются степени числа 10 (10^0 , 10^1 , 10^2 и т.д.). Расширенная форма степеней (1, 10, 100 и т.д.) используется в тех случаях, когда необходимо обратить внимание на действительное значение десятичного числа. Для прослеживания всего этого помогает применение таблиц. Табл. Ж.1 имеет три строки: в первой строке приводятся *степени 10*, во второй строке — *расширенная* (результат умножения) *форма степеней 10*, и в третьей строке ставятся числа (от 0 до 9), требующиеся, чтобы сообщить количество необходимых степеней 10.

Таблица Ж.1

10^7	10^6	10^5	10^4	10^3	10^2	10^1	10^0
10000000	1 000 000	100000	10000	1 000	100	10	1

Например, в табл. Ж.2 показано, как выразить в таблице число 23 605 с основанием 10

Таблица Ж.2

10^4	10^3	10^2	10^1	10^0
10000	1000	100	10	1
2	3	6	0	5

Способ выражения двоичных чисел очень похож на способ выражения десятичных чисел.

Двоичные числа используют тот же принцип знакомств, который применяется при выражении десятичных чисел. Разница состоит в том, что в этом случае используются степени числа 2, а не числа 10 и для выражения числа используются только символы нуля и единицы (нет символов 2, 3, 4, 5, 6, 7, 8, 9). Таким образом, двоичная таблица (сравните с табл. Ж. 1) имеет три строки: в первой строке перечислены *степени 2*, во второй — *расширенная* (результат умножения) *форма степеней 2* и в третьей — числа (0 или 1), требующиеся для того, чтобы сообщить необходимое количество данной степени 2 (табл. Ж.3). *Заметим, что во второй строке стоят числа, записанные в десятичной системе счисления.*

Таблица Ж.3

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1

В качестве примера можно разбить двоичное число 1101, размещая цифры в таблице (табл. Ж.4). После составления таблицей можно воспользоваться для преобразования двоичного числа в его десятичный эквивалент.

Таблица Ж.4

2^3	2^2	2^1	2^0
8	4	2	1
1	1	0	1

Теперь можно воспользоваться табл. Ж.4, чтобы *преобразовать* двоичное число 1101 в десятичное:

$$1101 = 1 \times 8 + 1 \times 4 + 0 \times 2 + 1 \times 1 + 13.$$

В качестве другого примера можно рассмотреть двоичное число 10010001, поместив цифры в двоичную таблицу (табл. Ж.5). После составления таблицы воспользуемся ею и преобразуем двоичное число в десятичное.

Таблица Ж.5

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1
1	0	0	1	0	0	0	1

Теперь можно использовать табл. Ж.3, чтобы преобразовать двоичное число 10010001 в число, записанное в системе счисления с основанием 10. $10010001 = 1 \times 128 + 0 \times 64 + 0 \times 32 + 1 \times 16 + 0 \times 8 + 0 \times 4 + 0 \times 2 + 1 \times 1 = 128 + 16 + 1 = 145$

При работе с сетями число 11111111 встречается так же часто, как и любое другое (табл. Ж.6).

Таблица Ж.6

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1
1	1	1	1	1	1	1	1

Теперь преобразуем двоичное число 11111111 в десятичное: $11111111 = 1 \times 128 + 1 \times 64 + 1 \times 32 + 1 \times 16 + 1 \times 8 + 1 \times 4 + 1 \times 2 + 1 \times 1 = 255$.

Работая с сетями, в основном приходится иметь дело с двоичными числами, которые связаны с байтами или октетами, т.е. с 8-разрядными числами.

IP-адрес выражается числом в десятичной форме с разделением точками вида W.X.Y.Z, где W, X, Y и Z — десятичные числа, двоичное представление каждого из которых содержит 8 разрядов. Наименьшее десятичное значение, которое может быть представлено одним байтом (00000000 в двоичной форме), равно 0. Наибольшее десятичное значение, представляемое одним байтом (11111111 в двоичной форме), как было вычислено в табл. Ж.6, равно 255. Отсюда следует, что диапазон десятичных чисел, которые могут быть представлены байтом,

составляет от 0 до 255, т.е. всего 256 возможных значений. Поэтому в IP-адресе десятичные числа (W, X, Y и Z) могут принимать значения от 0 до 255. В качестве примеров можно привести следующие IP-адреса: 140.57.255.0, 204.65.103.243 и 5.6.7.8.

Теперь вы знаете, как преобразовывать двоичное число в десятичное. В качестве упражнения покажите с помощью таблицы, что двоичное число 11111001 равно десятичному числу 249. После решения нескольких подобных задач вы сможете разработать свой собственный способ, который, возможно, не потребует использования таблицы.

Преобразование десятичного числа в двоичное

Преобразование десятичного числа в двоичное является одной из наиболее распространенных процедур, выполняемых при работе с IP-адресами. Как и для большинства задач в математике, существует несколько способов ее решения. В данном разделе описывается один метод, но читатель волен использовать любой другой, если считает его легче.

Чтобы преобразовать десятичное число в двоичное, сначала необходимо найти наибольшую степень 2, которая не превышает это десятичное число. Рассмотрим десятичное число 35. Если обратиться к табл. Ж 3, то какая степень 2 меньше или равна 35? Что ж, 64 слишком велика, а 32 подходит как раз, так что теперь понятно, что в столбце 2^5 должна стоять 1. Что там остается? Это определяется путем вычитания 32 из 35: $35 - 32 = 3$. Затем следует просмотреть оставшиеся степени 2 в каждом столбце. Поскольку следующая меньшая степень 2 — 2^4 , то определяется, является ли степень 2^4 меньше 16 или равна 3. Так как это не так, то в столбце 2^4 ставится 0. Следующая степень 2 — 2^3 , и снова делается вывод о том, является ли степень 2^3 меньше 8 или равна 3; это не так, поэтому в столбце 2^3 тоже ставится 0. Далее, 2^2 меньше 4 или равно 3? Нет, и в столбце 2^2 ставится 0. Степень 2^1 меньше 2 или равна 3? Да, и в столбце 2^1 ставится 1. Сколько остается? Вычитаем: $3 - 2 = 1$. Наконец, ставится вопрос. 2^0 меньше 1 или равно оставшейся 1? Поскольку эта степень равна 1, то в столбце 2^0 ставится 1. Таким образом, десятичное число 35 равно двоичному числу 00100011 или 100011. Все! Табл Ж.7 сводит этот процесс воедино.

Таблица Ж.7

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1
0	0	1	0	0	0	1	1

В качестве второго примера преобразуем десятичное число 239 в двоичное. Заметим, что мы здесь придерживаемся байт-ориентированного подхода, т.е. работаем с числами от 0 до 255: десятичными числами, которые могут быть выражены одним байтом. Если посмотреть в табл. Ж.3, то какая степень 2 меньше или равна 239? Мы видим, что 128 удовлетворяет данному критерию, поэтому ставим 1 в столбец 2^7 . Сколько остается? Находим это, вычитая 128 из 239: $239 - 128 = 111$. Поскольку следующая степень 2 — это 2^6 , то определяем, является ли степень 2^6 меньше 64 или равна 111. Это так, и мы ставим 1 в столбец 2^6 . Снова определяем, сколько остается. Для этого вычитаем 64 из 111: $111 - 64 = 47$. Следующая степень — 2^5 , поэтому определяем, является ли степень 2^5 меньше 32 или равна остатку 47. Это так, поэтому ставим 1 и в столбец 2^5 . Каков остаток? Находим его, вычитая 32 из 47: $47 - 32 = 15$. Далее, является ли степень 2^4 меньше 16 или равна 15? Это не так, и в столбец 2^4 ставим 0. Далее, является ли степень 2^3 , меньше 8 или равна 15? Да, так что в столбец 2^3 ставится 1. Сколько остается? Вычитаем: $15 - 8 = 7$. Теперь определяем, является ли степень 2^2 меньше 4 или равна 7. Да, и в столбец 2^2 заносится 1. Каков остаток? Вычитаем: $7 - 4 = 3$. Определяем, является ли следующая степень 2^1 меньше 2 или равна 3. Да, это так, поэтому в столбец 2^1 тоже ставим 1. Сколько остается? Вычитаем: $3 - 2 = 1$. Наконец, находим ответ на последний вопрос: является ли степень 2^0 меньше 1 или равна остатку 1? Поскольку это так, то ставим 1 и в столбец 2^0 . Таким образом, десятичное число 239 равно двоичному числу 11101111 Табл Ж.8 подводит итог

Таблица Ж.8

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1
1	1	1	0	1	1	1	1

Эта процедура работает в отношении любого десятичного числа. Рассмотрим десятичное число 1 000 000 (один миллион). Какова наибольшая степень 2, которая меньше или равна 1 000 000? Если запастись терпением, то можно вычислить, что $2^9 = 512$ и $2^{10} = 1024$, так что 2^9 является наибольшей степенью 2, которая вмещается в 1 000 000. Если продолжить описанную ранее процедуру, то можно определить, что десятичное число один миллион равно двоичному числу 11110100001001000000.

Как видно, двоичные числа занимают значительно больше места, чем десятичные. Частично именно из-за этого люди не используют двоичную систему счисления. Но, вероятно, основная причина, почему люди пользуются основанием 10, заключается в том, что у нас 10 пальцев. Если бы у нас их было 12, мы, наверное, использовали бы основание 12.

Счет в двоичной системе

Сеть может делиться на *подсети* путем "заимствования битов" из крайней левой части поля хост-машин сетевого IP-адреса. Заимствованные биты позволяют дифференцировать подсети двоичными цепочками, которые и определяют их. Например, если позаимствовать 2 бита из четвертого октета сети класса C 200.10.20.0, то можно сформировать четыре подсети. Из 2 битов можно получить четыре двоичные комбинации: 00, 01, 10 и 11. Первая и последняя подсети обычно отбрасываются (те, что связаны со всеми нулями и единицами в адресе). Заметим, что последовательность комбинаций 00, 01, 10 и 11 представляет собой счет от 0 до 3 в двоичной системе.

Поэтому, определяя адреса подсетей для данной IP-сети, полезно уметь считать в двоичной системе. Счет в двоичной системе счисления позволяет получать в явном виде двоичные представления подсетевых IP-адресов, получаемых при заимствовании битов.

С помощью 4 битов можно получить $2^4 = 16$ возможных комбинаций нулей и единиц. Просто для сведения ниже показаны первые 16 двоичных чисел в порядке возрастания (счет от 0 до 15 в двоичном представлении):

0, 1, 10, 11, 100, 101, 1001, 1011, 1000, 1001, 1010, 1011, 1100, 1101, 1110, 1111

Четные и нечетные числа

Иногда полезно представлять себе, как понятия *четного* и *нечетного* числа транслируются на двоичные числа. Четным десятичным числом называется число, кратное 2 (например, 0, 2, 4, 6, 8, 10, 12 и т.д.). Заметим, что во второй строке табл. Ж.9 все числа кратны 2, за исключением одного справа: 1.

Таблица Ж.9

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1

Если подумать, то это означает, что *двоичное число кратно 2 тогда и только тогда, когда крайняя правая цифра является нулем*. Поэтому **двоичное число является четным тогда и только тогда, когда его крайняя правая цифра — 0**. Нечетным называется такое число, которое не является четным (например, 1, 3, 5, 7, 9, 11 и т.д.). Отсюда, **двоичное число нечетно тогда и только тогда, когда его крайняя правая цифра — 1**.

Несколько примеров: двоичное число 10011 — нечетно (десятичное 19), а двоичное число 1010100010 — четно (десятичное 674).

Шестнадцатеричные числа

В системе счисления с основанием 16, или в шестнадцатеричной системе, работают со степенями числа шестнадцать. Шестнадцатеричное представление используется в системах адресации канального уровня (например, MAC-адреса) и при указании адресов в памяти электронных устройств. Символы шестнадцатеричной системы: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E и F. Символ A соответствует десятичному числу 10, B — 11, C — 12, D — 13, E — 14 и F — 15. Примерами шестнадцатеричных чисел являются, скажем, числа 2A384C5D9E7F, A001 и 237. Опять же, следует быть внимательным, чтобы из контекста было понятно, о каком основании идет речь. В противном случае в предыдущих примерах число 237 может быть по ошибке принято за десятичное.

Для шестнадцатеричных чисел существуют два типа специальных обозначений. Иногда встречаются обозначения вида 0x1A3B или 1A3Bh. Означают они одно и то же, а именно¹ число 1A3B в шестнадцатеричном представлении. Повторяя, скажем, что если встречается цепочка, впереди которой стоят символы "0x" или за ней стоит символ "h", то она интерпретируется как шестнадцатеричное число. В частности, подобные обозначения встречаются, когда приходится работать с регистрами памяти.

Важно также помнить тот факт, что одним шестнадцатеричным символом можно представить любое десятичное число от 0 до 15. В двоичном представлении 15 соответствует 1111, а 10 — 1010. Отсюда следует, что для представления одного шестнадцатеричного символа в двоичной системе счисления требуется четыре бита. MAC-адрес имеет длину 48 бит (6 байтов), что транслируется в $48 : 4 = 12$ шестнадцатеричных символов, требующихся для его выражения. Это можно проверить, введя в командной строке ОС Windows 95/98 команду winipcfg или ipconfig /all, если используется ОС Windows NT4/2000.

Табл. Ж. 10 представляет собой шестнадцатеричную таблицу (сравните с табл. Ж.1) с тремя строками. В первой строке приведены *степени 16*, во второй — *расширенные* (результат умножения) *степени 16* и в третьей — числа (от 0 до F), которые необходимы, чтобы сообщить о нужном количестве конкретной степени 16. Заметим, что вторая строка содержит числа, написанные в системе счисления с основанием 10! В данной таблице только четыре столбца, поскольку значения степеней 16 становятся очень большими с увеличением показателя степени; кроме того, общепринято ставить шестнадцатеричные символы в группы по два или по четыре.

Таблица Ж.10

16^3	16^2	16^1	16^0
4096	256	16	1

Рассмотрим шестнадцатеричное число 3A. Десятичное значение числа 3A можно определить с помощью шестнадцатеричной таблицы (табл. Ж.11).

Таблица Ж.11

16^1	16^0
16	1
3	A

Воспользовавшись табл. Ж.11, преобразуем шестнадцатеричное число 3A в число с основанием 10:

$$3A = 3 \times 16 + A \times 1 = 3 \times 16 + 10 \times 1 = 48 + 10 = 58.$$

Теперь рассмотрим шестнадцатеричное число 23CF. Табл. Ж. 12 помогает посмотреть на процесс преобразования в перспективе.

Таблица Ж.12

16^3	16^2	16^1	16^0
4096	256	16	1

2	3	C	F
---	---	---	---

Воспользовавшись табл. Ж. 12, преобразуем шестнадцатеричное число 23CF в число с основанием 10:

$$23CF = 2 \times 4096 + 3 \times 256 + C \times 16 + F \times 1 = 2 \times 4096 + 3 \times 256 + 12 \times 16 + 15 \times 1 = 8192 + 768 + 192 + 15 = 9167.$$

Наименьшее десятичное значение, которое может быть представлено четырьмя шестнадцатеричными символами, 0000, равно 0. Наибольшее десятичное значение, представляемое четырьмя шестнадцатеричными числами, FFFF, равно 65 535. Отсюда следует, что диапазон десятичных чисел, представляемых четырьмя шестнадцатеричными символами, составляет от 0 до 65 535 или всего 65 536, или 2^{16} возможных значений.

Итак, мы познакомились с преобразованием шестнадцатеричного числа в десятичное. В качестве упражнения покажите с использованием таблицы, что шестнадцатеричное число 8D2B3 преобразуется в десятичное число 578 227. Как и в случае с преобразованием двоичных чисел в десятичные, после нескольких повторений этой процедуры читатель, вероятно, сам разработает свой собственный короткий способ, который может и не предусматривать использование таблицы.

Преобразование десятичного числа в шестнадцатеричное

Опять же, существует несколько способов решения этой задачи, так что читатель может придраться к своему излюбленному. Приводимое ниже описание демонстрирует один из методов выполнения такого преобразования. Если читатель уже освоил какой-либо другой конкретный метод, то остальную часть данного раздела можно пропустить.

При преобразовании десятичного числа в шестнадцатеричное идея состоит в том, чтобы сначала найти наибольшую степень 16, которая бы была меньше или равна десятичному числу, а затем определить, сколько раз она помещается в этом десятичном числе. Поскольку подобный процесс уже рассматривался при выполнении преобразования десятичного числа в двоичное, то можно сразу к нему и перейти. Следует отметить только одно отличие, которое заключается в том, что иногда наибольшая степень 16 может уместиться в десятичном числе несколько раз.

Рассмотрим десятичное число 15 211. Если посмотреть в табл. Ж. 10, то какая наибольшая степень 16 меньше или равна 15 211? Как видим, этому критерию удовлетворяет 4096. Сколько раз она помещается в числе 15 211? Находим, что она помещается не более 3 раз ($4096 \times 3 = 12\,288$), и поэтому в столбце 4096 (или 16^3) будет стоять 3. Сколько остается? Находим это путем вычитания: $15\,211 - 12\,288 = 2923$. Теперь мы видим, что 256 помещается в 2923 одиннадцать (и не больше) раз ($256 \times 11 = 2816$), таким образом в столбце 256 (или 16^2) будет стоять В (не 11!). Вычитая, получаем: $2923 - 2816 = 107$. Поскольку 16 помещается в 107 шесть (и не больше) раз ($16 \times 6 = 96$), то в столбце 16 (или 16^1) стоит 6. Вычитая, получаем: $107 - 96 = 11$, так что последней цифрой будет В. Шестнадцатеричное значение десятичного числа 15 211 равно 3В6В. Весь этот процесс сведен в табл. Ж. 13.

Таблица Ж.13

16^3	16^2	16^1	16^0
4096	256	16	1
3	В	6	В

Преобразование шестнадцатеричного числа в двоичное

Преобразование шестнадцатеричных чисел в двоичные выполняется относительно просто.

Это можно делать по одному шестнадцатеричному символу за раз. Заметим, что этот метод не является общим подходом при преобразовании различных оснований; он работает только благодаря тому, что 16 является степенью 2: $16 = 2^4$.

В качестве примера возьмем шестнадцатеричное число A3, которое равно двоичному числу 10100011, поскольку A преобразуется в 1010, а 3 — в 0011. Чтобы этот метод работал, будьте особенно внимательны и включайте четыре двоичные цифры для каждого шестнадцатеричного символа. (Если забыть об этом, то, скажем, в последнем примере результат будет 101011, что, как можно проверить, неправильно.) Шестнадцатеричное число FOFO преобразуется в двоичное число 1111000011110000, так как F преобразуется в двоичное 1111, а 0 — в 0000. Наконец, широковещательный MAC-адрес FF-FF-FF-FF-FF-FF преобразуется в двоичный эквивалент вида 1111Ш1-1111Ш1-1Ш1Ш-11Ш11-Ш11Ш-11111111-11111111-11111111. Как видно, шестнадцатеричные представления занимают значительно меньше места, чем их двоичные аналоги.

На этом обсуждение двоичных и шестнадцатеричных чисел завершается. Следует помнить, что для привыкания к этим концепциям требуется некоторое время, но вам это наверняка удастся. Придерживайтесь их, и с приобретением достаточной практики со временем вы сможете объяснять их другим!

Практические упражнения

1. Преобразуйте двоичное число 1010 в число с основанием 10.
2. Преобразуйте число с основанием 2 11110000 в десятичное.
3. Преобразуйте двоичное число 10101111 в десятичное.
4. Преобразуйте десятичное число 1111 в двоичное.
5. Преобразуйте десятичное число 249 в число с основанием 2.
6. Преобразуйте десятичное число 128 в число с основанием 2.
7. Преобразуйте десятичное число 65 в двоичное.
8. Преобразуйте число 63 с основанием 10 в двоичное.
9. Преобразуйте число 31 с основанием 10 в двоичное.
10. Преобразуйте десятичное число 198 в двоичное.
11. Двоичное число 11100011 четное или нечетное?
12. Преобразуйте OхAB в число с основанием 10.
13. Преобразуйте ABCDh в число с основанием 10.
14. Преобразуйте OхFF в десятичное число.
15. Преобразуйте десятичное число 249 в число с основанием 16.
16. Преобразуйте десятичное число 65 000 в шестнадцатеричное.
17. Преобразуйте число Oх2B в число с основанием 2.
18. Преобразуйте число Oх1OFS в число с основанием 2.
19. Переведите MAC-адрес 00-AO-CC-3C-4A-39 в двоичную систему счисления.
20. Переведите IP-адрес 166.122.23.130 и маску подсети 255.255.255.128 в шестнадцатеричное представление с разделением точками.

Приложение 3

Поиск и устранение неисправностей в сетях

Выполняя лабораторные работы по теме "Маршрутизатор", вы сможете еще лучше освоить процесс поиска и устранения неисправностей. В данном приложении поиск и устранение неисправностей будут рассмотрены более подробно. Этот процесс в некоторой степени индивидуален. Однако некоторые принципы являются общими для любой методологии поиска и устранения неисправностей. Чтобы увязать описание процесса поиска и устранения неисправностей с лабораторными работами по теме "Маршрутизатор", которые выполняются во втором семестре, на последующих страницах используется язык модели OSI. В конце будет представлен общий подход к решению возникающих в сетях проблем.

Лабораторные работы по устранению неисправностей, которые выполняются во втором семестре обучения

Выполняя конфигурирование маршрутизатора в ходе лабораторных работ (рис. 3.1-3.4) второго семестра обучения на курсах сертифицированных специалистов компании Cisco, студенты получают достаточно большую практику и в вопросах поиска и устранения неисправностей. Они учатся работать, начиная с уровня 1 модели OSI, идя вверх от физического уровня к каналному, затем к сетевому и т.д. Ниже приведен обзор некоторых наиболее часто встречающихся проблем, относящихся к уровням 1—3.

На уровне 1 могут возникать такие проблемы:

- обрыв кабеля;
- неподсоединение кабеля;
- подключение кабеля не к тому порту, что нужно;
- нестабильный контакт в месте подсоединения кабеля;
- неправильная заделка кабеля в разъем.
- применение для поставленной задачи не тех типов кабелей (кроссовые, шлейфовые и соединительные кабели следует использовать в соответствии с их назначением);
- проблемы с трансивером;
- проблемы с кабелем подключения DCE-устройства;
- проблемы с кабелем подключения DTE-устройства;
- отсутствие питания на устройстве.

