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

Редактор серии "Основы организации сетей Cisco" — Вито Амато

Авторизованное учебное пособие по программе "Основы организации сетей Cisco"

Основы организации сетей Cisco

том 2

Cisco Systems
Cisco Press

ББК 32.973.26-018.2.75
А61
УДК 681.3.07

Издательский дом "Вильяме"

Зав. редакцией *С.Н. Тригуб*
Перевод с английского *А.Н. Крикуна*

По общим вопросам обращайтесь в Издательский дом "Вильяме" по адресу:
info@williamspublishing.com, http://www.williamspublishing.com

Амато, Вито.
А61 Основы организации сетей Cisco, том 2. : Пер. с англ. — М. : Издательский дом "Вильяме", 2002. — 464 с.: ил. — Парал. тит. англ.

ISBN 5-8459-0283-5 (рус.)

Данная книга является второй частью учебного пособия для студентов, соответствующего учебному плану версии 2.1 Сетевой академии Cisco. Являясь продолжением части 1 пособия, материал второго тома углубляет познания студентов в сетевых технологиях. В первом томе подробно рассматривались отдельные компоненты и устройства сетей, второй том посвящен более общим вопросам. В нем подробно описываются сети различных видов (локальные, виртуальные и распределенные), используемые в них протоколы и методы проектирования вышеупомянутых сетей. В первой главе изложены основные положения, относящиеся к Эталонной модели OSI, которая является базой при рассмотрении последующих тем. Отдельная глава посвящена вопросам обеспечения информационной безопасности путем использования списков управления доступом. Для каждого типа сетей, описанного в отдельной главе, подробно рассмотрена методология проектирования. Для практической реализации приобретенных знаний на протяжении всей книги рассматривается проект учебной сети.

Книга рекомендуется для подготовки к тесту CCNA и сертификационному экзамену CompTIA Net+.

ББК 32.973.26-018.2.75

ISBN 5-8459-0283-5 (рус.)
ISBN 1 -58713-005-X (англ.)

Оглавление

Содержание

Глава 5. Протоколы маршрутизации IGRP

Глава 6. Списки управления доступом (ACL)

О редакторе серии

Вито Амато (Vito Amato) — старший технический автор во Всемирной образова-тельной системе компании Cisco. В свое время он работал директором по информа-ционным технологиям отдела образования штата Аризона Степень доктора филосо-фии Вито получил в Аризонском государственном университете, где специализиро-вался на разработке учебных курсов и методичек с ударением 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 внедре-ние 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 Уорда (George Ward), Кевина Уорнера (Kevin Warner), Алекса Белоуса (Alex Belous), Дэвида Александера (Devid Alexander) и всей группы, которая занимается разработкой учебных курсов. Мне хотелось бы высказать слова призна-тельности 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 позво-лило мне организовать материал книги. Кроме того, хотелось бы поблагодарить Уэйна Льюиса (Wayne Lewis), обновившего устаревшие данные. Уэйн является координато-ром 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 сер-тифицированным специалистом Cisco по сетям и проектированию, а также сертифи-цированным инструктором Академии Cisco и специалистом Microsoft В свободное время Уэйн занимается серфингом на северном побережье Оаху. И, конечно же, я хо-тел бы поблагодарить свою жену Бонни и моих детей Тори, Майкла, Меттью 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 Льюис (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 сетейСЛзсо. 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 Хоит (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 сертифицирование 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 Сиэтле. 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 Сиэтла. 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: mfo@ciscopress.ru
WWW: http://www.ciscopress.ru

Введение

Второй том книги *Основы организации сетей Cisco* задуман как дополнение к классным и лабораторным занятиям студентов, изучающих интерактивный курс Сетевой академии Cisco версии 2.1.

Книга предназначена для дополнения учебных материалов, уже использованных в этой программе, а также освещает темы, входящие в программу экзамена на получение сертификата Сетевой Ассоциации Cisco (Cisco Certified Networking Associate, CCNA). Книга строго следует стилю и формату, которые использованы корпорацией Cisco в учебной программе *Основы организации сетей Cisco*. К книге прилагается компакт-диск, на котором имеются видеоклипы, представленные в интерактивном мультимедийном формате и предлагаемые в качестве справочного учебного материала.

Цель книги

Целью книги является обучение сетевым технологиям, поддерживаемым корпорацией Cisco и содействие обучающимся в понимании процессов проектирования и реализации сети, а также процесса установки конфигурации маршрутизаторов Cisco. Предполагается, что книга будет использоваться в тесной связи с программой *Основы организации сетей Cisco*.

Вашингтонский проект

В главе 4, "Проектирование локальных сетей", начинается описание и разработка учебного, так называемого Вашингтонского проекта. Предполагается, что он поможет в изучении предмета, поскольку позволяет применить приобретенные знания к примеру из реальной жизни. Первоначально Вашингтонский проект был описан в первом томе настоящего пособия. Однако реальная работа по проектированию начинается только во второй части программы, которая описана в настоящей книге. По мере ввода новых понятий происходит обучение их практическому применению. В каждой главе приводятся общие принципы, конкретные положения и термины, знание которых необходимо для реализации Вашингтонского проекта.

Метод изложения материала

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 список тем, которые будут в ней рассмотрены. Этот список также включает в себя понятия, вводимые в этой главе, что может быть использовано для ориентации в материале книги.
- *Рисунки, примеры и таблицы*. В книге содержатся рисунки, примеры и таблицы, которые помогают понять теоретические положения, термины, команды и последовательности команд, применяемые при установке конфигурации; они делают более наглядными используемые понятия и помогают лучше представить себе излагаемый материал. Кроме того, примеры и таблицы могут рассматриваться как обзоры команд с описаниями и примерами вывода на экран; они также содержат полезную практическую и теоретическую информацию.
- *Задачи проекта Вашингтонского учебного округа*. В каждой главе, начиная с 4-й, ставится некоторая задача по созданию проекта сети учебного округа. Решение этой задачи углубляет понимание тем и понятий, изложенных в главе, поскольку позволяет практически применить приобретенные знания.
- *Примечания к Вашингтонскому проекту*. В каждой главе, начиная с 4-й, приводятся примечания к Вашингтонскому проекту. Эти примечания относятся к

введенным в главе понятиям и помогают применить приобретенные знания к данному конкретному проекту.

- *Заметки в инженерном журнале*. Начиная с 4-й главы в тексте приводятся инженерные заметки. Они относятся к введенным в главе понятиям и предоставляют дополнительную информацию, выходящую за рамки основного курса и помогающую применить изучаемый материал к ситуациям из реальной практики.
- *Резюме*. В конце каждой главы приведено ее краткое изложение; оно представляет собой небольшой реферат главы и помогает при изучении ее материала.
- *Контрольные вопросы*. В конце каждой главы приводятся 10 контрольных вопросов, которые можно использовать для оценки приобретенных знаний. В процессе ответа на вопросы углубляется понимание изученного материала; они также позволяют оценить уровень готовности при переходе к изучению нового материала.
- *Основные термины*. После контрольных вопросов приводится список основных терминов, в который включены все новые термины, использованные в этой главе. Этот небольшой толковый словарь помогает при изучении материала главы.

Обозначения и принятые соглашения

В этой книге используются следующие условные обозначения.

- Новые и важные термины набраны *курсивом*.
- Основные термины, содержание которых описано в конце главы, набраны **полужирным шрифтом.**
- Новые или важные термины выделены *курсивом*.
- Все коды программ набраны моноширинным шрифтом, а для выделения отдельных частей кода приняты следующие соглашения.
- Команды и ключевые слова набраны полужирным моноширинным шрифтом.
- Аргументы, значения которых вводятся пользователем, набраны *моноширинным* курсивом.
- Квадратные скобки ([ ]) указывают на необязательные ключевые слова или аргументы.
- Фигурные скобки ({ }) указывают на необходимость выбора одного из не скольких вариантов.
- Вертикальная черта (|) разделяет варианты, из которых необходимо вы брать один.

Структура книги

Книга включает в себя 12 глав, 3 приложения и глоссарий.

В главе 1, "Эталонная модель OSI и маршрутизация", приведено описание Эталонной модели открытых систем (Open System Interconnection reference model, OSI), обзор сетевого планирования и обсуждены вопросы проектирования, связанные с маршрутизацией.

В главе 2, "Коммутация в локальных сетях", обсуждаются проблемы локальных сетей и возможные способы повышения эффективности их использования. Кроме того, в этой главе рассмотрены преимущества и недостатки использования мостов, коммутаторов и маршрутизаторов для сегментации локальных сетей и проанализировано влияние коммутации, использования мостов и маршрутизации на пропускную способность сети. В заключение описываются и сравниваются между собой сети типов Ethernet, Fast Ethernet и виртуальные локальные сети. Здесь также обсуждаются достоинства и недостатки этих технологий.