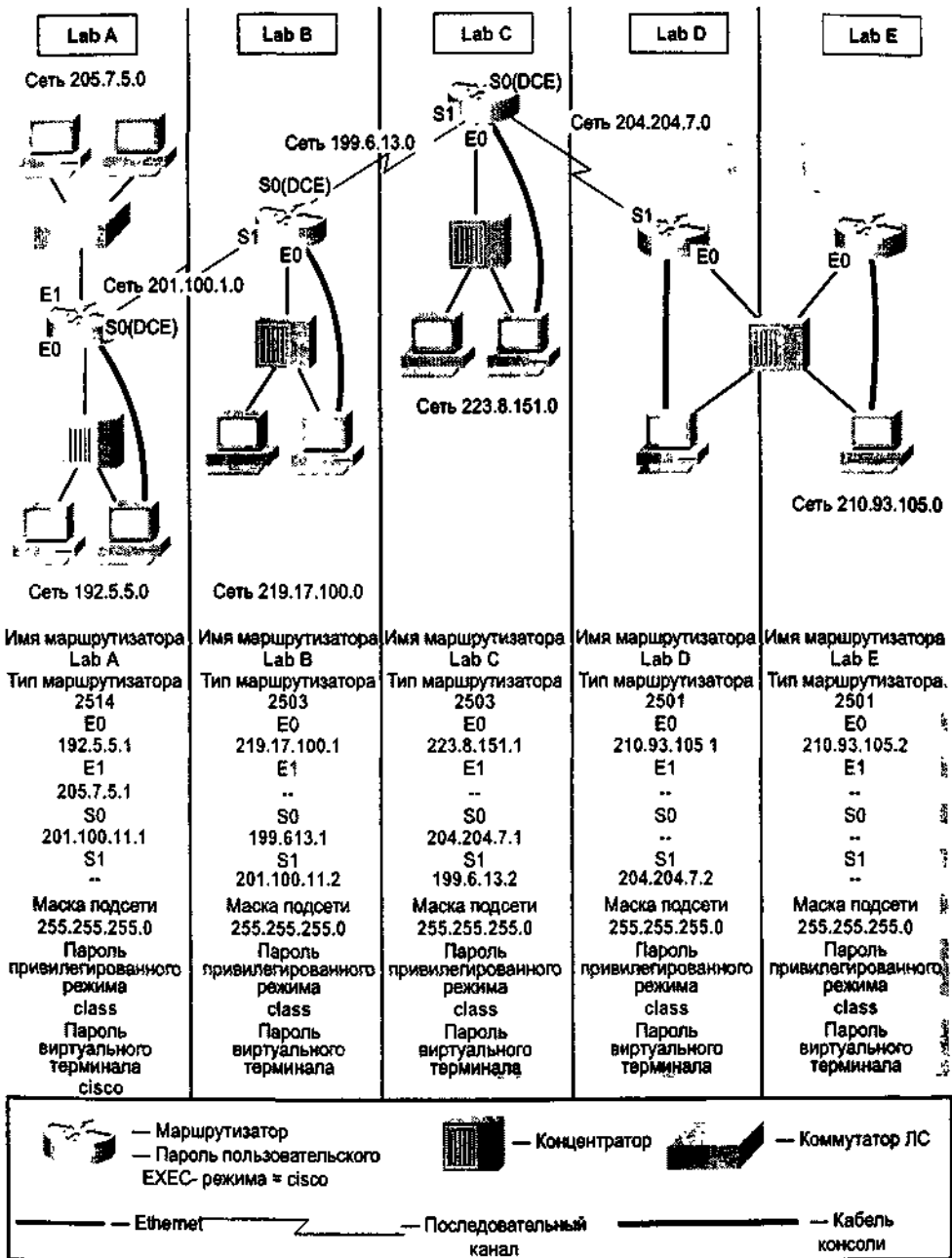


Рис. 3.1. Типовые лабораторные работы второго семестра и обычно используемые в них исходные данные

Устранение неисправностей — уровень 2

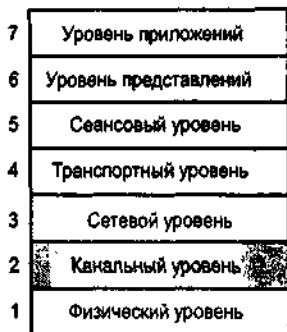


Рис. 3.3. Уровень 2 — следующий уровень модели OSI, на котором ищут неисправности

Устранение неисправностей — уровень 1

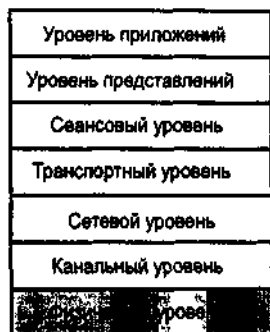


Рис. 3.2. Поиск и устранение неисправностей всегда следует начинать с уровня 1

Устранение неисправностей — уровень 3

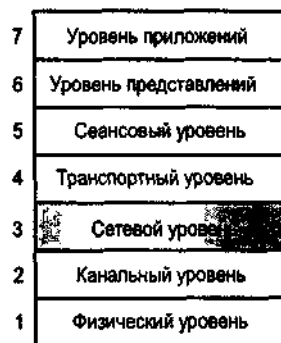


Рис. 3.4. Как правило, поиск и устранение неисправностей завершаются на уровне 3 модели OSI

На уровне 2 могут встречаться следующие ошибки:

- неправильное конфигурирование последовательных интерфейсов;
- неправильное конфигурирование интерфейсов Ethernet;
- неправильная установка значения тактовой частоты на последовательных интерфейсах;
- неправильное задание метода инкапсуляции на последовательных интерфейсах (по умолчанию используется инкапсуляция по протоколу HDLC);
- неработающая плата сетевого интерфейса.
- Ошибки на уровне 3 могут включать:
- невыполнение активизирования работы протокола маршрутизации;
- активизирование не того протокола маршрутизации;
- некорректный IP-адрес сети;
- задание неправильной маски подсети;
- задание неправильного адреса интерфейса;
- неправильное задание привязки DNS и IP-адресов (записи в таблице хост-машин);
- задание неправильного номера автономной системы для протокола IGRP.

Важно знать приемы устранения неисправностей на уровнях 1—3, которые приведены выше. Однако это еще далеко не все, так как необходимо знать, где искать помощь, если не удастся сразу определить причину, почему сеть работает не так, как должна. На рис. 3.5 приведен перечень некоторых ресурсов для устранения неисправностей. Одним из часто используемых профессиональными разработчиками сетей ресурсов является Web-сервер документации службы интерактивного взаимодействия с клиентами компании Cisco (Cisco Connection Online — CCO) (www.cisco.com).

Ресурсы для устранения неисправностей






 <p>Члены команды</p>	<p>Журналы</p> 
 <p>Эксперты</p>	<p>Система помощи ОС IOS</p> 
<p>Все ОК?</p> <p>Да <input type="checkbox"/> Нет <input type="checkbox"/></p> <p>Стратегии действий</p>	<p>Web-ресурсы</p> 
<p>Инструментальные средства</p> <ul style="list-style-type: none"> - Аппаратные (кабельный т... - Программные средства компьютерных прот... (CD) 	<p>Команды ОС IOS</p> <ul style="list-style-type: none"> - Ping - Telnet - Trac Route - Debug

Рис 3.5. Перечень ресурсов для выполнения поиска и устранения неисправностей на случай, если обычные методики не срабатывают

Общая модель поиска и устранения неисправностей

Полезно иметь общую методику, к которой можно прибегать при решении задачи поиска и устранения неисправностей в компьютерных сетях. В настоящем разделе кратко описан один такой метод, который используется многими профессиональными разработчиками сетей.

В соответствии с этим методом поиск и устранение неисправностей выполняются пошагово

1. **Определение проблемы.** Каковы симптомы и потенциальные причины?
2. **Сбор фактов.** Изолирование возможных причин.
3. **Рассмотрение возможностей.** На основе собранных фактов основное внимание концентрируется на тех узких областях, которые имеют отношение к данной конкретной проблеме. На этом этапе устанавливаются границы проблемы.
4. **Составление плана действий.** Разрабатывается план, который предусматривает одновременное изменение только одной переменной.
5. **Воплощение плана действий.** Тщательно выполняется каждый шаг действий и одновременно проверяется, исчезли симптомы или нет.
6. **Наблюдение за результатами.** Определяется, решена проблема или нет. Если проблема решена, то процесс на этом завершается.
7. **Повторение процесса.** Если проблема не решена, необходимо перейти к следующей наиболее вероятной причине из составленного списка. В этом случае осуществляется возврат к шагу 4, и процесс повторяется до тех пор, пока проблема не будет решена.

Практическое применение модели поиска и устранения неисправностей

Ниже приведен пример применения модели поиска и устранения неисправностей при выполнении типовых лабораторных работ по теме "Маршрутизатор".

При попытке пропинговать маршрутизатор Lab-E из маршрутизатора Lab-A принимается ряд сообщений о превышении предела ожидания эхо-ответа по времени.

```
lab-a#ping lab-e
Type escape sequence to abort.
Sending 5,100-byte ICMP Echos to 210.93.105.2, timeout is 2 seconds:
. . . . .
Success rate is 0 percent (0/5)
```

Начинаем с шага 1 модели поиска и устранения неисправностей.

1. Определение проблемы. Каковы симптомы и потенциальные причины? Составляем список симптомов: - Невозможность пропинговать маршрутизатор Lab-E из маршрутизатора Lab-A.

Затем составляем список возможных причин, группируя их в соответствии с уровнями модели OSI:

а) Уровень 1

- Плохой кабель.
- Кабель не подсоединен.
- Потеря питания на концентраторе.

б) Уровень 2

- Интерфейс отключен.
- Неправильная установка метода инкапсуляции (на последовательных интерфейсах по умолчанию используется протокол HDLC).
- Неправильная установка значения тактовой частоты на последовательных интерфейсах.

в) Уровень 3

- Неправильный адрес интерфейса.
- Неправильная маска подсети.
- Неправильная маршрутная информация.

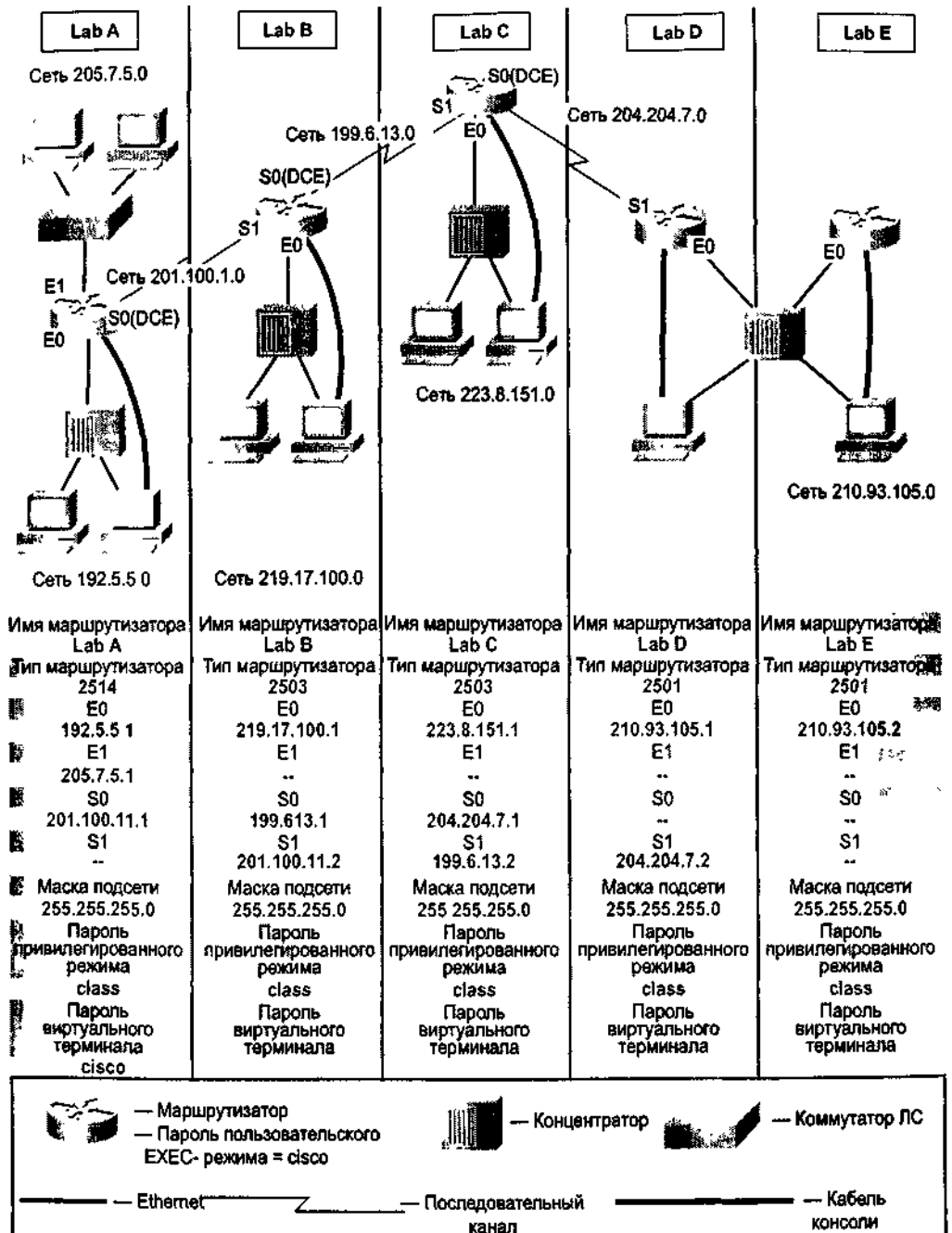


Рис. 3 6. Уже знакомая диаграмма лабораторных работ второго семестра

2. Сбор фактов. Изолирование возможных причин.

Для изоляции проблемы следует воспользоваться командами маршрутизатора show. Начинать следует с проверки всей сети. Поскольку эта сеть находится под единым управлением, то таблица маршрутизации каждого маршрутизатора содержит информацию обо всех сетях, входящих в данную глобальную сеть.

В командной строке привилегированного режима EXEC на маршрутизаторе Lab-A вводится команда show ip route, благодаря чему выводится содержимое таблицы маршрутизации маршрутизатора Lab-A. Должны быть выведены данные обо всех восьми сетях. Согласно приведенному ниже результату в таблице маршрутизации присутствуют только семь из восьми сетей.

```
lab-a#show ip route
Codes:C -connected,S -static,! -IGRP,R -RIP,M -mobile,B -BGP
D -EIGRP,EX -EIGRP external,0 -OSPF,IA -OSPF inter area
N1 -OSPF NSSA external type 1,N2 -OSPF NSSA external type 2
E1 -OSPF external type 1,E2 -OSPF external type 2,E -EGP
i -IS-IS,L1 -IS-IS level-1,L2 -IS-IS level-2,*-candidate default
U -per-user static route,o -ODR
Gateway of last resort is not set
C 205.7.5.0/24 is directly connected,Ethernet1
R 219.17.100.0/24 [120/1] via 201.100.11.2, 00:00:24, Serial0
R 199.6.13.0/24 [120/1] via 201.100.11.2, 00:00:24, Serial0
R 204.204.7.0/24 [120/2] via 201.100.11.2, 00:00:24, Serial0
C 192.5.5.0/24 is directly connected, Ethernet0
R 223.8.151.0/24 [120/2] via 201.100.11.2, 00:00:24, Serial0
C 201.100.11.0/24 is directly connected, Serial0
```

3. Рассмотрение возможностей. На основе собранных фактов основное внимание концентрируется на тех узких областях, которые имеют отношение к данной конкретной проблеме. На этом этапе устанавливаются границы проблемы. Чтобы сделать это, необходимо упростить область поиска, что достигается за счет перехода от общей картины к более сфокусированному и детальному рассмотрению вопроса о возможном местонахождении проблемы.

Информация, приведенная в таблице маршрутизации, свидетельствует о том, что сеть 204.204.7.0 находится на расстоянии двух переходов, что показано записью [120/2] В строке R 204.204.7.0/24 [120/2] via 201.100.11.2, 00:00:24, Serial0. В двух переходах от маршрутизатора Lab-A находится маршрутизатор Lab-C, который является последним предоставляющим в коллективное пользование свою информацию протокола RIP. Поиск и устранение неисправностей следует начинать с последнего маршрутизатора, от которого принимается информация. Теперь надо собрать данные на более низком уровне. Сосредоточимся на одном маршрутизаторе. Устанавливаем Telnet-сеанс с маршрутизатором Lab-C и вводим на нем команду show run, чтобы посмотреть его текущую исполняемую конфигурацию. Обязательно запротоколируйте конфигурационный файл (для этого можно записать его в свой журнал или скопировать и вставить в Notepad-файл).

```
lab-a#lab-c
Trying lab-c (199.6.13.2)...Open

User Access Verification

Password:
lab-c>ena
Password: 1
ab-clshow run

Building configuration...

interface Ethernet0
ip address 223.8.151.1
255.255.255.0
!
interface Serial0
ip address 204.204.7.1
255.255.255.0
no ip mroute-cache
clockrate 56000
!
interface Serial1
ip address
199.6.13.2.255.255.0
!
```

```

interface BRIO                               shutdown
no ip address                                !
Current configuration:                        router rip
!                                             network 199.6.13.0
version 11.3                                 network 204.204.7.0
service timestamps debug uptime             network 223.8.151.0
service timestamps log uptime               !
no service password-encryption              ip host lab-a
!                                             192.5.5.1 205.7.5.1
hostname lab-c                               ip host lab-b
enable password class <more>                 201.100.11.2.219.17.
                                              100.1
                                              <more>

```

Теперь получим информацию об интерфейсе, подключенном к последней выводимой командой `show ip route` сети. Введем в командной строке команду `show int s0`, что позволит получить всю текущую информацию об этом интерфейсе. Запротоколируем ее.

```

lab-c#sho int s0
Serial0 is up,line protocol is up
Hardware is HD64570
Internet address is 204 . 204.. 7 .1/24
MTU 1500 bytes,BW 1544 Kbit,DLY 20000 usec,,
reliability 255/255,txload 1/255,rxload 1/255
Encapsulation HDLC,loopback not set,keepalive set (10 sec)
Last input 00:00:01,output 00:00:00,output hang never
Last clearing of "show interface"counters never
Input queue:0/75/0 (size/max/drops);Total output drops:0
Queueing strategy:weighted fair
Output queue:0/1000/64/0 (size/max total/threshold/drops)
Conversations 0/1/256 (active/max active/max total)
Reserved Conversations 0/0 (allocated/max allocated)
 5 minute input rate 0 bits/sec,0 packets/sec
 5 minute output rate 0 bits/sec,0 packets/sec
185 packets input,12570 bytes,0 no buffer
Received 185 broadcasts,0 runts,0 giants,0 throttles
0 input errors,0 CRC,0 frame,0 overrun,0 ignored,0 abort
241 packets output,20487 bytes,0 underruns
0 output errors,0 collisions,21 interface resets
0 output buffer failures,0 output buffers swapped out
10 carrier transitions
DCD=up DSR=up DTR=up RTS=up CTS=Up

```

4. Составление плана действий. Разрабатывается план, который предусматривает одновременное изменение только одной переменной.

Из информации о текущей конфигурации маршрутизатора Lab-C видно, что все сконфигурировано правильно. Если далее посмотреть на результат исполнения команды `show int s0`, то видно, что интерфейс и канальный протокол находятся в рабочем состоянии. Следовательно, на другом конце кабель подсоединен к устройству и канальный уровень функционален. Если бы кабель не был подсоединен соответствующим образом, то канальный протокол был бы неработоспособен. Благодаря этим двум командам `show` понятно, что маршрутизатор сконфигурирован правильно и функционирует. Значит, проблема, вероятнее всего, заключается в следующем маршрутизаторе: Lab-D. Здесь мы имеем пример процесса исключения или упрощения проблемы. Хорошим планом действий была бы попытка установления Telnet-сеанса с маршрутизатором Lab-D с последующим переходом в режим работы с терминалом для проверки на наличие ошибок в текущей конфигурации. Если ошибок найдено не будет, то, возможно, придется проверить интерфейс S1.

5. Воплощение плана действий. Тщательно выполняется каждый шаг действий и одновременно проверяется, исчезли симптомы или нет.

Предположим, что попытка установления Telnet-сеанса с маршрутизатором Lab-D оказалась

безуспешной. В этом случае необходимо перейти на терминал, непосредственно подключенный к маршрутизатору Lab-D. Входим в привилегированный режим EXEC и вводим команду show run. В выведенном результате замечаем, что на маршрутизаторе Lab-D в качестве протокола маршрутизации активизирован не протокол RIP (который используется маршрутизатором Lab-C), а протокол IGRP. Чтобы исправить эту ошибку, необходимо войти в режим глобального конфигурирования и ввести команды по router igrp 111 и router rip. Затем следует ввести команды network: network 210.93.105.0 и network 204.204.7.0 (это сети, которые непосредственно подключены к маршрутизатору Lab-D). После этого надо нажать клавиши <Ctrl+Z> и вывести команду copy run start.

6. Наблюдение результатов. Определяется, решена проблема или нет. Если проблема решена, то процесс на этом завершается.

Теперь путем пингования маршрутизаторов Lab-A и Lab-E проверяется возможность осуществления связи.

```
lab-d#ping lab-a
Type escape sequence to abort.
Sending 5,100-byte ICMP Echos to 192.5.5.1,timeout is 2 seconds:
!!!!
Success rates is 100 percent (5/5) , round-trip rtun/avg/max =96/100/108
ms lab-d#ping lab-e Type escape sequence to abort.
Sending 5,100-byte ICMP Echos to 210.93.105.2,timeout is 2 seconds :
!!!!
Success rate is 100 percent (5/5),round-trip min/avg/max =1/3/4 ms
```

7. Повторение процесса. Если проблема не была решена, то осуществляется переход к следующей наиболее вероятной причине из составленного списка. В этом случае осуществляется возврат к шагу 4, и процесс повторяется до тех пор, пока проблема не будет решена.

Хотя в нашем примере и была выявлена и исправлена ошибка в конфигурационном файле маршрутизатора, может случиться так, что это не восстановит связь. Некоторые проблемы имеют составной или многопричинный характер. Если проведенные действия не устранили проблему, то осуществляется возврат к шагу 4 и выполняется разработка нового плана действий. Поскольку большинство проблем в сетях вызывается ошибками пользователей, разработанный план действий тоже может содержать ошибки. Наиболее типичными ошибками в плане действий являются пропуски или просмотры очевидных причин. Процесс поиска и устранения неисправностей может приносить массу разочарования. Помните: не надо паниковать. Если вам необходима помощь со стороны, не бойтесь ее попросить.

Чтобы наглядно представить все изложенное выше, на рис. 3.7 показана блок-схема модели процесса поиска и устранения неисправностей.



Проблема решена: Прекращение процесса

Рис. 3.7. Каждый человек разрабатывает свои собственные методы поиска и устранения неисправностей. Однако полезно иметь общую методiku, к которой можно обратиться, если все другое не помогает

С помощью изложенного выше руководства можно решить большинство проблем, связанных с неисправностями в сетях. Для профессиональных специалистов по сетям задача поиска и устранения неисправностей играет важную роль в повседневной работе, так что наличие богатого практического опыта критично для совершенствования навыков в решении задач поиска и устранения неисправностей. Для многих устранение неисправностей является наиболее приятной и благодарной частью работ с сетями. При небольших затратах времени и терпении этот процесс станет вашей второй натурой.

Словарь терминов

В данном словаре собраны термины и аббревиатуры, используемые в теории и практике создания сетей передачи данных. Как и в любой другой развивающейся технической области, некоторые термины эволюционируют и имеют несколько значений, поэтому в тех случаях, когда это необходимо, здесь приводятся несколько определений и расшифровок аббревиатур. Термины, состоящие из нескольких слов, приводятся в алфавитном порядке так, словно пробелы между словами отсутствуют, а термины с дефисами — так, как если бы дефиса не было.

Определения терминов обычно приводятся после их аббревиатур. Расшифровки аббревиатур приводятся отдельно с перекрестной ссылкой на аббревиатуру. Дополнительно многие определения содержат ссылки на связанные термины.

Авторы надеются, что этот словарь терминов поможет читателю лучше разобраться в технологиях межсетевых взаимодействий.

Числовые аббревиатуры

100BaseFX — спецификация монополосной сети **Fast Ethernet** со скоростью передачи данных 100 Мбит/с с использованием для каждой линии связи двухжильного многомодового

оптоволоконного кабеля Чтобы гарантировать нужную синхронизацию сигналов, линия связи сети **100BaseFX** не должна превышать длину более 400 метров См также *100BaseFX; Fast Ethernet, IEEE 802.3*

100BaseT — спецификация монополосной сети Fast Ethernet со скоростью передачи данных 100 Мбит/с с использованием разводки на основе кабелей типа UTP (неэкранированная витая пара) Как и технология **10BaseT**, на которой она основана, технология **100BaseT** регламентирует посылку канальных импульсов по сегменту сети в момент отсутствия трафика Однако эти импульсы содержат больше информации, чем те, которые используются в технологии **10BaseT** Имеет в основе стандарт IEEE 802.3 См также *10BaseT, Fast Ethernet, IEEE 802.3*

100BaseT4 — спецификация монополосной сети Fast Ethernet со скоростью передачи данных 100 Мбит/с с использованием четырех пар проводов разводки на основе кабелей типа UTP категории 3, 4 или 5 Чтобы гарантировать правильную синхронизацию сигналов, сегмент сети **100BaseT4** не должен превышать в длину более 100 метров Имеет в основе стандарт IEEE 802.3 См также *Fast Ethernet, IEEE 802.3*

100BaseTX — спецификация монополосной сети Fast Ethernet со скоростью передачи данных 100 Мбит/с с использованием двух пар проводов разводки на основе кабелей типа UTP или STP (экранированная витая пара) Первая пара используется для приема данных, а вторая — для передачи Чтобы гарантировать правильную синхронизацию сигналов, сегмент сети 100BaseTX не должен превышать в длину более 100 метров. Имеет в основе стандарт IEEE 802.3. См. также *100BaseX; Fast Ethernet; IEEE 802.3*. **100BaseX** — спецификация монополосной сети Fast Ethernet со скоростью передачи данных 100 Мбит/с, которая включает стандарты сетей Fast Ethernet на оптоволоконном кабеле 100BaseFX и 100BaseTX. Имеет в основе стандарт IEEE 802.3. См. также *100BaseFX; 100BaseTX; Fast Ethernet; IEEE 802.3*.

100VG-AnyLAN — технология среды сетей Fast Ethernet и Token Ring, предусматривающая использование четырех пар проводов кабеля типа UTP категорий 3, 4 или 5. Эта высокоскоростная технология транспорта данных была разработана компанией Hewlett-Packard и может работать в существующих сетях Ethernet 10BaseT. Имеет в основе стандарт IEEE 802.12.

10Base2 — спецификация реализации монополосной сети Ethernet со скоростью передачи данных 10 Мбит/с на 50-омном тонком коаксиальном кабеле. Спецификация 10Base2, являющаяся частью стандарта IEEE 802.3, устанавливает предельное значение протяженности одного сегмента 185 метров. См. также *Ethernet; IEEE 802.3*.

10Base5 — спецификация реализации монополосной сети Ethernet со скоростью передачи данных 10 Мбит/с на стандартном (толстом) монополосном 50-омном коаксиальном кабеле. Спецификация 10Base5, являющаяся частью стандарта монополосного физического уровня IEEE 802.3, устанавливает предельное значение протяженности одного сегмента 500 метров. См. также *Ethernet; IEEE 802.3*.

10BaseF — спецификация монополосной сети Ethernet со скоростью передачи данных 10 Мбит/с, которая включает в себя стандарты реализации сети Ethernet на оптоволоконном кабеле 10BaseFB, 10BaseFL и 10BaseFP. См. также *10BaseFB; 10BaseFL; 10BaseFP; Ethernet*.

10BaseFB — спецификация монополосной сети Ethernet со скоростью передачи данных 10 Мбит/с по ОПТОВОЛОКОННОМУ кабелю. Эта спецификация является частью спецификации IEEE 10BaseF. Такие сети не используются для соединения пользовательских станций, а обеспечивают синхронный магистральный канал, позволяющий подключать к сети дополнительные сегменты и повторители. Сегмент сети 10BaseFB может иметь длину до 2 000 метров. См. также *10BaseF; Ethernet*.

10BaseFL — спецификация монополосной сети Ethernet со скоростью передачи данных 10 Мбит/с по оптоволоконному кабелю. Эта спецификация является частью IEEE 10BaseF и, хотя и способна обеспечивать взаимодействие с сегментами, реализованными по спецификации FOIRL (Fiber Optic

Inter Repeater Link — звено оптоволоконной связи между повторителями), разработана была для замены спецификации FOIRL. Сегменты сети IOBaseFL могут иметь длину до 1 000 метров, если используются совместно с сегментами FOIRL, и до 2 000 метров, если в сети используются только сегменты, реализованные по спецификации IOBaseFL. См. также *WBaseF; Ethernet*.

IOBaseFP — спецификация пассивной монополосной сети Ethernet со скоростью передачи данных 10 Мбит/с по оптоволоконному кабелю. Является частью спецификации IEEE IOBaseF и позволяет объединить ряд компьютеров в топологию "звезда" без применения повторителей. Сегменты сети IOBaseFP могут иметь длину до 500 метров. См. также *IOBaseF; Ethernet*.

IOBaseT — спецификация монополосной сети Ethernet со скоростью передачи данных 10 Мбит/с с использованием двух пар проводников кабеля типа "витая пара" (категорий 3, 4 или 5), при этом одна пара используется для передачи данных, а вторая — для приема данных. Спецификация IOBaseT, являющаяся частью стандарта IEEE 802.3, устанавливает предельное значение протяженности одного сегмента на уровне приблизительно 100 метров. См. также *Ethernet; IEEE 802.3*.

10Broad36 — спецификация широкополосной сети Ethernet со скоростью передачи данных 10 Мбит/с по широкополосному коаксиальному кабелю. Эта спецификация, являющаяся частью стандарта IEEE 802.3, устанавливает предельное значение протяженности одного сегмента 3 600 метров. См. также *Ethernet; IEEE 802.3*.

A

ABM — сбалансированный асинхронный режим. Режим обмена по протоколу HDLC (или производному от него), поддерживающий двухточечную связь между одноранговыми рабочими станциями, когда передачу данных может инициировать каждая станция.

ACK — См. *сигнал подтверждения*. **Address Resolutions Protocol** — См. *ARP*. **Advanced Research Projects Agency** — См. *ARPA*.

AEP — протокол обмена эхо-пакетами в среде AppleTalk (AppleTalk Echo Protocol). Протокол, используемый для проверки возможности установления связи между двумя узлами в сети AppleTalk. Один узел посылает пакет другому узлу и принимает дубликат, или эхо, этого пакета.

AFP — файловый протокол в среде AppleTalk (AppleTalk Filing Protocol). Протокол уровня представлений, который позволяет пользователям коллективно пользоваться файлами данных и прикладными программами, размещенными на файл-сервере. Протокол AFP поддерживает механизмы коллективного использования файлов AppleShare и OS Mac.

ANSI — Американский национальный институт стандартов (American National Standards Institute). Общественная организация, объединяющая корпорации, правительственные органы и другие организации, координирующая связанную со стандартами деятельность; утверждает национальные стандарты США и разрабатывает позицию Соединенных Штатов в международных организациях по разработке стандартов. ANSI участвует в разработке международных и американских стандартов, относящихся, среди прочего, к вопросам коммуникации и создания сетей. ANSI является членом Международной электротехнической комиссии (IEC) и Международной организации по стандартизации (ISO).

API — интерфейс прикладных программ. Спецификация вызовов функций, которые определяют интерфейс к службе.

AppleTalk — ряд коммуникационных протоколов, разработанных компанией Apple Computer и имеющих две фазы. Фаза 1, являющаяся более ранней версией, поддерживает одну физическую сеть, которая может иметь только один сетевой номер и находиться в одной зоне. Фаза 2 поддерживает несколько логических сетей в одной физической сети и позволяет сетям

находиться не только в одной зоне. См. также *зона*.

APPN — развитая архитектура одноранговых сетей (Advanced Peer-to-Peer Networking). Усовершенствованный вариант исходной архитектуры сетевых систем (SNA) компании IBM. APPN определяет порядок установления сеанса между одноранговыми узлами, выполняет динамическое прозрачное вычисление маршрута и приоритезацию трафика расширенного интерфейса межпрограммной связи (APPC).

ARA — протокол удаленного доступа в сетях AppleTalk (AppleTalk Remote Access), который предоставляет пользователям компьютеров Macintosh прямой доступ к информации и ресурсам, находящимся на удаленном AppleTalk-узле.

ARIN — организация, обслуживающая Internet-сообщество, которая предоставляет пользователям помощь, документацию, обучение, услуги по регистрации имен доменов в сети Internet и сетевых адресов, а также другие услуги. Первоначальное название — *InterNIC*.

ARP — протокол преобразования адресов. Internet-протокол, используемый для отображения IP-адреса на MAC-адрес. Определен в документе RFC 826. Сравните с *RARP*.

АРРА — управление перспективных исследовательских проектов. Проектно-исследовательская организация в составе министерства обороны США. Управление ARPA имеет в своем активе многочисленные технологические достижения в области коммуникаций и сетей. ARPA было преобразовано в DARPA, а затем, в 1994 году, опять в ARPA.

ARPANET — сеть управления перспективных исследовательских проектов (Advanced Research Projects Agency Network). Веховая сеть с коммутацией пакетов, установленная в 1969 году. Сеть ARPANET была разработана в 1970-х компанией BBN и финансировалась управлением ARPA (позднее DARPA). В конечном итоге она превратилась в сеть Internet. Термин *ARPANET* был официально упразднен в 1990 году.

ASBR — пограничный маршрутизатор автономной системы (Autonomous System Boundary Router), который находится между автономной OSPF-системой и не OSPF-сетью. На нем выполняется как протокол OSPF, так и какой-либо другой протокол маршрутизации, например RIP. Маршрутизатор ASBR должен размещаться в OSPF-области, которая не является тупиковой.

ASCII — американский стандартный код для обмена информацией (American Standard Code for Information Interchange). 8-разрядный двоичный код (7 бит плюс бит четности) представления символов.

Asynchronous Balanced Mode — См. ABM.

Asynchronous Transfer Mode — См. ATM.

АТМ — режим асинхронной передачи. Международный стандарт метода ретрансляции ячеек, при котором различные типы услуг (например, передача голоса, видеоизображений или данных) преобразовываются в ячейки фиксированной (53 байта) длины. Фиксированная длина ячеек позволяет обрабатывать их аппаратным образом, уменьшая тем самым транзитные задержки. Метод АТМ был разработан для того, чтобы в полной мере использовать возможности таких высокоскоростных сред передачи, как каналы типа ЕЗ, SONET и ТЗ.

АТМ-форум (ATM Forum) — международная организация, основанная в 1991 году компаниями Cisco Systems, NET/ADAPTIVE, Northern Telecom и Sprint, которая разрабатывает и продвигает на рынке стандартизованные рекомендуемые решения по реализации технологии АТМ. АТМ-форум занимается дополнениями к официальным стандартам, разработанным ANSI и ITU-T, и разработкой рекомендуемых решений до появления официальных стандартов.

АТР — протокол транзакций в сетях AppleTalk (AppleTalk Transaction Protocol). Протокол транспортного уровня, который без потерь выполняет транзакции между сокетами. Такая служба позволяет осуществлять обмен между двумя сокет-клиентами, при котором один клиент просит другого выполнить конкретную задачу и сообщить результат. Протокол АТР связывает вместе запрос и ответ, гарантируя тем самым надежный обмен парами запрос/ответ.

AURP — протокол маршрутизации с обновлением маршрутной информации в среде AppleTalk (AppleTalk Update-Based Routing Protocol). Метод инкапсуляции AppleTalk-трафика в заголовок внешнего протокола, позволяющий двум или более разорванным сетевым комплексам Apple Talk соединяться через внешнюю сеть (например, через сеть TCP/IP), образуя глобальную сеть Apple Talk. Такое соединение называется *AURP-тоннелем*. Кроме функции инкапсулирования протокол AURP, благодаря обмену маршрутной информацией между внешними маршрутизаторами, позволяет вести таблицы маршрутизации для всей глобальной сети Apple Talk.

B

Banyan VINES - См. VINES.

Basic Rate Interface — См. BRJ.

BOOTP (Bootstrap Protocol) — протокол начальной загрузки, используемый узлом сети для определения IP-адреса своего интерфейса Ethernet, чтобы использовать его затем при загрузке сетевого программного обеспечения.

Bootstrap Protocol — См. *BOOTP*.

BPDU (bridge protocol data unit) — блок данных протокола обмена между мостами. Пакет приветствия протокола на основе алгоритма охватывающего дерева, который отсылается через конфигурируемые по величине интервалы времени с целью обмена информацией между мостами, стоящими в сети.

BRI — интерфейс передачи данных с номинальной скоростью. ISDN-интерфейс, состоящий из двух В-каналов и одного D-канала для передачи по коммутируемым каналам голоса, видеоизображений и данных. Сравните с *PRL*

В-канал (B channel) — канал-носитель. В технологии ISDN полнодуплексный канал 64 Кбит/с, используемый для посылки пользовательских данных. Сравните с *D-, E- и H-каналом*.

C

CCITT (Consultative Committee for International Telegraph and Telephone) — Консультативный комитет по международной телеграфной и телефонной связи. Международная организация, отвечающая за разработку стандартов в области связи. Современное название ITU-T. См. *ITU-T*.

CDDI (Copper Distributed Data Interface) — распределенный интерфейс передачи данных по медным проводам. Реализация протоколов FDDI при использовании кабелей типа STP или UTP. Технология CDDI позволяет передавать данные на относительно короткие расстояния (около 100 метров), обеспечивая скорость до 100 Мбит/с, при этом для резервного дублирования используется архитектура с двойным кольцом. Имеет в основе стандарт ANSI TRPMD (Twisted-Pair Physical Medium Dependent — стандарт на "витую пару" в качестве физической среды передачи данных). Сравните с *FDDI*.

Challenge Handshake Authentication Protocol — См. *CHAP*.

CHAP — протокол аутентификации по квитированию вызова. Защитная функция, поддерживаемая на линиях связи, использующих PPP-инкапсуляцию, которая предотвращает несанкционированный доступ. Сам протокол не предотвращает несанк-

ционированный доступ, а только идентифицирует противоположную сторону. Затем уже маршрутизатор или сервер доступа определяет, разрешен ли доступ этому пользователю. Сравните с *PAP*.

CIDR — бесклассовая междоменная маршрутизация. Методика, поддерживаемая протоколом BGP, которая основана на агрегировании маршрутов. Техника CIDR позволяет маршрутизаторам группировать маршруты, чтобы отсечь ту информацию, носителями которой являются внутренние маршрутизаторы сети. При использовании метода CIDR несколько IP-сетей выглядят для сетей вне группы как единственный более крупный объект.

CLNS (Connectionless Network Service) — сетевая служба без установления соединения. Служба сетевого уровня модели OSI, которая не требует формирования канала перед передачей данных. Служба CLNS маршрутизирует сообщения до пункта назначения независимо от любых других сообщений.

CMIP (Common Management Information Protocol) — общий протокол передачи управляющей информации. Протокол управления OSI-сетями, созданный и стандартизованный ISO, для мониторинга и управления гетерогенными сетями. См. также CM/5.

CMIS (Common Management Information Services) — служба общей управляющей информации. Интерфейс службы управления OSI-сетями, созданный и стандартизованный ISO, для мониторинга и управления гетерогенными сетями. См. также CM/5.

CO (central office) — центральный офис. Офис местной телефонной компании, к которому подключены все локальные линии связи в данном районе и в котором коммутируются каналы линий абонентов.

CPE (customer premises equipment) — оборудование, устанавливаемое у заказчика. Оконечное оборудование, например терминалы, телефоны, модемы, которое поставляется телефонной компанией, устанавливается на площадке заказчика и подключается к сети этой телефонной компании.

CSMA/CD (carrier sense multiple access with collision detect) — множественный доступ с контролем несущей и обнаружением конфликтов. Механизм доступа к среде, в соответствии с которым устройства, готовые к передаче данных, сначала проверяют канал на присутствие несущей. Если в течение заданного периода времени присутствие несущей не обнаруживается, тогда устройство может передавать. Если передачу начинают сразу два устройства, то возникает конфликт, который обнаруживается всеми сталкивающимися устройствами. В результате выявления конфликта повторная передача этими устройствами задерживается на случайным образом задаваемые периоды времени. Доступ по методу CSMA/CD используется в сетях Ethernet и IEEE 802.3. **CSU (channel service unit)** — блок обслуживания канала. Цифровое интерфейсное устройство, которое соединяет оборудование конечного пользователя с местной телефонной линией. Часто эта аббревиатура используется с другим сокращением DSU: CSU/DSU. См. *DSU*.

D

DARPA (Defense Advanced Research Projects Agency) — управление перспективных исследований и разработок министерства обороны США. Правительственная организация, которая финансирует исследования и экспериментальные работы в области Internet. Прежнее название ARPA, к которому снова вернулись в 1994 году. См. также *AKPA*.

DAS — 1. Станция двойного подключения (dual attachment station). Устройство, подключаемое как к первичному, так и ко вторичному кольцу FDDI. Двойное подключение обеспечивает резервное дублирование для FDDI-кольца. Если отказывает первичное кольцо, то станция может завернуть первичное кольцо на вторичное, изолируя отказ и сохраняя целостность кольца. Также

называется станцией класса А. Сравните с SAS. 2. Динамически назначаемый сокет (dynamically assigned socket). Сокет, который назначается динамически протоколом DDP по запросу клиента. В сети AppleTalk сокеты с номерами от 128 до 254 выделяются в качестве DAS.

DCE — аппаратура передачи данных (data communication equipment) — в интерпретации EIA или оконечное оборудование канала передачи данных (data circuit-terminating equipment) — в интерпретации ITU-T. Устройства и соединения коммуникационной сети, находящиеся со стороны сети интерфейса "пользователь-сеть". Устройства DCE обеспечивают физическое подсоединение к сети, пропуск через себя трафика и выдачу тактовых сигналов, используемых для синхронизации передачи данных между DCE- и DTE-устройствами. Примерами DCE-устройств могут быть модемы и интерфейсные карты. Сравните с DTE.

DDN (Defence Data Network) — сеть передачи данных министерства обороны США. Военная сеть, состоящая из несекретной сети (MILNET) и различных секретных и совершенно секретных сетей. Сеть DDN эксплуатируется и обслуживается DISA.

DDP (Datagram Delivery Protocol) — протокол доставки дейтаграмм. Протокол сетевого уровня в сетях AppleTalk, отвечающий за доставку дейтаграмм из одного сокета в другой в сетевых комплексах AppleTalk.

DDR (dial-on-demand routing) — маршрутизация вызовов по запросу. Техника, при которой маршрутизатор может автоматически инициировать и закрывать сеанс работы по коммутируемым линиям связи по запросу передающей станции. Маршрутизатор имитирует сигналы "я живой", так что конечные станции считают сеанс активным. Метод DDR иногда позволяет осуществлять маршрутизацию по ISDN или телефонным каналам с использованием внешнего терминального ISDN-адаптера или модема.

DECnet Routing Protocol — См. DRP

DECnet — группа коммуникационных продуктов (включая набор протоколов), разработанных и поддерживаемых компанией Digital Equipment Corporation. Последней итерацией является семейство DECnet/OSI (также называемое DECnet Phase V). Эта версия поддерживает как OSI-протоколы, так и протоколы собственной разработки компании Digital. Семейство Phase IV Prime поддерживает наследуемые MAC-адреса, что позволяет DECnet-узлам сосуществовать с системами, выполняющими другие протоколы, которые имеют ограничения по MAC-адресам.

DHCP (Dynamic Host Configuration Protocol) — протокол динамического конфигурирования хост-машины. Протокол, который обеспечивает механизм динамического выделения IP-адресов, так что адреса могут автоматически использоваться повторно после того, как перестают быть нужными хост-машинам.

DNS (Domain Name System) — система доменных имен. Система, используемая в сети Internet, для трансляции имен узлов сети в адреса.

DoD (Department of Defence) — Министерство обороны. Правительственное учреждение, отвечающее за защиту национальной безопасности; часто финансировало разработки коммуникационных протоколов.

DRP (DECnet Routing Protocol) — протокол маршрутизации DECnet. Собственная схема маршрутизации, введенная компанией Digital Equipment Corporation в семейство продуктов DECnet Phase III. В семействе DECnet Phase V был завершен переход на OSI-протоколы маршрутизации (ES-IS и IS-IS).

DSAP (destination service access point) — точка доступа к службам в пункте назначения. Точка доступа к службам в узле сети, указанная в поле Destination ("Пункт назначения") пакета. Сравните с SSAP. См. также SAP.

DSU (digital service unit) — блок обслуживания данных. Устройство, используемое в цифровой передаче данных, которое согласует физический интерфейс DTE-устройства со средствами передачи данных, например с передающей аппаратурой канала T1 или E1. Это устройство также несет ответственность за выполнение таких функций, как, например, синхронизация сигналов. Термин часто используется с аббревиатурой CSU: CSU/DSU. См. также CSU.