В главе 3, "Виртуальные локальные сети", представлен обзор виртуальных сетей и коммутации в сетях с общей передающей средой, сравниваются между собой традиционные конфигурации локальных сетей с конфигурациями коммутируемых LAN и обсуждаются преимущества использования коммутируемой архитектуры локальных сетей.

В главе 4, "Проектирование локальных сетей", представлен обзор методов проектирования локальных сетей. В ней также обсуждаются цели проектирования локальных сетей, вопросы сетевого дизайна, методология сетевого проектирования и развитие топологий локальных сетей.

В главе 5, "Протоколы маршрутизации IGRP", обсуждается использование маршрутизаторов для соединения между собой двух или более сетей и их использование для передачи пакетов данных между сетями на основе сетевой протокольной информации. В этой главе описана работа маршрутизаторов и типы используемых ими протоколов. В заключение описывается процесс маршрутизации, IP-протоколы маршрутизации и обсуждается протокол IGRP.

В главе 6, "Списки управления доступом (ACL)", описаны стандартные и расширенные списки управления доступом (ACL) , которые применяются для управления потоками данных в сети и рассмотрено использование этих списков в качестве средства обеспечения безопасности сети. Глава также включает в себя рекомендации и общие принципы использования списков управления доступом, а также команды и типы конфигураций, необходимые для создания таких списков. В заключение приведены примеры стандартных и расширенных списков и их применение к интерфейсам маршрутизатора.

В главе 7, "Протокол Novell IPX", описаны протоколы, работа и конфигурация сетей Novell IPX. Кроме того, объясняется использование маршрутизаторов Cisco в сетях NetWare, обсуждаются вопросы тестирования работы протокола IPX и связь между маршрутизаторами. Рассмотрены также вопросы устранения ошибок в работе протокола IPX.

В главе 8, "Распределенные сети", описаны различные протоколы и технологии, используемые в средах распределенных сетей. В этой главе изложены основы теории распределенных сетей, включая вопросы типичных технологий таких сетей, типы служб, форматы инкапсуляции и параметры каналов. В заключение рассматриваются каналы связи типа "точка-точка", коммутация каналов и пакетов, виртуальные каналы, службы набора и устройства распределенных сетей.

В главе 9, "Проектирование распределенной сети", приведен обзор методологий, используемых при проектировании распределенных сетей Глава включает в себя описание коммуникации в распределенных сетях и описание процесса их проектирования. Рассмотрен процесс сбора требований пользователей к проектируемым распределенным сетям и проанализированы преимущества использования иерархической модели проектирования.

В главе 10, "Протокол PPP", обсуждаются основные элементы сети, процессы действия, определяющие коммуникацию типа "точка-точка". В этой главе также описан процесс конфигурирования и проверки работоспособности протокола PPP.

В главе 11, "ISDN — цифровая сеть интегрированных служб", описаны службы стандарты, компоненты, функционирование и конфигурация ISDN-коммуникации.

В главе 12, "Протокол Frame Relay", обсуждаются службы, стандарты и компоненты протокола Frame Relay и описана его работа. В главе также описаны задачи кон фигурирования служб протокола Frame Relay, команды мониторинга и поддержки соединений протокола.

В приложении А, "Ответы на контрольные вопросы", приведены ответы на находящиеся в конце каждой главы контрольные вопросы.

В приложении Б, "Список команд", описаны команды, необходимые для конфигурирования и использования маршрутизаторов Cisco. Они расположены в алфавит ном порядке, что позволяет легко найти информацию, относящуюся к данной команде. Для каждой команды дана перекрестная ссылка на главы, в которых она использована, что позволяет без труда найти дополнительную информацию об этой команде.

В приложении В, "Список видеороликов", содержится справочная информации обо всех видеоклипах, находящихся на прилагаемом к книге компакт-диске.

В глоссарии даны определения всех терминов и аббревиатур, использованных книге для описания сетей и происходящих в них процессов.

Ключевые темы этой главы

- Рассмотрены общие функции эталонной модели OSI и решаемые ею проблемы
- Описаны характеристики физического уровня эталонной модели OSI
- Описаны характеристики канального уровня эталонной модели OSI
- Описаны характеристики сетевого уровня эталонной модели OSI
- Описаны характеристики транспортного уровня эталонной модели OSI
- Рассмотрены функции маршрутизатора в сети
- Описана работа различных протоколов

Глава 1

Эталонная модель OSI и маршрутизация

Введение

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

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

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

Многоуровневая модель сети: эталонная модель OSI

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

Среди причин подразделения различных сетевых функций на уровни отметим следующие.