DTE (data terminal equipment) — аппаратура обработки данных. Устройство, находящееся в интерфейсе "пользователь-сеть" со стороны пользователя и обслуживающее источник данных, пункт назначения или и того и другого. DTE-устройство подключается к сети передачи данных через DCE-устройство (например, модем) и обычно использует тактовые сигналы, генерируемые DCE-устройством. К DTE-устройствам относятся компьютеры, маршрутизаторы и мультиплексоры. Сравните с *DCE*.

D-канал (D channel) — дельта-канал. 1. Полнодуплексный ISDN-канал с полосой пропускания 16 Кбит/с (интерфейс BRI) или 64 Кбит/с (интерфейс PRI). Сравните с *B*-, *E*- и *//*-каналом. 2. В архитектуре SNA — устройство, которое соединяет процессор и основную память с периферийными устройствами.

E

E1 — схема передачи данных на большие расстояния, используемая преимущественно Европе. Обеспечивает скорость передачи данных 2,048 Мбит/с. Линии связи E1 могут арендоваться у операторов связи в частное пользование. Сравните с *T1*.

E3 — схема передачи данных на большие расстояния, используемая преимущественно Европе. Обеспечивает скорость передачи данных 34,368 Мбит/с. Линии связи E3 могут арендоваться у операторов связи в частное пользование. Сравните с *T3*.

EIA (Electronic Industries Association) — Ассоциация электронной промышленности. Группа, которая вводит стандарты на передачу электрических сигналов. EIA и TIA разработали многочисленные и широко известные стандарты обмена данными, включая EIA/TIA-232 и EIA/TIA-449.

ES-IS (End System-to-Intermediate System) — протокол "конечная система-промежуточная система". OSI-протокол, определяющий способ извещения, которым конечные системы (хост-машины) объявляют о себе промежуточным системам (маршрутизаторам). См. также *IS-IS*.

Ethernet — спецификация монополосной локальной сети, созданной компанией Xerox Corporation, доведенная до документа совместными усилиями компаний Xerox, Intel и Digital Equipment Corporation. В сетях Ethernet используется метод CSMA/CD, и они могут работать на кабелях различных типов со скоростями 10, 100 и 1000 Мбит/с. Спецификация Ethernet подобна набору стандартов IEEE 802.3.

E-канал (E channel) — эхо-канал. ISDN-канал передачи управленческой информации по коммутируемым линиям связи со скоростью 64 Кбит/с. Определение E-канала было введено в спецификации 1984 ИТУ-Т ISDN, однако было изъято из спецификации 1988 года. Сравните с *B*-, *D*- и *E*-каналов.

F

Fast Ethernet — любая из ряда спецификаций на сеть Ethernet со скоростью передачи данных 100 Мбит/с. Спецификация Fast Ethernet обеспечивает в десять раз более высокую скорость передачи данных, чем спецификация 10BaseT Ethernet, одновременно сохраняя такие качества, как формат кадра, механизмы управления доступом к среде и максимальный размер блока передачи. Такое сходство позволяет использовать в сетях Fast Ethernet существующие приложения для сетей 10BaseT и инструментальные средства управления. Имеет в основе дополнение к спецификации IEEE 802.3. Сравните с *Ethernet*. См. также *100BaseFX*, *100BaseT*, *100BaseT4*, *100BaseTX*, *100BaseXu IEEE 802.3*.

FDDI (Fiber Distributed Data Interface) — распределенный интерфейс передачи данных по оптоволоконным каналам. Стандарт локальной сети, описанный в документе ANSI X3T9.5 и определяющий сеть с передачей маркера на основе оптоволоконного кабеля со скоростью 100 Мбит/с на расстояние до 2 км. В целях обеспечения резервного дублирования сети FDDI используют архитектуру с двумя кольцами. Сравните с *CDDI* и *FDDI II*.

FDDI II — стандарт ANSI, который усовершенствует технологию FDDI. Технология FDDI II обеспечивает изохронную передачу для каналов передачи данных без установления соединения и каналов передачи голоса и видеоизображений с установлением соединения. Сравните с *FDDI*.

Fiber Distributed Data Interface - См. FDDI.

File Transfer Protocol — См. FTP.

Frame Relay — стандартный промышленный протокол канального уровня с коммутацией пакетов, который за счет использования формы HDLC-инкапсуляции между соединенными устройствами обеспечивает работу с несколькими виртуальными каналами. Протокол Frame Relay эффективнее, чем протокол X.25, заменой которого он в общем-то считается. См. также X.25.

FTP (File Transfer Protocol) — протокол пересылки файлов. Прикладной протокол, являющийся частью группы протоколов TCP/IP и используемый для пересылки файлов между узлами сети. Протокол FTP описан в документе RFC 959.

G

Get Nearest Server — см. GNS.

GNS — "Мне нужен ближайший сервер". Запросный пакет, посылаемый клиентом в сеть IPX с целью найти ближайший активный сервер конкретного типа. Клиент в сети IPX выдает GNS-запрос, чтобы добиться либо прямого ответа от подключенного сервера, либо ответа от маршрутизатора, в котором будет содержаться информация о том, где в сетевом комплексе может быть получена требуемая услуга. GNS-пакеты являются частью механизма работы протокола IPX SAP. См. также *IPX* и *SAP (протокол извещения об услугах)*.

GUI — графический интерфейс пользователя. Пользовательская среда, которая использует текстовое и графическое представления операций ввода и вывода прикладных программ, а также иерархической или иной структуры данных, в которой хранится информация. Для этой среды типичными являются такие органы управления, как экранные кнопки, пиктограммы и окна, а многие действия выполняются с помощью указательного устройства (например, мыши). Яркими примерами платформ, использующих GUI, являются ОС Microsoft Windows и Apple Macintosh.

H

HDLC (High-Level Data Link Control) — высокоуровневый протокол управления каналом передачи данных. Бит-ориентированный синхронный протокол канального уровня, разработанный ISO. Он задает метод инкапсуляции данных в линиях синхронной последовательной связи с использованием символов кадра и контрольных сумм.

HTML — язык гипертекстовой разметки документов (Hypertext Markup Language). Простой язык форматирования гипертекстовых документов, в котором для указания способа интерпретации заданной части документа прикладной программой визуализации, например Web-браузером, используются дескрипторы (теги).

HTTP — протокол передачи гипертекста (Hypertext Transfer Protocol). Протокол, используемый Web-браузерами и Web-серверами, для передачи файлов, например текстовых и графических.

Hypertext Markup Language — См. *HTML*. **Hypertext Transfer Protocol** - см. *HTTP*.

Н-канал (H channel) — высокоскоростной канал. Полнодуплексный ISDN-канал передачи данных с базовой скоростью при полосе пропускания 384 Кбит/с. Сравните с *B*-, *D*- и *E*-каналом.

I

IAB (Internet Architecture Board) — Архитектурный совет Internet. Совет исследователей в области межсетевого взаимодействия, занимающийся обсуждением вопросов, связанных с архитектурой сети Internet. Назначает состав различных групп, связанных с Internet и межсетевым взаимодействием, например IANA, IESG и IRSG. Состав совета IAB назначается доверенными лицами ISOC. См. также *IANA*; *ISOC*.

IANA (Internet Assigned Numbers Authority) — управление назначения номеров в Internet. Организация, работающая под эгидой ISOC как часть совета IAB. IANA делегирует полномочия по выделению пространств IP-адресов и назначению имен доменов InterNIC и другим организациям. Оно также поддерживает базу данных назначенных идентификаторов протоколов, используемых в группе протоколов TCP/IP, включая номера автономных систем.

ICMP (Internet Control Message Protocol) — протокол управляющих сообщений в Internet. Используемый в сети Internet протокол сетевого уровня, который сообщает об ошибках и обеспечивает другую информацию, связанную с обработкой IP-пакетов. Документирован в RFC 792.

IDF (Intermediate Distribution Facility) — промежуточная распределительная станция. Вторичное помещение для коммуникационного оборудования в здании со звездообразной топологией сети. Промежуточная распределительная станция зависит от главной распределительной станции. См. *MDF*.

IEC (International Electrotechnical Commission) — Международная электротехническая комиссия. Группа, состоящая из представителей компаний-производителей, которая разрабатывает и внедряет стандарты на электротехнические изделия и компоненты.

IEEE (Institute of Electrical and Electronic Engineers) — Институт инженеров по электротехнике и электронике. Профессиональная организация, которая занимается разработкой стандартов в области коммуникаций и сетей передачи данных. Разработанные IEEE стандарты локальных сетей сегодня являются доминирующими.

IEEE 802.2 — разработанный IEEE протокол для локальных сетей, который определяет реализацию LLC-подуровня канального уровня эталонной модели OSI. Протокол IEEE 802.2 обеспечивает работу с ошибками, разбивку на кадры, управление потоком и интерфейс служб сетевого уровня (уровня 3 модели OSI). Используется в локальных сетях IEEE 802.3 и IEEE 802.5. См. также *IEEE 802.3*; *IEEE 802.5*.

IEEE 802.3 — разработанный IEEE протокол для локальных сетей, который определяет реализацию физического уровня и MAC-подуровня канального уровня эталонной модели OSI. В этом протоколе используется доступ по методу CSMA/CD с разными скоростями и в разных физических средах. Дополнения к стандарту IEEE 802.3 определяют реализацию сетей с технологией Fast Ethernet. Физические вариации исходной спецификации IEEE 802.3 включают спецификации 10Base2, 10BaseS, 10BaseF, 10BaseT и 10Broad36. Физические вариации сетей Fast Ethernet включают 100BaseTX и 100BaseFX. IEEE 802.5 — разработанный IEEE протокол для локальных сетей, который определяет реализацию физического уровня и MAC-подуровня канального уровня эталонной модели OSI. В этом протоколе используется доступ с передачей

маркера на скоростях 4 или 16 Мбит/с по кабелям типа STP или UTP. По функциональным и операционным характеристикам эквивалентен протоколу Token Ring компании IBM. См. также *Token Ring*. IETF (Internet Engineering Task Force) — комитет по инженерным проблемам Internet. Состоит из более чем 80 рабочих групп, отвечающих за разработку стандартов для сети Internet. Комитет IETF работает под эгидой ISOC.

IGP (Interior Gateway Protocol) — протоколы внутренних шлюзов. Класс протоколов использующихся для обмена маршрутной информацией в пределах автономной системы. Широко известными примерами протоколов этого класса являются IGRP OSPF и RIP.

IGRP (Interior Gateway Routing Protocol) — протокол внутренней маршрутизации между шлюзами. Протокол класса IGP, разработанный компанией Cisco для решения проблем, связанных с маршрутизацией в больших гетерогенных сетях. Сравните с *усовершенствованным протоколом IGRP*. См. также *IGP; OSPF; RIP*.

Institute of Electrical and Electronic Engineers — см. *IEEE. Integrated Services Digital Network* — см. *ISDN. International Organization for Standardization* — см. *ISO*.

Internet — крупнейший глобальный многосетевой комплекс, соединяющий десятки тысяч сетей во всем мире и имеющий культуру проведения исследований и стандартизации исходя из повседневного использования в реальных условиях. Из Internet-сообщества вышли многие передовые сетевые технологии. Частично прародителем Internet была сеть ARPANET. Одно время эту сеть называли DARPA Internet, но не надо путать с обобщенным английским термином internet, который пишется со строчной буквы.

internet — сокращение от *internetwork*: многосетевой комплекс или в значении прилагательного — межсетевой. См. *многосетевой комплекс*.

Internetwork Packet Exchange — см. *IPX*.

IOS — межсетевая операционная система. См. *ОС IOS компании Cisco*.

IP (Internet Protocol) — межсетевой протокол. Протокол сетевого уровня из состава группы протоколов TCP/IP, предназначенный для обслуживания сетевых комплексов без установления соединения. Протокол IP обладает средствами для адресации, задания типа служб, фрагментации и последующей обратной сборки пакетов, а также для организации защиты информации. Описан в документе RFC 791. IPv4 (Internet Protocol версии 4) является наилучшим протоколом с коммутацией пакетов без установления логического соединения. См. также *IPv6*.

IPv6 — протокол IP версии 6, заменивший текущую версию протокола IP (версию 4). IPv6 включает поддержку идентификаторов потока в заголовке пакета, которые могут использоваться для опознавания потоков. Предыдущее название этого протокола — IPng (протокол IP следующего поколения).

IPX (Internetwork Packet Exchange) — межсетевой протокол обмена пакетами. Протокол сетевого уровня ОС NetWare, используемый для передачи данных от серверов рабочим станциям. Этот протокол похож на протоколы IP и XNS.

IPXWAN (IPX wide-area network) — глобальная IPX-сеть. Протокол, который предусматривает для вновь образуемых связей предварительное согласование опций на обеих сторонах такой связи. При переходе связи в активное состояние первыми посылаются IPXWAN-пакеты, с помощью которых осуществляется взаимное согласование опций на концах связи. После успешного определения IPXWAN-опции начинается нормальная IPX-передача. Этот протокол документирован в RFC 1362.

IP-адрес (IP address) — 32-разрядный двоичный адрес, назначаемый хост-машинам, использующим протокол TCP/IP. IP-адрес принадлежит одному из пяти классов (A, B, C, D, E) и записывается в виде четырех октетов, разделяемых точкой (т.е. в десятичном представлении с разделением точками). Каждый адрес включает номер сети, необязательный номер подсети и номер хост-машины. Номера сети и подсети используются вместе для маршрутизации, а номер хост-машины — для адресования отдельной хост-машины, находящейся в сети или подсети. Для извлечения из IP-

адреса информации о сети и подсети используется маска подсети. Новый способ представления IP-адресов и масок подсети дает метод CIDR. IP-адрес также называют *Internet-адресом*.

IP-дейтаграмма (IP datagram) — основная единица информации, передаваемой в сети Internet. Содержит адреса источника и пункта назначения с данными и ряд полей, которые задают такие величины, как длина дейтаграммы, контрольная сумма заголовка и флаги, указывающие на то, может ли дейтаграмма быть (или была) фрагментирована.

ISDN (Integrated Services Digital Network) — цифровая сеть с предоставлением комплексных услуг. Коммуникационный протокол, предлагаемый телефонными компаниями, который позволяет передавать по телефонным сетям данные, речь и трафик других источников.

IS-IS (Intermediate System-to-Intermediate System) — протокол "промежуточная система — промежуточная система". OSI-протокол иерархической маршрутизации с учетом состояния каналов связи, основанный на DECnet Phase V-маршрутизации, когда для выяснения топологии промежуточные системы (маршрутизаторы) обмениваются маршрутной информацией, имеющей в основе только одну метрику. См. также *ES-IS*; *OSPF*.

ISO (International Organization for Standardization) — Международная организация по стандартизации. Международная некоммерческая организация, разрабатывающая и распространяющая научные и технологические стандарты, включая и те, что относятся к области создания сетей. ISO разработала OSI — популярную эталонную модель структуры работы сети.

ISOC (Internet Society) — сообщество Internet. Международная некоммерческая организация, основанная в 1992 году. Занимается координацией развития и использования сети Internet. Кроме того, ISOC делегирует полномочия другим группам, связанным с деятельностью Internet, например IAB. Штаб-квартира ISOC находится в г. Рестон, штат Вирджиния, США. См. также *IAB*.

ITU-T (International Telecommunication Union Nelecommunication Standardization Sector) — сектор стандартизации телекоммуникаций Международного союза по электросвязи. Ранее назывался Консультативным комитетом по международной телеграфной и телефонной связи (ССИТТ). Международная организация, разрабатывающая стандарты в области телекоммуникаций. См. также *ССИТТ*.

L

LAN — локальная сеть (local-area network). Высокоскоростная с минимальным количеством ошибок сеть передачи данных, охватывающая относительно небольшую территорию (до нескольких тысяч метров). Локальные сети соединяют рабочие станции, периферийное оборудование, терминалы и другие устройства, располагающиеся в одном здании или в другой территориально ограниченной области. Стандарты локальных сетей задают методы реализации кабельной системы и наборы сигналов на физическом и канальном уровнях эталонной модели OSI. Широко используемыми технологиями локальных сетей являются Ethernet, FDDI и Token Ring. Сравните с *MAN (региональная сеть)* и *WAN (глобальная сеть)*.

LAPB (Link Access Procedure, Balanced) — процедура сбалансированного доступа к каналу. Протокол канального уровня из группы протоколов X.25. LAPB является бит-ориентированным протоколом, производным от протокола HDLC. См. также *HDLC*; *X.25*.

LAPD (Link Access Procedure on the D channel) — процедура доступа к D-каналу. ISDN-протокол канального уровня для работы в D-канале. LAPD является производным от протокола LAPB и был разработан главным образом для того, чтобы удовлетворить сигнальные требования механизма основного доступа протокола ISDN. Определен в документах ITU-T "Рекомендации Q.920" и "Рекомендации Q.921".

LAT (Local-Area Transport) — протокол доступа к терминалу. Сетевой протокол для работы с виртуальным терминалом, разработанный компанией Digital Equipment Corporation.

Link Access Procedure on the D channel — см. *LAPD*. Link Access Procedure, Balanced — см. *LAPB*.

Link layer — См. *канальный уровень*.

LLC (logical link control) — управление логическим каналом. Высший из двух подуровней канального уровня, определенных IEEE. LLC-подуровень несет ответственность за управление ошибками, управление потоком данных, разбиением на кадры и адресацию на MAC-подуровне. Наиболее распространенным LLC-протоколом является IEEE 802.2, который включает варианты без установления соединения и с установлением соединения.

LSA (Link-State Advertisement) — пакет объявления о состоянии канала. Широковещательный пакет, используемый протоколами с учетом состояния канала связи, который содержит информацию о соседях и стоимости путей. LSA-пакеты используются принимающими маршрутизаторами для ведения своей таблицы маршрутизации. Иногда эти пакеты называют *пакетами состояния канала связи (LSP)*.

М

MAC (Media Access Control) — уровень управления доступом к среде. Нижний из двух подуровней канального уровня, определенных IEEE. MAC-подуровень определяет способ доступа к среде коллективного пользования, например, будет ли использоваться передача маркера или режим конкуренции. См. также *канальный уровень*; *LLC*.

MAC-адрес (MAC address) — стандартизованный адрес канального уровня, который должен быть у каждого устройства, подключенного к локальной сети. Другие устройства в сети используют эти адреса для нахождения местоположения конкретных устройств в сети и для создания и обновления таблиц маршрутизации и структур данных. MAC-адреса имеют длину 6 байт и контролируются IEEE. Также известен под названием *аппаратный адрес*, или *физический адрес*. Сравните с *сетевым адресом*.

MAN (Metropolitan-Area Network) — региональная сеть. Сеть, которая охватывает регион. В общем случае региональная сеть охватывает большую область, чем локальная сеть, но меньшую, чем глобальная сеть. Сравните с *LAN* и *WAN*. Management Information Base — См. *MIB*.

MAU (Media Attachment Unit) — блок подключения к среде. Устройство, используемое в сетях Ethernet и IEEE 802.3, которое обеспечивает интерфейс между портом AUI станции и общей средой Ethernet. Блок подключения к среде, который может быть встроенным в устройство или отдельным устройством, выполняет функции физического уровня модели OSI, включая преобразование цифровых данных, поступающих из интерфейса Ethernet, обнаружение конфликтов и ввод битов в сеть. Иногда его называют *блоком управления доступом к среде (media access unit)*, сокращенно — тоже MAU, или *трансивером*. В сетях Token Ring блок подключения к среде известен под названием *блока многостанционного доступа (multistation access unit)*, и обычно во избежание путаницы используют сокращенное название MSAU.

MDF (Main Distribution Facility) — главная распределительная станция. Основное помещение для коммутационного оборудования в здании. Центральная точка сети с топологией "звезда", в которой размещаются коммутационные панели, концентратор и маршрутизатор.

Media Access Control — См. *MAC*.

Media Access Unit — см. *MAU*.

MIB (Management Information Base) — база данных управляющей информации. База данных сетевой управляющей информации, которая используется и поддерживается протоколом

управления сетью, например протоколом SNMP. Значение объекта MIB может изменяться или извлекаться с помощью команд протокола SNMP, обычно посредством графического интерфейса пользователя системы управления сетью. Объекты MIB организованы в древовидную структуру, которая включает открытые (стандартные) и частные (оригинальной природы) ветви.

MSAU (Multistation Access Unit) — блок многостанционного доступа. Концентратор разводки, к которому подключаются все конечные станции сети Token Ring. MSAU обеспечивает интерфейс между этими устройствами и интерфейсом Token Ring маршрутизатора. Иногда используется аббревиатура MAU.

MTU (Maximum Transfer Unit) — максимальный блок передачи. Максимальный размер пакета в байтах, с которым может работать конкретный интерфейс.

N

NAK (Negative Acknowledgment) — сигнал отрицательного подтверждения. Ответ, посылаемый принимающим устройством посылающему устройству, говорящий о том, что принятая информация содержит ошибки. Сравните с *сигналом подтверждения ACK*.

NAT (Network Address Translation) — трансляция сетевого адреса. Механизм для уменьшения потребности в глобально уникальных IP-адресах. Позволяет организации с адресами, которые не являются глобально уникальными, подключаться к сети Internet, транслируя эти адреса в глобально маршрутизируемое адресное пространство. Также называют *транслятором сетевых адресов*.

NAUN (nearest active upstream neighbor) — ближайший активный соседний узел в направлении восходящего потока данных. В сетях Token Ring или IEEE 802.5 — ближайшее, находящееся в активном состоянии сетевое устройство в направлении восходящего потока данных от какого-либо заданного устройства.

NCP (Network Control Program) — программа управления сетью. В архитектуре SNA программа, которая маршрутизирует и управляет потоком данных между контроллером связи (в котором она размещается) и другими ресурсами сети.

NetBEUI (NetBIOS Extended User Interface) — расширенный интерфейс пользователя NetBIOS. Усовершенствованная версия протокола NetBIOS, используемого сетевой операционной системой, например LAN Manager, LAN Server, Windows for Workgroups и Windows NT. Этот протокол формализует транспортные кадры и обеспечивает ряд дополнительных функций. NetBEUI реализует протокол OSI LLC2.

NetBIOS (Network Basic Input/Output System) — сетевая базовая система ввода/вывода. Интерфейс прикладного программирования, используемый приложениями в локальных IBM-совместимых сетях для запроса услуг от сетевых процессов более низкого уровня. Эти услуги могут включать установление и завершение сеанса и передачу информации. **NetWare Link Services Protocol** — См. *NLSP*. **NetWare Loadable Module** - см. *NLM*.

NetWare — популярная распределенная сетевая операционная система, разработанная компанией Novell. Обеспечивает прозрачный доступ к удаленным файлам и другие многочисленные распределенные сетевые услуги.

Network Basic Input/Output System — См. *NetBIOS*.

Network File System - см. *NFS*

NFS (Network File System) — сетевая файловая система. Обычно так называют группу протоколов распределенной файловой системы, разработанных компанией Sun Microsystems,

которые позволяют осуществлять доступ к удаленным файлам по сети. Фактически NFS — это просто один из протоколов этой группы. Протоколы NFS реализуют механизмы вызова удаленных процедур (RPC) и внешнего представления данных (XDR). Эти протоколы являются частью более крупной архитектуры, которую компания Sun называет ONC (так называемая архитектура открытых сетевых вычислений. — *Прим. перев.*).

NIC — 1. Плата сетевого интерфейса (network interface card). Печатная плата, которая обеспечивает компьютерной системе возможность двусторонней связи. Также называют *адаптером*. 1. Центр информации о сетях (Network Information Center). Организация, функции которой взяла на себя другая организация— ARIN. См. *ARIN*.

NLM (NetWare Loadable Module) — загружаемый модуль ОС NetWare. Отдельная программа, которая может загружаться в память и функционировать как часть сетевой операционной системы NetWare.

NLSP NetWare (NetWare Link Service Protocol) — протокол обслуживания канала ОС NetWare. Протокол маршрутизации с учетом состояния канала, основанный на протоколе *IS-IS*.

NMS (Network Management System) — система управления сетью. Система, ответственная за управление по крайней мере частью сети. Обычно NMS представляет собой достаточно мощный и хорошо укомплектованный компьютер, например инженерная рабочая станция. NMS связывается с агентами, помогая вести статистику сети и отслеживать имеющиеся сетевые ресурсы.

NOS (Network Operation System) — сетевая операционная система. Распределенные файловые системы, например, LAN Manager, NetWare, NFS, VINES и Windows NT.

Novell IPX - см. *IPX*.

NTP (Network Tune Protocol) — протокол сетевого времени. Протокол, созданный поверх протокола TCP, который гарантирует ведение точного местного времени за счет синхронизации по радиосигналам точного времени или с атомными часами, стоящими в сети Internet. Этот протокол позволяет синхронизировать географически удаленные системные часы с точностью до миллисекунд на продолжительный период времени.

NVRAM — энергонезависимая память. Запоминающее устройство, которое сохраняет содержимое при прекращении подачи электроэнергии на блок питания.

O

ODI (Open Data-link Interface) — открытый интерфейс канала данных. Спецификация компании Novell, обеспечивающая стандартизованный интерфейс для плат сетевого интерфейса, который позволяет одной плате работать с несколькими протоколами.

Open Shortest Path First — см. *OSPF*.

Open System Interconnection — см. *OSI*.

OSI (Open System Interconnection) — взаимодействие открытых систем. Международная программа по стандартизации, открытая ISO и ИТУ-Т с целью разработки стандартов создания сетей передачи данных, которые бы облегчили обеспечение совместимости работы оборудования различных поставщиков.

OSI-адрес представления (OSI presentation address) — адрес, используемый для указания местонахождения объекта OSI-приложения. Он состоит из сетевого OSI-адреса и нескольких (до трех) селекторов, по одному для использования объектами транспортного, сеансового уровней и уровня представлений.

OSPF (Open Shortest Path First) — открытый протокол выбора первого кратчайшего пути.

Иерархический алгоритм маршрутизации с учетом состояния канала связи класса ЮР, предложенный Internet-сообществу в качестве преемника протокола RIP. Функциональные особенности этого протокола включают маршрутизацию по наименьшей стоимости, многопутевую маршрутизацию и балансировку нагрузки. Протокол OSPF был разработан на основе ранней версии протокола IS-IS.

OUI (Organizational Unique Identifier) — уникальный идентификатор организации. Назначаемые ШЕЕ три октета из состава блока 48-разрядного адреса в локальной сети.

Р

PAP (Password Authentication Protocol) — протокол аутентификации по паролю, который позволяет одноранговым PPP-клиентам аутентифицировать друг друга. От удаленного маршрутизатора, пытающегося связаться с локальным маршрутизатором, требуется, чтобы он послал запрос на аутентификацию. В отличие от протокола CHAP, протокол PAP посылает пароль и имя хост-машины или имя пользователя в открытом (незашифрованном) виде. Сам по себе протокол PAP не предотвращает несанкционированный доступ, а просто идентифицирует противоположную сторону. После этого маршрутизатор или сервер доступа сам определяет, разрешать ли данному пользователю доступ. Протокол PAP поддерживается только PPP-каналами связи. Сравните с CHAP.

Password Authentication Protocol — См. PAP.

PDN (Public Data Network) — сеть передачи данных общего пользования. Сеть, находящаяся под управлением либо правительства (как в Европе), либо частной компании и предоставляющая услуги по организации связи между компьютерами населению, обычно за плату. Такие сети позволяют небольшим организациям создавать глобальные сети, не неся затрат, связанных со стоимостью оборудования для связи на большие расстояния.

PDU (Protocol Data Unit) — блок данных протокола. Термин OSI для пакета.

PHY — 1. Физический подуровень. Один из двух подуровней физического уровня технологии FDDI. 2. Физический уровень. В технологии ATM физический уровень обеспечивает передачу ячеек в физической среде, которая соединяет два ATM-устройства. Физический уровень включает два подуровня: PMD и TC.

PLP (Packet Level Protocol) — протокол пакетного уровня. Протокол сетевого уровня из группы протоколов X.25. Иногда его называют *протоколом X.25 уровня 3* и *X.25-оооколом*. См. также X.25.

Point-to-Point Protocol — См. PPP.

POST (Power-On Self-Test) — автопроверка после включения питания. Набор диагностик, которые выполняются аппаратной частью устройства после подачи на него электропитания.

PPP (Point-to-Point Protocol) — протокол двухточечной связи. Преемник протокола SLIP. Этот протокол устанавливает соединения "маршрутизатор—маршрутизатор" и хост-машина—сеть" по синхронным и асинхронным линиям связи. Если протокол SLIP был спроектирован для работы только с протоколом IP, то протокол PPP — для работы с несколькими протоколами сетевого уровня, включая IP, IPX и ARA. Протокол PPP также имеет встроенный механизм защиты информации: протоколы CHAP и AP. В своей основе опирается на два протокола: LCP и NCP.

PRI (Primary Rate Interface) — интерфейс передачи с основной скоростью. ISDN-нтерфейс основного доступа. Средства основного доступа включают один D-канал 64 бит/с плюс 23 (T1) или 30 (E1) B-каналов для передачи речи и данных.

Proxy Address Resolution Protocol — См. *протокол ARP с посредником*.

PVC (Permanent Virtual Circuit) — постоянный виртуальный канал. Постоянные виртуальные каналы сберегают полосу пропускания, связанную с процессом установления канала, и разрываются в ситуациях, когда определенные виртуальные каналы должны существовать все время. В ATM-терминологии они называются постоянными виртуальными соединениями. Сравните с *SVC*.

Q-R

QoS (quality of service) — качество обслуживания. Мера качества работы системы передачи данных, которая отражает качество передачи и доступность услуг.

RARP (Reverse Address Resolution Protocol) — протокол обратного преобразования адреса. Протокол из группы протоколов TCP/IP, который обеспечивает метод нахождения IP-адресов на основе MAC-адресов. Сравните с *ARP*.

RFC (Request for Comments) — запрос на комментарий. Серия документов, используемых в качестве основного средства для доведения информации о технологии Internet. Некоторые запросы на комментарий" назначаются IAB стандартами Internet. Большинство "запросов комментариев" документируют спецификации протоколов, например Telnet и FTP, но некоторые носят юмористический или исторический характер. Эти документы доступны в интерактивном режиме из многочисленных источников.

RIP (Routing Information Protocol) — протокол маршрутной информации. Протокол класса ЮР, поставляемый с UNIX BSD-системами. Наиболее широко используемый IGP-протокол в Internet. В качестве метрики маршрутизации этот протокол использует количество переходов.

RMON (Remote Monitoring) — дистанционный мониторинг. Спецификация MIB-агента, описанная в RFC 1271, который определяет функции дистанционного мониторинга сетевых устройств. Спецификация RMON предусматривает наличие многочисленных функциональных возможностей по мониторингу, нахождению проблем и формированию отчетов.

Routing Table Maintenance Protocol — См. *RTMP*.

RFC (Remote Procedure Call) — вызов удаленной процедуры. Технологическая основа клиент-серверных вычислений. Вызовы удаленной процедуры строятся или задаются клиентом и исполняются сервером, при этом результат возвращается по сети клиенту.

RPF (Reverse Path Forwarding) — переадресация по обратному пути. Техника многоадресной передачи, при которой многоадресная дейтаграмма направляется на все интерфейсы, кроме того, на котором она была принята, если принимающий интерфейс является тем, который использовался для перенаправления одноадресных дейтаграмм к источнику многоадресной дейтаграммы.

RSVP (Resource Reservation Protocol) — протокол резервирования ресурсов. Протокол, который поддерживает резервирование ресурсов в IP-сети. Приложения, выполняемые на оконечных системах, стоящих в IP-сети, могут использовать протокол RSVP для того, чтобы сообщать другим узлам характер (полоса пропускания, нечеткая синхронизация, максимальный размер пачки пакетов и т.д.) потоков пакетов, которые они способны принимать. Этот протокол функционирует с протоколом IPv6. Его также называют *протоколом настройки резервирования ресурсов* (Resource Reservation Setup Protocol).

RTMP (Routing Table Maintenance Protocol) — протокол управления таблицами маршрутизации. Протокол маршрутизации разработки компании Apple Computer. Этот протокол формирует и управляет маршрутной информацией, требующейся для прокладывания маршрутов дейтаграмм от произвольного сокета-отправителя до произвольного сокета-получателя в сети AppleTalk. Используя протокол RTMP, маршрутизаторы динамически управляют содержимым таблиц маршрутизации для отражения изменений в топологии. RTMP является производным от протокола RIP.

RTP — 1. Протокол таблиц маршрутизации (Routing Table Protocol). Основанный на протоколе RIP протокол маршрутизации для архитектуры VINES (Virtual Networking System). Распространяет информацию о топологии сети и помогает VINES-серверам найти соседние клиенты серверов и маршрутизаторы. В качестве метрики маршрутизации использует величину задержки. 2. Быстрый транспортный протокол (Rapid Transport Protocol). Протокол, который задает темп продвижения и исправляет ошибки данных, пересекающих APPN-сеть. При использовании протокола RTP восстановление после ошибок и управление потоком данных осуществляется не в каждом узле, а на концах установленного соединения. Этот протокол скорее предотвращает перегрузку, чем реагирует на нее. 3. Транспортный протокол реального времени (Real-Time Transport Protocol). Один из протоколов, входящих в состав протокола IPv6. Спроектирован, чтобы обеспечить функцию сквозного транспорта в сети для приложений, передающих данные в реальном времени (например, таких, как аудио- и видеоданные или данные моделирования) с использованием много- или одноадресных служб. Протокол RTP предоставляет такие услуги, как идентификация типа полезной нагрузки, нумерация последовательностей, снабжение метками времени и мониторинг доставки для приложений реального времени.

S

SAP (Service Access Point) — 1. Точка доступа к службе. Поле, заданное в спецификации IEEE 802.3, которое идентифицирует процесс верхнего уровня и является частью спецификации адреса. Таким образом, адрес пункта назначения и DSAP (точка доступа к службе в пункте назначения) определяют получателя пакета. То же самое справедливо и в отношении SSAP (точка доступа к службе в источнике). 2. Протокол объявления об услугах (Service Advertising Protocol). IPX-протокол, который обеспечивает средства для информирования сетевых клиентов через маршрутизаторы и серверы о доступных сетевых ресурсах и услугах.

SAS (Single Attachment Station) — станция с однократным подключением. Устройство, подключаемое только к первичному кольцу сети FDDI. Также известна под названием *станции класса В*. Сравните с DAS. См. также FDDI.

SDLC (Synchronous Data Link Control) — протокол управления синхронным каналом передачи данных. Коммуникационный протокол канального уровня модели SNA. Представляет собой бит-ориентированный полнодуплексный протокол последовательной передачи данных, породивший большое количество похожих протоколов, включая HDLC и LAPB.

Sequenced Packet Exchange — См. SPX. **Service Advertising Protocol** — см. SAP.

SLIP (Serial Line Internet Protocol) — протокол последовательной межсетевой связи. Стандартный протокол для двухточечных последовательных соединений, использующих различные варианты протокола TCP/IP. Предшественник протокола PPP.

SMI (Structure of Management Information) — структура управленческой информации. Документ (RFC 1155), определяющий правила, используемые для описания объектов управления в базе данных MIB.

SNA (Systems Network Architecture) — архитектура сетевых систем. Большая, сложная многофункциональная архитектурная модель, разработанная в 1970-х годах компанией IBM. В некоторых отношениях подобна эталонной модели OSI, однако имеет ряд отличий. Фактически модель SNA состоит из 7 уровней. См. *уровень управления потоком данных; уровень управления каналом; уровень управления путем; уровень физического управления; уровень обслуживания представлений; уровень обслуживания транзакций; уровень управления передачей*.

SNAP (Subnetwork Access Protocol) — протокол доступа к подсети. Межсетевой протокол, который работает между сетевым объектом подсети и сетевым объектом в оконечной системе. Протокол SNAP определяет стандартный метод инкапсуляции IP-дейтаграмм и ARP-сообщений в IEEE-сетях.

SNAP-объект в оконечной системе использует услуги, предоставляемые подсетью, и выполняет три ключевые функции: передачу данных, управление соединением и выбор параметра качества обслуживания (QoS).

SNMP (Simple Network Management Protocol) — простой протокол управления сетью. Протокол управления сетью, используемый почти исключительно в TCP/IP-сетях. Протокол SNMP обеспечивает средства для мониторинга и управления сетевыми устройствами, а также для управления конфигурациями, сбором статистических данных, производительностью и защитой информации.

SPF (Shortest Path First) — алгоритм выбора первого кратчайшего пути. Алгоритм маршрутизации, который итеративным образом рассчитывает длину пути для нахождения охватывающего дерева с кратчайшим путем. Обычно используется в алгоритмах маршрутизации с учетом состояния канала связи. Иногда называют *алгоритмом Дейкстры* (Dijkstra's algorithm).

SPP (Sequenced Packet Protocol) — протокол последовательной передачи пакетов. Обеспечивает надежную с управлением потоком и установлением соединения передачу пакетов от имени процессов клиента. Входит в состав группы протоколов XNS.

SPX (Sequenced Packet Exchange) — протокол последовательного обмена пакетами. Надежный с установлением соединения протокол, который дополняет возможности службы обслуживания дейтаграмм протоколов сетевого уровня модели OSI. Компания Novell разработала этот широко используемый транспортный протокол OS NetWare на основе протокола SPP из состава группы протоколов XNS.

SQE (Signal Quality Error) — ошибка качества сигнала. В сетях Ethernet посылка, осуществляемая трансивером контроллеру для того, чтобы дать ему знать, функционирует ли цепь обнаружения конфликтов. Его также называют *пульсом*.

SSAP (Source Service Access Point) — точка доступа к службе источника. Точка доступа к службе узла сети, заданная в поле пакета "Источник" ("Source"). Сравните с *DSAP*. См. также *SAP*.

STP (Shielded Twisted-Pair) — экранированная витая пара. Среда разводки с двумя парами проводов, используемая в разнообразных вариантах реализации сети. В целях снижения влияния электромагнитных помех кабель типа STP имеет слой изоляции, окруженный экраном. Сравните с *UTP*.

SVC (switched virtual circuit) — коммутируемый виртуальный канал. Виртуальный канал, динамически создаваемый по запросу и уничтожаемый после завершения передачи. Коммутируемые виртуальные каналы используются в ситуациях, когда передача данных носит спорадический характер. В терминологии технологии ATM называются *коммутируемыми виртуальными соединениями*. Сравните с *PVC*.

T

T1 — средства оператора цифровой глобальной сети, позволяющие передавать по коммутируемой телефонной сети данные в формате DS-1 со скоростью 1,544 Мбит/с, используя алгоритмы кодирования AMI (с чередующейся инверсией единиц) и B8ZS (с заменой восьми последовательных нулей). Сравните с *E1*.

T3 — средства оператора цифровой глобальной сети, позволяющие передавать по коммутируемой телефонной сети данные в формате DS-3 со скоростью 44,736 Мбит/с. Сравните с *E3*.

TACACS (Terminal Access Controller Access Control System) — система управления доступом с помощью контроллера доступа к терминалу. Разработанный сообществом пользователей

цифровых сетей передачи данных протокол аутентификации, который обеспечивает аутентификацию в процессе удаленного доступа и связанные с этим услуги, например протоколирование событий. Пароли пользователей хранятся в центральной базе данных, а не в отдельных маршрутизаторах, что обеспечивает получение легко масштабируемых решений защиты сети.

TCP (Transmission Control Protocol) — протокол управления передачей. Протокол транспортного уровня с установлением соединения, обеспечивающий надежную полнодуплексную передачу данных. Входит в состав группы протоколов TCP/IP.

TCP/IP (Transmission Control Protocol/Internet Protocol) — протокол управления передачей/межсетевой протокол. Общее название группы протоколов, разработанных министерством обороны США в 1970-х годах для поддержки строительства многосетевых комплексов, разбросанных по всему миру. Протоколы TCP и IP — наиболее известные из этой группы.

Telnet — стандартный протокол эмуляции терминала из группы протоколов TCP/IP. Протокол Telnet используется для организации соединений с удаленного терминала и позволяет пользователям входить в удаленную систему и использовать ее ресурсы так, словно они подключены к локальной системе. Описан в RFC 854.

TFTP (Trivial File Transfer Protocol) — простейший протокол передачи. Упрощенная версия протокола FTP, позволяющая передавать файлы с одного компьютера на другой по сети.

Time To Live — См. *TTL*.

Token Ring — локальная сеть с передачей маркера, разработанная и поддерживаемая компанией IBM. Сети Token Ring работают со скоростями передачи 4 или 16 Мбит/с и используют кольцевую топологию. Подобна сети IEEE 802.5.

TokenTalk — продукт канального уровня компании Apple Computers, который позволяет соединиться с AppleTalk-сетью по кабелям стандарта Token Ring.

traceroute — имеющаяся во многих системах программа, которая прослеживает путь пакета до пункта назначения. Используется главным образом для отладки процесса маршрутизации между хост-машинами. Существует также протокол отслеживания, определенный в RFC 1393.

Transmission Control Protocol — См. *TCP*.

TTL (Time To Live) — время жизни. Поле IP-заголовка, показывающее, как долго пакет считается достоверным.

U

UDP (User Datagram Protocol) — протокол дейтаграмм пользователя. Протокол транспортного уровня без установления соединения из группы протоколов TCP/IP. UDP — это простой протокол, который обеспечивает обмен дейтаграммами без подтверждений или гарантий доставки, требуя, чтобы обработку ошибок и повторение передач контролировал какой-либо другой протокол. Документирован в RFC 768.

UPS (Uninterruptable Power Supply) — источник бесперебойного питания. Резервное устройство, спроектированное для обеспечения бесперебойной подачи электропитания в случае отказа сети электропитания. UPS обычно устанавливаются на файл-серверы и концентраторы.

URL (Universal Resource Locator) — универсальный указатель ресурсов. Стандартизованная схема адресации для обращений к гипертекстовым документам и другим службам, используемым браузером.

User Datagram Protocol — См. *UDP*.

UTP (Unshielded Twisted-Pair) — неэкранированная витая пара. Среда разводки с четырьмя парами проводов, используемая в разнообразных сетях. UTP-кабель не требует фиксированного шага между соединениями, что необходимо при коаксиальных соединениях. Сравните с *STP*.

V

VINES (Virtual Integrated Network Service) — виртуальная сеть с интегрированными услугами. Сетевая ОС, разработанная и предлагаемая на рынке компанией Banyan Systems.

VLAN — виртуальная локальная сеть. Группа устройств локальной сети, которые конфигурируются (с использованием программного обеспечения управления) таким образом, что могут участвовать в обмене данными так, словно подключены к одному кабелю, хотя на самом деле они находятся в различных сегментах сети. Поскольку виртуальные сети основываются на виртуальных, а не физических соединениях, то они обладают чрезвычайно высокой гибкостью.

W-X

WAN (Wide-Area Network) — глобальная сеть. Сеть передачи данных, обслуживающая пользователей в широкой географической области и часто использующая передающую аппаратуру операторов связи. Примерами глобальных сетей являются Frame Relay, SMDS и X.25. Сравните с *LAN* и *MAN*.

X.25 — стандарт ИТУ-Т, который определяет способ поддержания соединений между DTE и DCE при доступе через удаленный терминал или при обмене данными между компьютерами в сетях общего пользования. Стандарт X.25 вводит определение протокола канального уровня LAPB и протокола сетевого уровня PLP. Протокол Frame Relay до некоторой степени превосходит протокол X.25.

XNS (Xerox Network Systems) — сетевая система компании Xerox. Группа протоколов, первоначально разработанная в Исследовательском центре компании Xerox в Паоло Альто. Многие компании, занимающиеся технологиями сетей ПК, например 3Com, Banyan, Novell и UB Networks, использовали или используют сейчас различные варианты XNS в качестве основного транспортного протокола.

Z

ZIP (Zone Information Protocol) — протокол передачи информации о зонах. AppleTalk-протокол сеансового уровня, который отображает номера сетей на имена зон. Протокол ZIP используется протоколом привязки имен NBP для определения сетей, содержащих узлы, которые принадлежат зоне.

A

Агент (Agent) — 1. В общем случае это программное обеспечение, которое от имени приложения

посылает запросы и принимает ответы. 2. В системах управления сетью процесс, который размещается во всех управляемых устройствах и сообщает станциям управления сетью значения заданных переменных.

Адаптер (Adapter) — См. *NIC*.

Администратор сети (Network Administrator) — человек, который отвечает за работу, техническое обслуживание и управление сети.

Адрес (Address) — структура данных или логическое условное обозначение, используемые для идентификации некоего уникального объекта, например конкретного процесса или сетевого устройства.

Адрес MAC-уровня (MAC-layer address) — См. *MAC-адрес*. **Адрес отправителя (Source Address)** — адрес сетевого устройства, отправляющего данные.

Адрес подсети (Subnet Address) — часть IP-адреса, задаваемая маской подсети в качестве идентификатора подсети.

Адрес пункта назначения (Destination Address) — адрес сетевого устройства, принимающего данные. См. также *адрес источника*.

Адрес хост-машины (Host Address) — См. *номер хост-машины*.