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

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

- **Уровень приложений (7-й уровень).** Этот уровень используется для обеспечения работы приложений пользователя. Например, для текстового редактора на этом уровне осуществляется передача файлов.
- **Уровень представления данных (6-й уровень).** Этот уровень обеспечивает представление данных и их форматирование, а также определяет синтаксис передачи данных. В случае, когда этот синтаксис соответствует требованиям сети, данные, используемые приложением могут быть получены из сети и переданы в нее.
- **Сеансовый уровень (5-й уровень).** Этот уровень обеспечивает сеанс обмена данными между приложениями, а также управляет этим процессом.
- **Транспортный уровень (4-й уровень).** На этом уровне происходит формирование сегментов данных и преобразование их в поток данных. Этот уровень способен гарантировать установление связи и надежную передачу данных.
- **Сетевой уровень (3-й уровень).** На этом уровне выбирается оптимальный способ передачи данных из одной точки сети в другую. На этом уровне работают маршрутизаторы. При этом используются схемы логической адресации, которыми может управлять сетевой администратор. Этот уровень использует схему адресации протокола IP, а также схемы адресации AppleTalk, DECNet, Vines и IPX.
- **Уровень канала связи или канальный уровень (2-й уровень).** На этом уровне происходит физическая передача данных. При этом посылаются уведомления об ошибках анализируется топология сети и осуществляется управление потоком данных. На этом уровне используются **MAC-адреса,** которые также называются **адресами управления доступом к среде или аппаратными адресами (Media** Access **Control).**
- **Физический уровень (1-й уровень).** На этом уровне используются электрические механические, процедурные и функциональные средства для установки и поддержки физической связи между различными устройствами сети. При этом используются такие физические передающие среды, как витые пары, коаксиальные и оптоволоконные кабели.

Рис. 1.1. Эталонная модель OSI определяет функции различных уровней, которые могут быть использованы производителями сетевых устройств для облегчения процесса проектирования и модернизации сетей

Обмен информацией между устройствами одного ранга

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

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

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

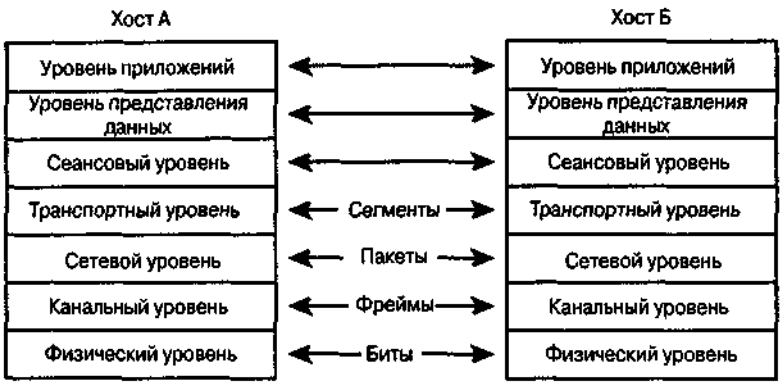


Рис. 1.2. При обмене информацией между хостами используются протоколы соответствующих уровней; при этом нижний уровень обеспечения возможность работы вышестоящего уровня

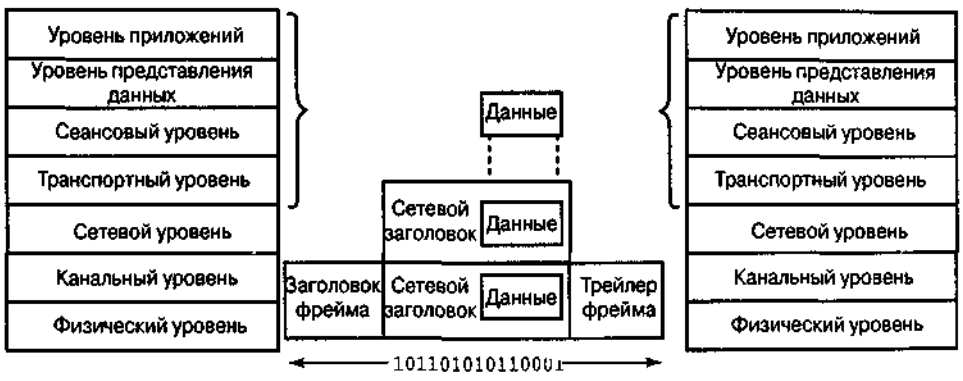
Хотя каждый уровень хоста А обменивается данными с прилегающими уровнями, он также выполняет некоторые первичные, присущие именно ему функции. Они состоят в обмене данными с соответствующим уровнем хоста В, т.е. 1-й уровень хоста В выполняет обмен данными с 1-м уровнем хоста А, 2-й уровень хоста В выполняет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