Активный монитор (Active Monitor) — устройство, ответственное за выполнение функций сопровождения в сети Token Ring. В качестве активного монитора выбирается узел сети, который имеет самое высокое значение MAC-адреса в кольце. Активный монитор ответствен за решение таких задач по поддержанию работоспособности кольца, как обеспечение отсутствия потерь маркера и недопущение бесконечного циркулирования кадров.

Алгоритм (Algorithm) — строго определенное правило или процесс решения задачи. В сетях алгоритмы обычно используются для определения наилучшего маршрута трафика от конкретного отправителя к конкретному получателю.

Алгоритм маршрутизации по вектору расстояния (Distance-Vector Routing Algorithm) —

класс алгоритмов маршрутизации, которые при определении охватывающего дерева с кратчайшим путем предусматривают итерационные вычисления на основе количества переходов в маршруте. Алгоритмы маршрутизации по вектору расстояния заставляют каждый маршрутизатор посылать в каждом пакете обновления маршрутной информации всю свою таблицу маршрутизации, но только в отношении маршрутов до своих соседей. Такие алгоритмы могут быть склонны к образованию петель маршрутизации, но с вычислительной точки зрения они проще, чем алгоритмы с учетом состояния каналов связи. Также называется алгоритмом маршрутизации Беллмана-Форда (Bellman-Ford algorithm).

Алгоритм маршрутизации с учетом состояния канала связи (Link-State Routing Algorithm) — алгоритм маршрутизации, в соответствии с которым каждый маршрутизатор с помощью широковещательных или многоадресных пакетов сообщает всем узлам многосетевого комплекса информацию о стоимости связи с каждым из его соседей. Алгоритм с учетом состояния каналов связи создает совместимую картину сети и поэтому не склонен к образованию петель маршрутизации, но достигается это за счет относительно высокой вычислительной нагрузки и более разбросанного по площади трафика, чем это имеет место в случае применения алгоритмов на основе вектора расстояния. Сравните с *алгоритмом маршрутизации по вектору расстояния*.

Алгоритм распределенного связующего дерева (Spanning-Tree Algorithm) — алгоритм, используемый протоколом охватывающего дерева для порождения охватывающего дерева. Иногда используется сокращение *STA*.

Анализатор протоколов (Protocol Analyzer) — См. *сетевой анализатор*. **Аппаратный адрес (Hardware Address)** — См. *MAC-адрес*.

Арендная линия (Leased Line) — линия передачи, резервируемая оператором связи для

частного использования заказчиком. Арендуемая линия представляет собой разновидность выделенной линии.

Асинхронная передача (Asynchronous Transmission) — цифровые сигналы, передаваемые без жесткого тактирования. Такие сигналы в общем случае имеют различные частотные и фазовые отношения. При асинхронной передаче отдельные символы обычно заключаются между битами управления (так называемыми стартовыми и стоповыми битами), которые обозначают начало и конец каждого символа. Сравните с *синхронной передачей*.

Аттенюация (Attenuation) — потеря энергии сигналом при распространении в среде передачи данных.

Аутентификация (Authentication) — в средствах защиты функция проверки подлинности физического лица или процесса.

Балансировка нагрузки (Load Balancing) — в маршрутизации способность маршрутизатора распределять трафик по всем своим сетевым портам, которые находятся на одинаковом расстоянии от адреса пункта назначения. Хорошие алгоритмы балансировки нагрузки используют информацию как о быстродействии, так и о надежности. Балансировка нагрузки увеличивает используемость сегментов сети, тем самым увеличивая эффективную полосу пропускания сети в целом.

Без установления соединения (Connectionless) — передача данных без существования виртуального канала. Сравните с термином *с установлением соединения*. См. также *виртуальный канал*.

Блок многостанционного доступа — См. *MSAU*.

Брандмауэр (Firewall) — устройство, которое управляет доступом в частную сеть и само обладает иммунитетом к проникновению.

В

Виртуальный канал (Virtual Circuit) — логический канал, создаваемый для обеспечения надежной связи между двумя сетевыми устройствами. Виртуальный канал идентифицируется парой чисел VPI/VCI (VPI — идентификатор виртуального пути; VCI — идентификатор виртуального канала) и может быть либо постоянным (PVC), либо коммутируемым (SVC). Виртуальные каналы используются в технологиях Frame Relay и X.25. Иногда используется аббревиатура *VC*.

Время соединения по вызову (Call Setup Time) — время, необходимое для установления соединения по звонку между DTE-устройствами.

Вторичная станция (Secondary Station) — в таких канальных протоколах синхронной побитовой передачи данных, как HDLC, станция, которая отвечает на команды первичной станции. Иногда ее называют просто *вторичной*.

Выдержка (backoff) — принудительная задержка повторной передачи в случае возникновения конфликта.

Выход за временные пределы ожидания (Timeout) — событие, которое имеет место в том случае, когда одно сетевое устройство ожидает услышать другое сетевое устройство в течение заданного периода времени, но не слышит его. В результате это обычно приводит к повторной передаче данных или прекращению сеанса между двумя устройствами.

Г

Гарантированная скорость передачи (Insured Rate) — долгосрочная пропускная способность, измеряемая в битах или ячейках в секунду, которую обеспечивает АТМ-сеть при нормальных рабочих условиях. Эта гарантированная скорость, или полоса пропускания, выделяется пользователям: вся ее величина вычитается из общей полосы пропускания магистрали по пути следования канала. Сравните с *избыточной скоростью передачи и максимальной скоростью передачи*.

Гбит (Gb) — гигабит. Приблизительно 1 000 000 000 бит. **Гбит/с (Gbps)** — гигабит в секунду.

Гибридная сеть (Hybrid Network) — комплекс сетей, использующих несколько технологий, включая технологии локальных и глобальных сетей.

Горизонтальные кросс-соединения (Horizontal Cross-Connect) — коммутационный шкаф, в котором горизонтальная кабельная система подключается к коммутационной панели, которая, в свою очередь, подключена к магистральному каналу, обеспечивающему связь с основными средствами распространения информации.

Д

Данные (Data) — данные протокола верхнего уровня.

Двоичная система (Binary) — система счисления, характеризующаяся наличием только единиц и нулей (1 — вкл., 0 — выкл.).

Двойное кольцо с противоположным направлением распространения информации (Dual Counter-Rotating Ring) — топология сети, при которой сеть с передачей маркера имеет два пути распространения сигналов, причем направления распространения в них противоположны друг другу. На этой концепции основаны технологии FDDI и CDDI.

Двухточечное соединение (Point-To-Point Connection) — один из двух основных типов соединений. В технологии АТМ двухточечное соединение может быть одно- и двунаправленным соединением между двумя оконечными системами. Сравните с *соединением "один ко многим"*.

Дейтаграмма (datagram) — логическая группа информации, посылаемая по среде передачи данных в виде блока сетевого уровня без предварительного установления виртуального канала. В сети Internet основными информационными единицами являются IP-дейтаграммы. Для описания логических групп информации на различных уровнях эталонной модели OSI используются также термины *ячейка, кадр, сообщение, пакет и сегмент*.

Демаркационная точка (Demarc) — демаркационная точка между оборудованием оператора связи и оборудованием, устанавливаемым у заказчика.

Демультимплексирование (Demultiplexing) — разделение нескольких входных потоков, которые были мультимплексированы в общий физический сигнал, на несколько выходных потоков. См. также *мультимплексирование*.

Десятичное представление с разделением точками (Dotted-Decimal Notation) — принятое представление IP-адресов в формате a.b.c.d, где каждое число представляет в десятичной форме 1 байт 4-байтового IP-адреса. Также называют представлением с разделением точками или четырехэлементным представлением с разделением точками.

Динамическая маршрутизация (Dynamic Routing) — маршрутизация, которая автоматически адаптируется к изменениям топологии или трафика сети. Также называется *адаптивной*

маршрутизацией. Требуется, чтобы маршрутизаторы исполняли протокол маршрутизации.

Домен конфликта (Collision Domain) — в сетях Ethernet область сети, внутри которой распространяются претерпевшие столкновение кадры. Повторители и концентраторы пропускают конфликтующие пакеты; коммутаторы локальных сетей, мосты и маршрутизаторы — нет. См. также *конфликт*.

Домен широковещания (Broadcast Domain) — множество всех устройств, которые будут принимать широковещательные кадры, источником которых является устройство, принадлежащее этому множеству. Обычно домены широковещания ограничиваются маршрутизаторами (или в коммутируемых сетях — виртуальными локальными сетями), поскольку маршрутизаторы не перенаправляют широковещательные кадры.

Древовидная топология (Tree Topology) — топология локальной сети, подобная шинной топологии, но отличающаяся тем, что может содержать ответвления с несколькими узлами. Передаваемые станцией сообщения распространяются по всей длине среды передачи данных и принимаются всеми другими станциями. Сравните с *шинной, кольцевой топологией и топологией "звезда"*.

З

Заголовок (Header) — управляющая информация, помещаемая перед данными в процессе их инкапсуляции для передачи по сети. Сравните с термином *хвостовая часть*.

Задержка очереди (Queuing Delay) — продолжительность времени, которое данные должны ожидать перед отправкой в статистически мультиплексируемый физический канал.

Запрессовочное приспособление (Punch Tool) — пружинный инструмент, используемый для обрезки и подсоединения проводов к кабельному разъему или на коммутационной панели.

Запрос на комментарий — См. *RFC*.

Защищенное программное обеспечение (Firmware) — постоянным или полупостоянным образом записанные в ПЗУ программные команды.

Зона (Zone) — логическая группа сетевых устройств в сетях AppleTalk. **Зонный групповой адрес (Zone Multicast Address)** — многопунктовый зависимый от канального протокола адрес, по которому узел принимает широковещательные NBP-пакеты, направленные в его зону.

И

Избыточная скорость передачи (Excess Rate) — трафик, превышающий гарантированную полосу пропускания для данного соединения. В частности, избыточная скорость передачи равна максимальной скорости передачи минус гарантированная скорость передачи. Избыточный трафик доставляется только в том случае, когда имеются соответствующие ресурсы, и может быть отброшен во время периодов перегрузки. Сравните с *гарантированной и максимальной скоростью передачи*.

Инкапсуляция (Encapsulation) — погружение данных в заголовок конкретного протокола. Например, данные верхних уровней погружаются в заголовок протокола Ethernet перед их передачей в сеть. Аналогично, при мостовом объединении несхожих сетей весь кадр одной сети может быть целиком помещен в заголовок, используемый протоколом канального уровня другой сети. См. также *туннелирование*.

Интервал подтвержденного активного состояния (Keepalive Interval) — период времени между каждым сообщением, подтверждающим активность ("keep alive" message), посылаемым сетевым устройством.

Интерфейс (Interface) — 1. Соединение между двумя системами или устройствами. 2. В терминологии маршрутизации — это место подключения сети к маршрутизатору. 3. В телефонии — взаимная граница, определяемая общими физическими характеристиками межсоединения, общими характеристиками сигналов и смысловыми значениями сигналов, обмен которыми осуществляется на этой границе. 4. Граница между соседними уровнями эталонной модели OSI.

Исходный маршрутизатор (Seed Router) — маршрутизатор в сети AppleTalk, в котором номер сети или кабельный диапазон встроены в дескриптор его порта. Исходный маршрутизатор задает номер сети или кабельный диапазон для других маршрутизаторов, находящихся в этом сегменте сети, и отвечает на запросы о конфигурации от неосновных маршрутизаторов из состава подключенной к нему сети AppleTalk, позволяя им подтвердить или соответствующим образом модифицировать свою конфигурацию. Каждая сеть AppleTalk должна иметь по крайней мере один исходный маршрутизатор.

К

Кабельная система категории 1 (Category 1 Cabling) — одна из пяти градаций кабельных систем на основе кабелей UTP (неэкранированная витая пара), описанных в стандарте EIA/TIA 568B. Кабельная система категории 1 используется для телефонной связи и непригодна для передачи данных. Сравните с *кабельной системой категорий 2, 3, 4 и 5*. См. также *UTP*.

Кабельная система категории 2 (Category 2 Cabling) — одна из пяти градаций кабельных систем на основе кабелей UTP ("неэкранированная витая пара"), описанных в стандарте EIA/TIA 568B. Кабельная система категории 2 пригодна для передачи данных со скоростями до 4 Мбит/с. Сравните с *кабельной системой категорий 1, 3, 4 и 5*. См. также *UTP*.

Кабельная система категории 3 (Category 3 Cabling) — одна из пяти градаций кабельных систем на основе кабелей UTP ("неэкранированная витая пара"), описанных в стандарте EIA/TIA 568B. Кабельная система категории 3 используется в сетях IOBaseT и может передавать данные со скоростями до 10 Мбит/с. Сравните с *кабельной системой категорий 1, 2, 4 и 5*. См. также *UTP*.

Кабельная система категории 4 (Category 4 Cabling) — одна из пяти градаций кабельных систем на основе кабелей UTP ("неэкранированная витая пара"), описанных в стандарте EIA/TIA 568B. Кабельная система категории 4 используется в сетях Token Ring и может передавать данные со скоростями до 16 Мбит/с. Сравните с *кабельной системой категорий 1, 2, 3 и 5*. См. также *UTP*.

Кабельная система категории 5 (Category 5 Cabling) — одна из пяти градаций кабельных систем на основе кабелей UTP ("неэкранированная витая пара"), описанных в стандарте EIA/TIA 568B. Кабельная система категории 5 используется в технологии CDDI и может передавать данные со скоростями до 100 Мбит/с. Сравните с *кабельной системой категорий 1, 2, 3 и 4*. См. также *UTP*.

Кабельный диапазон (Cable Range) — диапазон номеров сетей, который может использоваться узлами расширенной сети AppleTalk. Значением кабельного диапазона может быть единственный номер сети или непрерывная последовательность из нескольких номеров сетей. Адреса узлов назначаются на основе значения кабельного диапазона.

Кадр (Frame) — логически сгруппированная информация, посылаемая в виде блока канального уровня в среду передачи данных. Часто под этим термином понимают заголовок и хвостовую часть, используемые для синхронизации и контроля ошибок, которые окружают

пользовательские данные, содержащиеся в блоке. Для описания логических групп информации на различных уровнях эталонной модели OSI используются также термины *ячейка*, *дейтаграмма*, *сообщение*, *пакет* и *сегмент*.

Канал (Circuit) — путь прохождения связи между двумя или более точками.

Канал (link) — сетевой коммуникационный канал, включающий цепь или путь передачи и все соответствующее оборудование между отправителем и получателем. Наиболее часто используется для обозначения соединения в глобальной сети. Иногда называют *линией* или *каналом передачи*.

Канальная группа (Circuit Group) — группа связанных последовательных линий, которые связывают два моста. Если одна из последовательных линий, принадлежащих канальной группе, лежит на охватывающем дереве сети, то тогда любая последовательная связь из этой канальной группы может быть использована для балансировки нагрузки. Подобная стратегия балансировки нагрузки исключает возникновение проблем с упорядочением данных благодаря тому, что каждый адрес пункта назначения приписывается к конкретной последовательной связи. **Канальный адрес (Link-Layer Address)** — См. *MAC-адрес*.

Канальный уровень (Data Link Layer) — уровень 2 эталонной модели OSI. Обеспечивает транзит данных по физической линии. Канальный уровень имеет дело с физической адресацией, топологией сети, дисциплиной в канале, извещениями об ошибках, упорядочением доставки кадров и с управлением потоком данных. IEEE делит его на два подуровня: MAC и LLC-подуровень. Иногда его называют *уровнем связи*. Приблизительно соответствует уровню управления каналом модели SNA.

Карта маршрутов (Route Map) — метод управления перераспределением маршрутов между доменами маршрутизации.

Карта нарезки (Cut Sheet) — схема, показывающая, где размещаются отрезки кабелей, и номера соответствующих комнат, куда они ведут.

Кбайт (kB) — килобайт. Приблизительно 1 000 байт.

Кбайт/с (kBps) — килобайт в секунду.

Кбит (kb) — килобит. Приблизительно 1 000 бит.

Кбит/с (kbps) — килобит в секунду.

Квитирование (Handshaking) — последовательность сообщений, которыми обмениваются два или более сетевых устройства для синхронизации передачи перед посылкой пользовательских данных.

Клиент (Client) — узел или программное обеспечение (входного по отношению к системе устройства), которые запрашивают услугу у сервера.

Клиент-серверная модель (Client/Server Model) — обобщенный способ описания сетевых служб и модели пользовательских процессов (программ) таких служб. Примерами могут служить парадигма сервера имен/преобразования имен службы DNS и отношения "файл—сервер/файл—клиент", реализуемые в сетевой файловой системе NFS и в | бездисковых машинах.

Клиент-серверные вычисления (Client/Server Computing) — сетевые системы с распределенными вычислениями (обработкой), в которых ответственность за совершение транзакции делится на две части: между клиентом (входная часть) и сервером (внутренняя часть). Оба термина (*клиент* и *сервер*) применимы как для программного обеспечения, так и для устройств, фактически выполняющих вычисления. Также называются *распределенными вычислениями (обработкой)*. Сравните с *одноранговыми вычислениями*.

Коаксиальный кабель (Coaxial Cable) — кабель, состоящий из полого внешнего цилиндрического проводника, который окружает единственный внутренний проводник в виде провода. В настоящее время в локальных сетях применяются два типа коаксиальных кабелей: 50-омный кабель, который используется для передачи цифровых сигналов, и 75-омный кабель, который

используется для передачи аналоговых сигналов и высокоскоростной передачи цифровых сигналов.

Кодирование (Coding) — электрическая методика, используемая для транспортирования двоичных сигналов.

Кодирование (Encoding) — процесс представления битов напряжением. **Количество переходов (Hop Count)** — метрика маршрутизации, используемая для измерения расстояния между источником и пунктом назначения. В частности, протокол RIP использует количество переходов в качестве своей единственной метрики. См. также *переход*; *RIP*.

Кольцевая топология (Ring Topology) — топология сети, которая состоит из ряда повторителей, соединенных друг с другом однонаправленными каналами передачи данных так, что они образуют единую замкнутую петлю. Каждая станция сети соединяется с сетью через повторитель. Хотя логически такая топология представляет собой кольцо, физически наиболее часто она является звездой с замкнутой петлей. Сравните с *шинной*, *звездообразной* и *древовидной топологиями*.

Кольцо (Ring) — соединение двух и более станций в логически круговую топологию, в которой информация передается последовательно между активными станциями. На этой топологии основаны сети Token Ring, FDDI и CDDI.

Коммутационная панель (Patch Panel) — сборка из контактных наборов и портов, которая может устанавливаться в стойке или крепиться на стенке коммутационного шкафа с помощью установочных скоб. Коммутационные панели выступают в роли коммутатора, который соединяет кабели от рабочих станций друг с другом и с внешним миром.

Коммутируемая линия (Dialup Line) — канал связи, который формируется соединением коммутируемых каналов сети телефонной компании.

Конкуренция (Contention) — метод доступа, при котором сетевые устройства соревнуются за получение разрешения на доступ к физической среде. Сравните с термином *передача маркера*.

Консоль (Console) — DTE-устройство, через которое команды вводятся в хост-машину.

Конфликт (Collision) — в сетях Ethernet результат одновременной передачи двух узлов. Кадры от каждого устройства сталкиваются и повреждаются, встречаясь в физической среде. См. также *домен конфликта*.

Концентратор (Concentrator) — См. *хаб (hub)*.

Кэширование (Caching) — форма реплицирования, при которой информация, полученная во время выполнения предыдущей транзакции, используется при обработке последующих транзакций.

Л

Локальная линия связи (Local Loop) — линия связи от помещения телефонного абонента до центрального офиса телефонной компании.

Локальная сеть (Local-Area Network) — См. *LAN*.

Локальный оптоволоконный канал типа 4B/5B (4B/5B local fiber) — локальный оптоволоконный канал связи с форматом кадра 4/5 байт. Оптоволоконная физическая среда, используемая в технологиях FDDI и ATM. Поддерживает скорость передачи данных до 100 Мбит/с по многомодовому оптоволокну.

Локальный оптоволоконный канал типа 8B/10B (8B/10B local fiber) — локальный оптоволоконный канал связи с форматом кадра 8/10 байтов. Оптоволоконная физическая среда,

поддерживающая скорость передачи данных до 149,76 Мбит/с по многомодовому оптоволокну.

М

Магистральная кабельная система (Backbone Cabling) — кабельная система, обеспечивающая соединение между помещениями для коммутационного оборудования и точками входа в телефонную сеть и между зданиями, объединенными в одной локальной сети.

Магистральный канал (Backbone) — часть сети, которая является главным путем для трафика, источником и пунктом назначения которого часто являются другие сети.

Максимальная скорость передачи (Maximum Rate) — максимальная общая пропускная способность по данным, допустимая на заданном виртуальном канале и равная сумме гарантированного и негарантированного трафика от источника. Негарантированные данные могут быть отброшены в случае перегрузки сети. Максимальная скорость передачи, которая не может превышать скорость передачи данных среды, отражает наибольшую пропускную способность виртуального канала по данным, которую тот способен достичь, и измеряется в битах или ячейках в секунду. Сравните с *избыточной скоростью передачи* и *гарантированной скоростью передачи*.

Маркер (Token) — кадр, который содержит информацию управления. Обладание маркером позволяет сетевому устройству передавать данные в сеть.

Маркерная шина (Token Bus) — архитектура локальной сети, использующая в шинной топологии метод передачи маркера. Такая архитектура является основой спецификации локальных сетей IEEE 802.4.

Маршрут по умолчанию (Default Route) — запись в таблице маршрутизации, используемая для перенаправления пакетов, для которых в этой таблице маршрутизации отсутствует явное указание следующего перехода.

Маршрутизатор (Router) — устройство, работающее на сетевом уровне модели OSI, которое использует одну или несколько метрик для определения оптимального пути, по которому должен быть направлен сетевой трафик. Маршрутизаторы переадресовывают пакеты из одной сети в другую, основываясь на информации сетевого уровня, содержащейся в пакетах обновления маршрутной информации. Иногда их называют *шлюзами* (хотя этот термин выходит из употребления).

Маршрутизация (Routing) — процесс нахождения пути до хост-машины пункта назначения. Из-за большого количества потенциальных промежуточных пунктов назначения, по которым должен пройти пакет прежде, чем достигнет хост-машину-получатель, маршрутизация в крупных сетях представляет собой весьма сложную операцию.

Маршрутизация вызовов по запросу — См. *DDR*.

Маршрутизация по кратчайшему пути (Shortest Path Routing) — маршрутизация, которая с помощью специального алгоритма минимизирует расстояние или стоимость пути. **Маршрутизируемый протокол (Routed Protocol)** — протокол, который может маршрутизироваться маршрутизатором. Последний должен уметь интерпретировать логическое объединение сетей в соответствии с тем, как это задает маршрутизируемый протокол. Примерами маршрутизируемых протоколов являются протоколы AppleTalk, DECnet и IP.

Маска (Mask) — См. *маска адреса* и *маска подсети*.

Маска адреса (Address Mask) — комбинация битов, используемая для описания того, какая часть адреса относится к сети или подсети, а какая — к хост-машине. Иногда ее называют просто маской.

Маска подсети (Subnet Mask) — 32-разрядная маска адреса, применяемая в системе IP-адресации для того, чтобы указать разряды IP-адреса, которые используются в качестве адреса подсети. Иногда называют просто *маской*. **Мбайт (MB)** — мегабайт. Приблизительно — 1 000 000 байт. **Мбит (Mb)** — мегабит. Приблизительно — 1 000 000 бит.

Межоперабельность (Interoperability) — возможность вычислительного оборудования, изготовленного различными производителями, успешно взаимодействовать друг с другом по сети.

Межсетевой искатель пакетов (Packet Internet Groper) — См. *ping*.

Метод двойного присутствия (Dual Homing) — топология сети, в соответствии с которой устройство подключается к сети через две независимые точки доступа (точки подключения). Одна точка доступа представляет собой основное соединение, а вторая является резервным соединением, которое активизируется в случае отказа основного.

Метод доступа (Access Method) — 1. В общем случае способ, посредством которого сетевое устройство обращается к сетевой среде. 2. Программное обеспечение SNA-процессора, которое управляет потоком информации в сети.

Метрика (Metric) — См. *метрика маршрутизации*.

Метрика маршрутизации (Routing Metric) — метод, с помощью которого алгоритм маршрутизации определяет, что один маршрут лучше другого. Эта информация хранится в таблицах маршрутизации и пересылается в пакетах обновления маршрутных данных. Метрики могут включать полосу пропускания, стоимость связи, величину задержки, количество переходов, нагрузку, максимальный размер блока передачи, стоимость пути и надежность. Иногда ее называют просто *метрикой*.

Многоадресный пакет (Multicast) — пакет, копируемый сетью и посылаемый в заданное подмножество сетевых адресов. Эти адреса определяются в поле адреса пункта назначения "Destination Address". Сравните с *широковещательным пакетом* и *одноадресным пакетом*.

Многомодовое оптоволокно (Multimode Fiber) — оптическое волокно, поддерживающее распространение световых волн с разной частотой.

Многоточковый адрес (Multicast Address) — адрес, который соответствует нескольким сетевым устройствам. Синоним группового адреса. Сравните с *широковещательным адресом* и *одноточковым адресом*.

Многосетевой комплекс (Internetwork) — группа сетей, соединенных с помощью маршрутизаторов и других устройств, которая работает (в общем случае) как одна сеть.

Модем (Modem) — модулятор-демодулятор. Устройство, которое преобразовывает цифровые и аналоговые сигналы. На стороне источника данных модем преобразовывает цифровые сигналы в форму, подходящую для передачи с помощью средств аналоговой связи. В пункте назначения аналоговые сигналы преобразуются в цифровые. Модемы позволяют передавать данные по телефонным линиям голосовой связи.

Мост (Bridge) — устройство, соединяющее и передающее пакеты между двумя сетевыми сегментами, в которых используется один и тот же коммуникационный протокол. Мосты работают на канальном уровне (уровне 2) эталонной модели OSI. В общем случае мост фильтрует, переадресовывает или лавинно размножает входной кадр на основе MAC-адреса, содержащегося в этом кадре.

Мультиплексирование (Multiplexing) — схема, позволяющая одновременно передавать по одному физическому каналу несколько логических сигналов. Сравните с *демультиплексированием*.

Н

Назначенный маршрутизатор (Designated Router) — OSPF-маршрутизатор, который генерирует LSA-пакеты для сетей с множественным доступом и выполняет другие специальные функции в протоколе OSPF. Каждая OSPF-сеть с множественным доступом, в которой по крайней мере два подключенных маршрутизатора, имеет назначенный маршрутизатор, который выбирается OSPF-протоколом приветствий "Hello". Назначенный маршрутизатор уменьшает количество отношений соседств, требующихся в сетях с множественным доступом, что, в свою очередь, снижает объем трафика маршрутного протокола и размер топологической базы данных.

Начальная загрузка (Bootstrap) — простая заранее определенная операция загрузки команд, которые, в свою очередь, загружают в память другие команды или вызывают переход в другие режимы конфигурирования.

Неосновной маршрутизатор (Nonseed Router) — маршрутизатор в сетях AppleTalk, который должен перед началом функционирования сначала получить и проверить свою конфигурацию через так называемый исходный маршрутизатор. См. также *исходный маршрутизатор*.

Нерасширенная сеть (Nonextended Network) — сеть с адресацией по методу AppleTalk Phase 2, которая поддерживает адресацию до 253 узлов и только одну зону.

Несущая (Carrier) — электромагнитная волна или переменный ток одной частоты, пригодные для модулирования другим сигналом, несущим данные.

Номер сети (Network Number) — часть IP-адреса, задающая сеть, к которой принадлежит хост-машина.

Номер сокета (Socket Number) — 8-разрядный номер, идентифицирующий сокет. В AppleTalk-узле может назначаться максимально 254 номера сокета.

Номер хост-машины (Host Number) — часть IP-адреса, которая определяет, какой узел подсети адресуется. Также называют *адресом хост-машины*.

O

Область (Area) — логическое множество сетевых сегментов (на основе протоколов CLNS, DECnet и OSPF) и включенных в них устройств. Области обычно соединяются с другими областями через маршрутизаторы, образуя автономную систему. Обратная сборка (Reassembly) — сборка в единое целое IP-дейтаграммы, после того, как она была фрагментирована либо отправителем, либо промежуточным узлом.

Обучение MAC-адресам (MAC Address Learning) — служба, являющаяся характерной для обучающихся коммутаторов, когда MAC-адрес источника каждого принимаемого пакета запоминается, так что будущие пакеты, предназначенные для этого адреса, могут переадресовываться только на тот интерфейс коммутатора, на котором находится этот адрес. Пакеты, имеющие пунктом назначения неопознанный широковещательный или многоадресный адрес, переадресовываются всеми интерфейсами коммутатора, исключая тот, на который они поступили. Такая схема помогает минимизировать трафик в подсоединенных локальных сетях. Процесс обучения MAC-адресам описан в стандарте IEEE 802.1.

Объединение в сеть (Networking) — соединение рабочих станций и периферийного оборудования, например принтеров, накопителей на жестких дисках, накопителей на компакт-дисках (CD-ROM) и др.

Одноадресный пакет (unicast) — сообщение, посылаемое в один пункт назначения в сети. Сравните с *широковещательным пакетом* и *многоадресным пакетом*.

Однопунктовый адрес (Unicast Address) — адрес, задающий одно сетевое устройство. Сравните с *широковещательным* и *многопунктовым* адресом.

Одноранговые вычисления (Peer-To-Peer Computing) — такая организация сети, когда на каждом

узле сети выполняется как клиентская, так и серверная часть приложения. Этот термин также обозначает обмен данными между реализациями одного и того же уровня эталонной модели OSI в двух различных сетевых устройствах. Сравните с *клиент-серверными вычислениями*.

ОЗУ (RAM) — оперативное запоминающее устройство. Энергозависимая память, которая допускает запись и считывание информации.

Октет (Octet) — 8 двоичных разрядов (бит). Часто используется именно термин *октет* (а не *байт*), поскольку в некоторых архитектурах машин работа осуществляется с байтами, длина которых не равна 8 битам.

Оперативное запоминающее устройство (Random Access Memory) — См. *ОЗУ*.

Оператор связи (Common Carrier) — частная коммунальная компания, имеющая лицензию на предоставление коммуникационных услуг населению по установленной цене.

Оповещение (Advertising) — процесс в маршрутизаторе, который отправляет пакеты обновления маршрутной информации или список доступных служб, чтобы другие маршрутизаторы в сети имели списки пригодных для использования маршрутов.

Опорная сигнальная земля (Signal Reference Ground) — опорная точка, используемая вычислительными устройствами для измерения и сравнения относительно нее входных цифровых сигналов.

Опволоконный кабель (Fiber-Optic Cable) — физическая среда, способная проводить модулированное световое излучение. По сравнению с другими средами передачи данных опволоконный кабель значительно дороже, но нечувствителен к электромагнитным помехам. Иногда его называют *оптическим волокном*.

Организация межсетевого взаимодействия (internetworking) — отрасль, занимающаяся вопросами соединения сетей. Термин может относиться к изделиям, процедурам и технологиям.

ОС IOS компании Cisco (Cisco Internetwork Operating System) — межсетевая операционная система компании Cisco. Системное программное обеспечение разработки компании Cisco, которое обеспечивает общие функциональные возможности, масштабируемость и средства защиты информации для всех продуктов с архитектурой CiscoFusion. ОС IOS осуществляет централизованную, интегрированную и автоматизированную установку и управляет сетевыми комплексами, одновременно обеспечивая поддержку широкого набора протоколов, типов сред, служб и платформ.

Очередь (Queue) — 1. Упорядоченный список элементов, ожидающих обработки. 2. В маршрутизации — накопленные пакеты, ожидающие своей переадресации через интерфейс маршрутизатора.

П

Пакет (Packet) — логически сгруппированная информация, которая включает заголовок, содержащий управленческую информацию, и (обычно) данные пользователя. Наиболее часто термин *пакет* используется для обозначения блока данных сетевого уровня модели OSI. Для описания логических групп информации на различных уровнях эталонной модели OSI используются также термины *дейтаграмма*, *кадр*, *сообщение* и *сегмент*.

Пакет мгновенного обновления (Flash Update) — пакет обновления маршрутной информации, посылаемый асинхронным образом в ответ на изменения топологии сети. Сравните с термином *пакет обновления маршрутной информации*.

Пакет обновления маршрутной информации (Routing Update) — сообщение, посылаемое маршрутизатором и показывающее достижимость сети и соответствующую стоимостную информацию. Обычно пакеты обновления маршрутной информации посылаются через

регулярные промежутки времени и после изменения топологии сети. Сравните с *пакетом мгновенного обновления*.

Пакет обратного исправления (Poison Reverse Update) — пакет обновления маршрутной информации, в котором явно указывается, что сеть или подсеть недостижима, а не говорится об этом в неявном виде путем невключения ее в обновленную информацию. Пакеты-"противоядия" посылаются с целью разрушения больших петель маршрутизации.

Пакет приветствия (Hello Packet) — многоадресный пакет, который используется маршрутизаторами, выполняющими определенные протоколы маршрутизации, в процессе выявления соседей и при восстановлении после отказа. Пакеты приветствия также показывают, что клиент находится в рабочем состоянии и сеть готова к работе.

Пакеты обновления с расщеплением горизонта (Split-Horizon Updates) — метод маршрутизации, в соответствии с которым не допускается выход информации о маршрутах с тех интерфейсов маршрутизатора, по которым эта информация поступила. Эта методика полезна для предотвращения возникновения петель маршрутизации.

Параллельная передача (Parallel Transmission) — метод передачи данных, в соответствии с которым биты символа данных передаются одновременно по нескольким каналам. Сравните с *последовательной передачей*.

Переадресация (Forwarding) — процесс пересылки кадра в конечный пункт назначения с помощью устройства межсетевого взаимодействия.

Переадресация кадров (Frame Forwarding) — механизм, посредством которого основанный на кадрах трафик, например трафик протоколов HDLC и SDLC, движется в сети ATM.

Перегрузка (Congestion) — трафик, превышающий возможности сети.

Передача маркера (Token Passing) — метод доступа, в соответствии с которым доступ сетевого устройства к физической среде происходит упорядоченным образом на основе обладания небольшим кадром, называемым маркером. Сравните с *коммутацией каналов и конкурентным доступом*.

Перенаправление (Redirect) — часть протоколов ICMP и ES-IS, позволяющая маршрутизатору сообщить хост-машине, что использование другого маршрутизатора будет более эффективным.

Петля (Loop) — маршрут, когда пакеты никогда не достигают своего пункта назначения, а просто ходят по кругу через неизменный набор узлов сети.

ПЗУ (ROM) — постоянное запоминающее устройство. Энергонезависимая память, данные из которой могут считываться микропроцессором, но записываться туда не могут.

Пинг (ping, Packet Internet Groper) — межсетевой искатель пакетов. Эхо-сообщение и ответ на него в рамках протокола ICMP. Часто используется в IP-сетях для проверки достижимости сетевого устройства.

Плата сетевого интерфейса — См. *NIC*.

Повторитель (Repeater) — устройство, которое регенерирует и передает дальше электрические сигналы между двумя сегментами сети.

Подсеть (Subnetwork) — 1. В IP-сетях сеть, которая идентифицируется конкретным подсетевым адресом. Подсети представляют собой сети, произвольным образом сегментированные сетевым администратором

целях обеспечения многоуровневой иерархической структуры маршрутизации с одновременным экранированием подсети от сложностей адресации подсоединенных сетей. 2. В OSI-сетях — группа оконечных и промежуточных систем, управляемых в одном административном домене и использующих один протокол доступа к сети.

Полезная нагрузка (Payload) — часть ячейки, кадра или пакета, которая содержит информацию верхнего уровня (данные).

Полноразмерная сетка (Full Mesh) — сеть, в которой устройства организованы в топологию "сетка", когда каждый узел сети имеет либо физический канал, либо виртуальный канал к каждому узлу сети. Топология полноразмерной сетки обеспечивает высокую степень дублирования, но, так как стоимость ее реализации может быть запредельно высокой, обычно она используется для организации магистральных каналов сети. См. также *сетка; частично полноразмерная сетка*.

Полный дуплекс (Full Duplex) — одновременная передача данных между посылающей и принимающей станциями. Сравните с *полудуплексом* и *симплексом*.

Полоса пропускания (Bandwidth) — разница между наибольшей и наименьшей частотой, с которой могут передаваться сигналы в сети. Также используется для описания номинальной производительности данной сетевой среды или протокола.

Полудуплекс (Half Duplex) — передача данных между посылающей и принимающей станциями в конкретный момент времени только в одном направлении. Сравните с *полным дуплексом* и *симплексом*.

Порт (Port) — 1. Интерфейс устройства межсетевое взаимодействия (например, маршрутизатора). 2. В IP-терминологии — процесс верхнего уровня, который принимает данные от нижних уровней. Порты нумеруются и многие связываются с конкретным процессом. Например, протокол SNMP приписан к порту 25. Номер порта такого типа называется *известным адресом*.

Портирование (Port) — переделка программного обеспечения или микрокода таким образом, чтобы они могли выполняться на другой аппаратной платформе или в другой программной среде, отличной от той, для которой они первоначально разрабатывались.

Последовательная передача данных (Serial transmission) — метод передачи данных, в соответствии с которым биты символов данных последовательно передаются по единственному каналу. Сравните с *параллельной передачей данных*.

Посредник (Proxy) — объект, который в интересах эффективности выдает себя за другой объект.

Постановка в очередь по приоритету (Priority Queuing) — функция маршрутизации, когда кадры в выходной очереди интерфейса ранжируются в зависимости от различных характеристик, например протокола, размера пакета и типа интерфейса.

Постоянный виртуальный канал — См. *PVC*.

Посылка служебных сигналов с помощью A&B-битов (A&B Bit Signalling) — процедура, используемая в передающей аппаратуре канала связи T1, когда в каждом из 24 подканалов канала T1 один бит каждого шестого кадра выделяется для передачи сигналов управляющей информации супервизора.

Поток (Flow) — поток данных между двумя конечными точками сети (например, от одной сетевой станции к другой). По одному каналу могут передаваться одновременно несколько потоков.

ППЗУ (PROM) — программируемое постоянное запоминающее устройство. ПЗУ, которое может быть запрограммировано с помощью специального оборудования. ППЗУ могут

программироваться только один раз. Сравните с *СППЗУ*.

Предотвращение перегрузки (Congestion Avoidance) — механизм, с помощью которого АТМ-сеть управляет поступающим в сеть трафиком с целью минимизации задержек. Для более эффективного использования ресурсов низкоприоритетный трафик отбрасывается на границе сети, если сложившиеся условия указывают на невозможность его доставки.

Преобразование адреса (Address Resolutions) — в общем случае это метод устранения различий в схемах адресации компьютеров. Преобразование адреса обычно определяет метод отображения адресов сетевого уровня (уровня 3) на адреса канального уровня (уровня 2).

Преобразование имени (Name Resolution) — это процесс связывания имени с сетевым адресом.

Приложение (Application) — программа, которая выполняет функцию непосредственно для пользователя. Примерами сетевых приложений являются клиентские части протоколов FTP и Telnet.

Пропускная способность (Throughput) — скорость поступления или, возможно, прохождения информации через определенную точку сетевой системы. **Простая адресация (Flat Addressing)** — схема адресации, в которой для определения местоположения не используется логическая иерархия.

Протокол (Protocol) — формальное описание набора правил и договоренностей о том, как устройства в сети обмениваются информацией.

Протокол ARP с посредником (Proxy ARP) — вариант протокола ARP, в котором промежуточное устройство (например, маршрутизатор) посылает запрашивающей хост-машине ARP-ответ от имени конечного узла. Этот протокол может снижать уровень использования полосы пропускания в медленных каналах глобальных сетей.

Протокол Internet (Internet Protocol) — любой из протоколов, принадлежащих группе протоколов TCP/IP. См. *IP*; *TCP/IP*.

Протокол маршрутизации (Routing Protocol) — протокол, который выполняет маршрутизацию посредством реализации конкретного алгоритма маршрутизации. Примерами протоколов маршрутизации являются IGRP, OSPF и RIP.

Протокол распределенного связующего дерева (Spanning-Tree Protocol) — мостовой протокол, который использует алгоритм охватывающего дерева, позволяющий обучающемуся коммутатору динамически обходить петли в топологии коммутируемой сети путем порождения охватывающего дерева. Обмениваясь BPDU-сообщениями с другими мостами, коммутаторы обнаруживают петли и затем удаляют их, отключая определенные интерфейсы. Если основной канал отказывает, тогда активизируется резервная связь. Этим термином называют как стандарт протокола охватывающего дерева IEEE 802.1, так и более ранний протокол охватывающего дерева компании Digital Equipment Corporation, на котором он основан. Версия IEEE поддерживает домены коммутаторов и позволяет коммутатору создавать свободную от петель топологию в расширенной локальной сети. Обычно версия IEEE предпочтительнее версии компании Digital.

Протокольный адрес (Protocol Address) — См. *сетевой адрес*.

Проходная область (Non-Stub Area) — OSPF-область с большим количеством ресурсов, которая может содержать маршрут по умолчанию, статические и внутренние маршруты, маршруты между областями и внешние маршруты. Проходные области являются единственными из OSPF-областей, которые могут иметь сконфигурированные через них виртуальные каналы и содержать ASBR. Сравните с *тупиковой областью*. См. также *ASBR*.

Р

Размер окна (Window Size) — количество сообщений, которое может быть передано в процессе ожидания подтверждения.

Резервирование полосы пропускания (Bandwidth Reservation) — процесс назначения полосы пропускания для пользователей и приложений, обслуживаемых сетью. Он связан с назначением приоритета различным трафикам на основе их важности и чувствительности к задержкам. Этот процесс позволяет наилучшим образом использовать имеющуюся полосу пропускания, и если сеть становится перегруженной, то трафик с более низким приоритетом отбрасывается. Иногда этот процесс называют *выделением полосы пропускания*.

Резервное дублирование (Redundancy) — 1. При организации межсетевого взаимодействия дублирование устройств, служб или соединений, чтобы в случае отказа резервные устройства службы или соединения могли выполнять работу отказавших. 2. В телефонии — часть общей информации, содержащейся в сообщении, которая может быть опущена без потери важной информации или смысла.

С

С установлением соединения (Connection-Oriented) — передача данных, которая требует формирования виртуального канала. См. также *без установления соединения*, *виртуальный канал*.

Сведение маршрутов (Route Summarization) — консолидация объявляемых номеров сетей в протоколах OSPF и IS-IS. В протоколе OSPF это приводит к тому, что пограничный маршрутизатор области объявляет другим областям только один сводный маршрут.

Связанная группа протоколов (Protocol Stack) — набор связанных коммуникационных протоколов, которые работают вместе и обеспечивают взаимодействие на нескольких или всех уровнях эталонной модели OSI. Не каждая группа протоколов покрывает каждый уровень модели, и часто один протокол из группы работает на нескольких уровнях сразу. Типичным примером связанной группы протоколов является группа TCP/IP.

Связующее дерево (Spanning Tree) — свободное от замкнутых петель топологическое подмножество сети (коммутируемой) на уровне 2 модели OSI.

Сеанс (Session) — 1. Связанный набор коммуникационных транзакций после установления соединения между двумя или более сетевыми устройствами. 2. В архитектурной модели SNA — логическое соединение, позволяющее двум адресуемым сетевым блокам обмениваться информацией.

Сеансовый уровень (Session Layer) — уровень 5 эталонной модели OSI. Устанавливает, поддерживает и завершает сеансы между приложениями и управляет обменом данными между объектами уровня представлений. Соответствует уровню управления потоком данных модели SNA.

Сегмент (Segment) — 1. Участок сети, ограниченный с обеих сторон мостами, маршрутизаторами или коммутаторами. 2. В локальной сети с шинной топологией — безразрывная электрическая связь, которая часто с помощью повторителей соединяется с другими такими сегментами. 3. В спецификации протокола TCP — это один блок информации транспортного

уровня. Для описания логических групп информации на различных уровнях эталонной модели используются также термины *дейтаграмма*, *кадр*, *сообщение* и *пакет*.

Сервер (Server) — узел или программа, которые предоставляют услуги клиенту.

Сервер имен (Name Server) — включенный в сеть сервер, который ставит в соответствие сетевые имена с сетевыми адресами.

Сетевая операционная система — См. *NOS*.

Сетевой адрес (Network Address) — адрес сетевого уровня модели OSI, который ссылается на логическое, а не физическое сетевое устройство. Также называют *протокольным адресом*. Сравните с *MAC-адресом*.

Сетевой анализатор (Network Analyzer) — аппаратно-программное устройство, обладающее различными функциями для поиска и устранения неисправностей в сетях, включая декодирование пакетов в зависимости от типа протокола, специальные предварительно запрограммированные тесты по выявлению неисправностей, фильтрацию пакетов и их передачу.

Сетевой интерфейс (Network Interface) — граница между сетью оператора связи и установленным оборудованием частного владельца.

Сетевой порядок следования байтов (Network Byte Order) — принятый в сети Internet порядок следования байтов, соответствующих числовым значениям.

Сетевой уровень (Network Layer) — уровень 3 эталонной модели OSI. Обеспечивает возможность связи и выбор пути между двумя оконечными системами. Именно на сетевом уровне выполняется маршрутизация. Приблизительно соответствует уровню управления путями модели SNA. См. также *уровень приложений*, *канальный уровень*, *физический уровень*; *уровень представлений*; *сеансовый уровень*; *транспортный уровень*.

Сетка (Mesh) — топология сети, в соответствии с которой устройства организуются управляемым сегментированным образом со множеством часто дублирующих, взаимных межсоединений, стратегически проложенных между узлами сети. См. также *полноразмерная сетка* и *частично полноразмерная сетка*.

Сеть (Network) — группа компьютеров, принтеров, маршрутизаторов, коммутаторов и других устройств, которые обмениваются информацией друг с другом через какую-либо среду передачи данных.

Сеть от многих поставщиков (Multivendor Network) — сеть, в которой используется оборудование от многих поставщиков. В таких сетях возникает значительно больше проблем, связанных с совместимостью, чем в сетях от одного поставщика. Сравните с *сетью от одного поставщика*.

Сеть от одного поставщика (Single-Vendor Network) — сеть, в которой используется оборудование только от одного поставщика. В таких сетях редко возникают проблемы совместимости. См. также *сеть от многих поставщиков*.

Сигнал подтверждения (Acknowledgment) — извещение, посылаемое одним сетевым устройством другому, о том, что произошло некоторое событие (например, прием сообщения). Иногда сокращенно называется АСК. Сравните с *NAC*.

Симплекс (Simplex) — возможность осуществления передачи между посылающей и принимающей станциями только в одном направлении. Примером симплексной технологии является широковещательное телевидение. Сравните с *полным дуплексом* и *полудуплексом*.

Синхронная передача (Synchronous Transmission) — цифровые сигналы, передаваемые с точным тактированием. Такие сигналы имеют одинаковую частоту, при этом отдельные

символы заключаются между битами управления (называемыми старт-битами и стоп-битами), которые обозначают начало и конец каждого символа. Сравните с *асинхронной передачей*.

Система управления сетью — См. *NMS*.

Соединение "один ко многим" (Point-To-Multipoint Connection) — один из двух основных типов соединений. В технологии ATM соединением "один ко многим" называется такое соединение, когда одна оконечная система-отправитель (называемая корневым узлом) однонаправленно соединяется с несколькими оконечными системами-получателями (называемыми листьями). Сравните с *двухточечным соединением*.

Сокет (Socket) — 1. Программная структура, работающая как абонент внутри сетевого устройства (подобно порту). 2. Адресуемый объект узла, подключенного к сети AppleTalk; сокеты находятся в собственности программных процессов, называемых *сокетными клиентами*. AppleTalk-сокеты делятся на две группы: сокеты доступа отправителя (SAS), которые резервируются для таких клиентов, как протоколы ядра группы протоколов AppleTalk, и сокеты доступа в пункте назначения (DAs), которые назначаются динамическим протоколом DDP по запросу клиентов на узле. AppleTalk-сокет концептуально похож на TCP/IP-порт.

Сообщение (Message) — логическая группа информации уровня приложения, часто составленная из ряда логических групп более низких уровней, например пакетов. Для описания логических групп информации на различных уровнях эталонной модели OSI используются также термины *ячейка, дейтаграмма, кадр, пакет и сегмент*.

Сообщение перехвата (Trap) — сообщение, посылаемое SNMP-агентом системе управления сетью на консоль или терминал, указывающее на то, что произошло значительное событие, например выполнилось какое-либо специально определенное условие или было достигнуто пороговое значение какого-либо параметра.

Соответствие адреса (Address Mapping) — методика, которая за счет перевода адресов из одного формата в другой позволяет взаимодействовать различным протоколам. Например, при маршрутизации IP-пакетов по сети X.25 IP-адреса должны быть отображены на адреса протокола X.25, чтобы эти пакеты могли передаваться в сети X.25.

Соседние маршрутизаторы (Neighboring Routers) — в протоколе OSPF два маршрутизатора, которые имеют интерфейсы, подключенные к общей сети. В сетях с множественным доступом соседи динамически выявляются протоколом приветствия OSPF Hello.

Соседство (Adjacency) — отношение, формируемое между отдельными маршрутизаторами и конечными узлами с целью обмена маршрутной информацией. Соседство основывается на использовании общего сегмента среды передачи данных.

Список доступа (Access List) — находящийся в маршрутизаторе список, с помощью которого осуществляется управление доступом ряда служб через маршрутизатор или к нему (например, для того, чтобы не допустить выхода пакетов с определенным IP-адресом через конкретный интерфейс маршрутизатора).

СПЗУ (EPROM) — стираемое программируемое постоянное запоминающее устройство. Микросхемы энергонезависимой памяти, которые программируются после изготовления, и записанная в них информация при необходимости может стираться и перепрограммироваться. Сравните с *ЭСПЗУ и ПЗУ*.

Спуфинг (Spoofing) — 1. Схема, используемая маршрутизаторами, которая заставляет хост-машину рассматривать интерфейс так, словно он активен и поддерживает сеанс. Маршрутизатор имитирует ответы на сообщения сохранения активности от хост-машины, чтобы убедить эту хост-машину в том, что сеанс еще существует. Техника спуфинга полезна в таких средах маршрутизации, как среды с динамической реконфигурацией устройств, в которых

в целях экономии платы за пользование каналом коммутируемый канал закрывается в отсутствие по нему трафика. 2. Действия, связанные с посылкой пакета, нелегально выдающего себя за такой, который имеет адрес отправителя, с которого он фактически никогда не отсылался. Спуфинг был придуман для обхода таких механизмов защиты сети, как фильтры и списки доступа.

Среда (Media) — различные физические среды, в которых движутся передаваемые сигналы. К обычным сетевым средам передачи данных относятся кабели типа "витая пара", коаксиальные и оптоволоконные кабели и атмосфера (в которой осуществляется распространение микроволновых, лазерных или инфракрасных сигналов). Иногда называют *физической средой*.

Стандарт (Standard) — набор правил или процедур, которые либо широко используются, либо определены официально. **Станция двойного подключения** — См. *DAS*.

Станция двойного присутствия (Dual-Homed Station) — устройство, подключаемое к нескольким FDDI-концентраторам, для обеспечения резервного дублирования. **Статический маршрут (Static Route)** — маршрут, который конфигурируется в явном виде и вводится в таблицу маршрутизации по умолчанию. Статические маршруты имеют преимущество по сравнению с маршрутами, которые выбираются протоколами динамической маршрутизации.

Сторожевой пакет (watchdog packet) — метод, используемый для обеспечения контроля за тем, что клиент все еще соединен с NetWare-сервером. Если в течение определенного периода времени сервер не получает пакеты от клиента, то он посылает ему серию сторожевых пакетов. В случае, если станция не отвечает на предварительно задаваемое количество сторожевых пакетов, то сервер делает вывод, что станция больше не подключена, и разрывает с ней соединение.

Сторожевой спуфинг (Watchdog Spoofing) — тип спуфинга, который используется исключительно в маршрутизаторе, работающем специально на клиента NetWare, посылая NetWare-серверу сторожевые пакеты для поддержания активного сеанса между клиентом и сервером. Полезен в тех случаях, когда клиент и сервер разделены каналом глобальной сети с динамической реконфигурацией устройств.

Сторожевой таймер (Watchdog Timer) — 1. Аппаратный или программный механизм, который используется для генерации события или выхода из процесса в том случае, если таймер периодически не переустанавливается. 2. В ОС Netware — таймер, который показывает максимальный период времени, в течение которого сервер будет ожидать ответ от клиента на сторожевой пакет. Если время таймера истекает, то сервер посылает другой сторожевой пакет (и так до установленного максимума).

Сходимость (Convergence) — скорость и способность группы устройств межсетевого взаимодействия выполнять специальный алгоритм маршрутизации по согласованию представления о топологии сетевого комплекса после изменения в этой топологии.

Счет до бесконечности (Count To Infinity) — проблема, которая может возникать при работе алгоритмов с медленной сходимостью, когда маршрутизаторы непрерывно увеличивают показания счетчика количества переходов до определенных сетей. Обычно для устранения этой проблемы устанавливается некоторое произвольное предельное значение количества переходов.

T

Таблица маршрутизации (Routing Table) — таблица, хранимая в маршрутизаторе или каком-

нибудь другом устройстве межсетевого взаимодействия, в которой записываются маршруты к конкретным сетям, а в некоторых случаях — метрика таких маршрутов.

Топология (Topology) — физическое взаиморасположение сетевых узлов и среды передачи данных, реализующее сетевую структуру предприятия.

Топология "звезда" (Star Topology) — топология локальной сети, когда оконечные точки сети соединяются с общим центральным коммутатором двухточечными связями.

Кольцевая топология, организованная в виде звезды, реализует "звезду" в виде однонаправленного замкнутого контура, а не с помощью двухточечных связей. Сравните с *шинной*, *кольцевой* и *древовидной* топологиями.

Точка доступа к службам в пункте назначения — См. *DSAP*. Точка доступа к службе (Service Access Point) — См. *SAS*. Трансляция сетевого адреса — См. *NAT*.

Транспортный уровень (Transport Layer) — уровень 4 эталонной модели OSI. Обеспечивает надежный обмен данными по сети между конечными узлами, механизмы установления, поддержания и закрытия виртуальных каналов, обнаружения отказов на транспортном уровне и восстановления после них, а также управление потоком информации. Соответствует уровню управления передачей модели SNA. См. также *уровень приложений*, *канальный уровень*, *сетевой уровень*, *физический уровень*; *уровень представлений*; *сеансовый уровень*.

Туннелирование (Tunneling) — архитектура, разработанная для предоставления услуг, необходимых, чтобы реализовать произвольную стандартную схему инкапсуляции при двухточечной передаче.

Тупиковая область (Stub Area) — OSPF-область, через которую могут проходить маршруты по умолчанию, маршруты, лежащие внутри области, и маршруты между областями. Через тупиковые области не могут конфигурироваться виртуальные каналы, и они не могут содержать пограничные маршрутизаторы автономной системы (ASBR). Сравните с *проходной областью*.

Тупиковая сеть (Stub Network) — сеть, которая имеет только одно соединение с маршрутизатором.

У

Удержание (Hold-Down) — состояние маршрута, при котором маршрутизатор не будет ни объявлять его, ни принимать объявления о нем в течение заданного периода времени (периода удержания). Режим удержания используется для удаления плохой информации о маршруте из всех маршрутизаторов в сети. Маршрут обычно переводится в состояние удержания, когда отказывает линия связи для этого маршрута.

Узел (Node) — 1. Оконечная точка сетевого соединения или точка перехода, общая для двух или более линий связи в сети. Узлами могут быть процессоры, контроллеры или рабочие станции. Узлы, которые разнятся по функциям маршрутизации и другим функциональным возможностям, могут соединяться друг с другом с помощью каналов связи и служить в качестве контрольных точек сети. Иногда термин *узел* используется в обобщенном смысле для обозначения любого объекта, способного иметь доступ к сети. Часто является синонимом термина *устройство*. 2. В архитектуре SNA — основной элемент сети и точка, в которой один или несколько функциональных блоков подключают каналы или цепи передачи данных.

Универсальный указатель ресурсов (Universal Resource Locator) — См. *URL*.

Управление отказами (Fault Management) — четыре категории управления в сетях: управление учетом, управление конфигурацией, управление производительностью и управление защитой информации, которые определены ISO для управления в сетях OSI. Управление отказами представляет собой попытку обеспечить обнаруживаемость и контролируемость отказов в сети.

Управление потоком (Flow Control) — методика, благодаря которой не допускается ситуация, когда передающий объект переполняет данными принимающий объект. При полном заполнении буферов принимающего устройства посылающему устройству отправляется сообщение о необходимости отложить передачу данных до завершения обработки данных в буферах. В IBM-сетях этот метод называется *выравниванием скоростей*.

Управление потоком данных посредством движущихся окон (Sliding Window Flow Control) — метод управления потоком данных, в соответствии с которым получатель разрешает отправителю передачу данных до тех пор, пока окно не заполнится. При заполнении окна передающая сторона должна прекратить передачу, пока приемник не объявит об установке более широкого окна. Этот метод управления потоком данных используется в протоколе TCP, в других транспортных протоколах и в нескольких протоколах канального уровня.

Управление сетью (Network Management) — применение систем или выполнение действий с целью технического сопровождения и определения характеристик сети, а также для устранения неполадок.

Управление трафиком (Traffic Management) — методы предотвращения возникновения перегрузок, а также формирования трафика и его политики. Позволяет каналам работать с более высокими уровнями использования, что достигается за счет уменьшения низкоприоритетного и нечувствительного к задержкам трафика на границе сети в момент возникновения перегрузки.

Уровень обслуживания представлений (Presentation Services Layer) — уровень 6 архитектурной модели SNA. Обеспечивает управление сетевыми ресурсами, обслуживание представлений в сеансе и некоторое управление приложениями. Приблизительно соответствует уровню представлений эталонной модели OSI.

Уровень обслуживания транзакций (Transaction Services Level) — уровень 7 архитектурной модели SNA. Представляет функции пользовательских приложений, например электронные таблицы, текстовый процессор или электронную почту, посредством которых пользователь взаимодействует с сетью. Приблизительно соответствует уровню приложений эталонной модели OSI. См. также *уровень управления потоком данных; уровень управления каналом; уровень управления путем; уровень физического управления; уровень обслуживания представлений; уровень управления передачей*.

Уровень представлений (Presentation Layer) — уровень 6 эталонной модели OSI. Он гарантирует, что информация, посланная уровнем приложений одной системы, будет читаемой уровнем приложений другой системы. Уровень представлений также работает со структурами данных, используемыми программами, и поэтому согласует синтаксис передачи данных для уровня приложений. Приблизительно соответствует уровню обслуживания представлений модели SNA. См. также *уровень приложений; канальный уровень; сетевой уровень; физический уровень; сеансовый уровень; транспортный уровень*.

Уровень приложений (Application Layer) — уровень 7 эталонной модели OSI, обслуживающий прикладные процессы (такие как электронная почта, пересылка файлов и эмуляция терминала), которые являются внешними по отношению к модели OSI. Уровень приложений идентифицирует и устанавливает доступность предполагаемых партнеров по коммуникации (и ресурсов, требующихся для их соединения),

синхронизирует взаимодействующие приложения и устанавливает согласованный порядок выполнения процедур восстановления после ошибок и управления целостностью данных. Приблизительно соответствует уровню службы транзакций в модели SNA. См. также *канальный уровень; сетевой уровень; физический уровень; уровень представлений; сеансовый уровень; транспортный уровень*.

Уровень управления каналом (Data link Control Layer) — уровень 2 архитектурной модели SNA. Ответствен за передачу данных по конкретной физической линии. Приблизительно соответствует каналному уровню эталонной модели OSI. См. *уровень управления потоком данных; уровень управления путем; уровень физического управления; уровень службы представлений; уровень службы транзакций; уровень управления передачей*.

Уровень управления передачей (Transmission Control Layer) — уровень 4 архитектурной модели SNA. Отвечает за установление, поддержание и завершение SNA-сеансов, выстраивание последовательности сообщений с данными и управление потоком данных уровня сеанса. Соответствует транспортному уровню эталонной модели OSI. См. также *уровень управления потоком данных; уровень управления каналом; уровень управления путем; уровень физического управления; уровень обслуживания представлений; уровень обслуживания транзакций*.

Уровень управления потоком данных (Data Flow Control Layer) — уровень 5 архитектурной модели SNA, который определяет взаимодействие партнеров в сеансе и управляет ими, в частности потоком данных. Соответствует сеансовому уровню эталонной модели OSI. См. *уровень управления каналом; уровень управления путем; уровень физического управления; уровень службы представлений; уровень службы транзакций; уровень управления передачей*.

Уровень управления путем (Path Control Layer) — уровень 3 архитектурной модели SNA. Этот уровень оказывает услуги по упорядочению в последовательность для правильной последующей сборки данных. Уровень управления путем также несет ответственность за маршрутизацию. Приблизительно соответствует сетевому уровню модели OSI. См. *уровень управления потоком данных; уровень управления каналом; уровень физического управления; уровень обслуживания представлений; уровень обслуживания транзакций; уровень управления передачей*.

Уровень физического управления (Physical Control Layer) — уровень 1 архитектурной модели SNA. Отвечает за спецификации физических каналов между оконечными системами и соответствует физическому уровню эталонной модели OSI. См. также *уровень управления потоком данных; уровень управления каналом; уровень управления путем; уровень обслуживания представлений; уровень обслуживания транзакций; уровень управления передачей*.

Усовершенствованный протокол IGRP (Enhanced Interior Gateway Routing Protocol) — усовершенствованный протокол внутренней маршрутизации между шлюзами. Улучшенная версия протокола IGRP, разработанная компанией Cisco. Обеспечивает превосходные показатели по сходимости и эффективности эксплуатации и объединяет преимущества протоколов с учетом состояния каналов связи с достоинствами протоколов на основе вектора расстояния. Сравните с IGRP. См. также IGP; OSPF; RIP.

Ф

Физический адрес (Physical Address) — См. *MAC-адрес*.

Физический уровень (Physical Layer) — уровень 1 эталонной модели OSI. Определяет электрические, механические, процедурные и функциональные спецификации активизации, поддержания и деактивизации физического канала между оконечными системами. Соответствует уровню физического управления модели SNA. См. также *уровень приложений'*, *канальный уровень'*, *сетевой уровень'*, *уровень представлений'*, *сеансовый уровень'*, *транспортный уровень'*.

Фильтр (Filter) — процесс или устройство, которое экранирует сетевой трафик по определенным характеристикам, например адрес источника, адрес пункта назначения или протокол, и на основе установленных критериев определяет, пропускать или не пропускать трафик.

Фильтрация локального трафика (Local Traffic Filtering) — процесс, посредством которого мост отфильтровывает (выбрасывает) кадры, MAC-адреса источника и пункта назначения в которых находятся на одном и том же интерфейсе моста, чем исключается переадресация лишнего трафика мостом. Описание содержится в стандарте IEEE 802.1.

Флэш-память (Flash memory) — энергонезависимое устройство для хранения информации, данные в котором могут электрически стираться и перепрограммироваться, так что образы программного обеспечения могут храниться, загружаться и переписываться. Флэш-память была разработана компанией Intel, и лицензия на ее производство была выдана другим компаниям-изготовителям полупроводниковых приборов.

Формирование сигналов (Signaling) — процесс посылки сигнала передачи в физическую среду в целях обеспечения обмена информацией.

Фрагмент (Fragment) — часть большего по размеру пакета, который был разбит на более мелкие блоки. В сетях Ethernet этим термином также иногда обозначают кадр, размер которого меньше установленного предела 64 байта.

Фрагментация (Fragmentation) — процесс разбиения пакета на более мелкие блоки при передаче в сетевой среде, которая не поддерживает исходный размер пакета.

X

Хаб (Hub) — 1. В общем случае это устройство, которое служит в качестве центральной точки сети со звездообразной топологией и подсоединяет конечные станции. Работает на уровне 1 эталонной модели OSI. 2. В сетях Ethernet и IEEE 802.3 многопортовый Ethernet-повторитель, иногда называемый *концентратором*.

Хвостовая часть (Trailer) — служебная информация, подсоединяемая к данным в процессе их инкапсуляции перед передачей по сети. Сравните с *заголовком*.

Хост-машина (Host) — компьютерная система, находящаяся в сети. По смыслу этот термин похож на термин *узел*, только под хост-машиной обычно понимают компьютерную систему, тогда как термин *узел* применяется в отношении любой сетевой системы, включая серверы доступа и маршрутизаторы. См. также *узел*.

Частично полноразмерная сетка (Partial Mesh) — сеть, в которой устройства организованы в топологию сетки, при этом часть узлов сети объединены в полноразмерную сетку, тогда как другие соединены только с одним или двумя другими узлами сети. Частично полноразмерная сетка не обеспечивает того уровня дублирования, который дает полноразмерная сетка, но она дешевле в реализации. Топология с частично полноразмерной сеткой обычно используется в периферийных сетях, которые соединяются с полноразмерной

сеткой магистрального канала.

Ш

Шинная топология (Bus Topology) — линейная архитектура локальной сети, при которой передаваемая рабочими станциями информация распространяется по всей длине среды передачи данных и принимается всеми другими станциями. Сравните с *кольцевой, звездообразной и древовидной топологиями*.

Широковещательный адрес (Broadcast Address) — специальный адрес, зарезервированный для рассылки сообщений всем рабочим станциям. В общем случае широковещательный адрес представляет собой MAC-адрес пункта назначения, состоящий из единиц. Сравните с *адресом многоадресного пакета и адресом одноадресного пакета*. См. также *широковещательный пакет*.

Широковещательный пакет (Broadcast) — пакет данных, который посылается во все узлы сети. Идентифицируются широковещательные пакеты адресом широковещания. Сравните с *многоадресным пакетом и одноадресным пакетом*. См. также *широковещательный адрес*.

Шлюз (Gateway) — раньше так называли маршрутизирующее устройство. Сегодня для описания узлов, выполняющих эту функцию, используется термин *маршрутизатор*, а *шлюзом* называют специальное устройство, которое на уровне приложений модели OSI преобразует информацию из формата одного набора протоколов в формат другого набора протоколов. Сравните с *маршрутизатором*.

Э

ЭСПЗУ (EEPROM) — электрически стираемое программируемое постоянное запоминающее устройство. Информация в ЭСПЗУ может стираться путем подачи электрических сигналов на определенные выводы микросхемы.

Эталонная модель — См. *эталонная модель OSI*.

Эталонная модель OSI (OSI Reference Model) — архитектурная модель сети, разработанная ISO и ITU-T. Модель состоит из семи уровней, каждый из которых определяет конкретные сетевые функции-, адресацию, управление потоком, управление ошибками, инкапсуляцию и надежную пересылку сообщений. Самый нижний уровень (физический) теснее других связан с технологиями сред передачи данных. Два нижних уровня реализуются аппаратно и программно, а верхние пять — только программно. Самый высокий уровень (уровень приложений) находится ближе всего к пользователю. Эталонная модель OSI имеет универсальное применение в качестве метода для обучения и объяснения функций, реализуемых сетью В некоторых аспектах она подобна архитектурной модели SNA. См. *уровень приложений; канальный уровень; сетевой уровень; физический уровень; уровень представлений; сеансовый уровень; транспортный уровень*.

Эхо-канал (Echo Channel) — См. *E-канал*.