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

Инкапсуляция данных

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

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



Рис, 1.3. Задачей сетевого уровня является передача данных по сети, по-

средством инкапсуляции данных и заголовка

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

Предположим, что хост А желает отправить хосту В по электронной почте следующее сообщение:

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

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

Этап 1. Когда пользователь посылает электронное сообщение, буквенноцифровые символы последовательно преобразуются в данные для передачи на 7, 6 и 5-м уровнях и после этого передаются в сеть.

Этап 2. Используя сегменты своего формата, транспортный уровень упаковывает данные для транспортировки их по сети и обеспечивает надежную связь между двумя хостами, участвующими в передаче и приеме электронного сообщения.

Этап 3. На 3-м уровне данные упаковываются в пакет (дейтаграмму), содержащий сетевой заголовок и логические адреса отправителя и получателя. После этого сетевые устройства пересылают пакеты по сети, используя выбранный маршрутизатором путь.

Этап 4. На 2-м уровне каждое сетевое устройство должно вставить пакет во фрейм. Фрейм позволяет осуществить соединение со следующим сетевым устройством. Каждое устройство на выбранном сетевом пути требует создания фрейма для соединения со следующим устройством.

Этап 5. На 1-м уровне фрейм должен быть преобразован в последовательность нулей и единиц для прохождения по передающей среде (обычно по проводу). Механизм синхронизации позволяет различать между собой эти биты по мере того как они проходят через передающую среду. На различных участках сетевого пути тип передающей среды может меняться. Например, электронное сообщение может начать свое движение в локальной сети, пересечь магистраль, выйти в распределенную сеть и достичь пункта назначения в другой удаленной локальной сети.

Физический уровень

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

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

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

- **Сети Ethernet и сети стандарта IEEE 802.3.** LAN-спецификации, работающие со скоростью 10 Мбит/с по коаксиальному кабелю.
- **Сети Ethernet 100 Мбит/с.** Отдельная спецификация локальной сети, также известная как **быстрый Ethernet (Fast Ethernet),** которая работает на витой паре со скоростью 100 Мбит/с.
- **Сети Ethernet 1000 Мбит/с.** Отдельная LAN-спецификация, также известная как **гигабитовый Ethernet (Gigabit-Ethernet),** работающая на оптоволоконном кабеле и на витой паре со скоростью 1000 Мбит/с.

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

Физические соединения сетей Ethernet 802.3

Спецификации Ethernet и стандарты на кабели IEEE 802.3 определяют шинную топологию локальных сетей, работающих со скоростями до 10 Мбит/с.
На рис. 1.4 проиллюстрировано применение трех существующих кабельных стандартов.

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

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

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

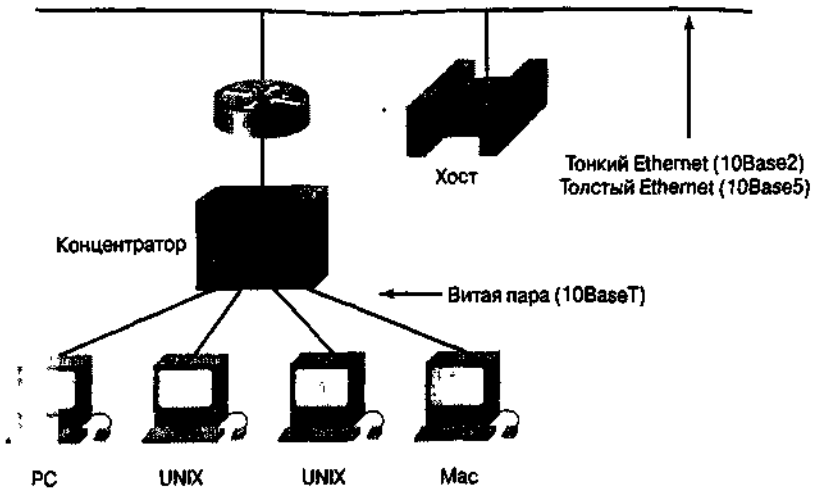


Рис. 1.4. Стандарты 10Base2, 10Base5 и 10BaseT обеспечивают доступ нескольким станциям к одному и тому же сегменту LAN

Уровень канала связи

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

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

Для записи MAC-адреса используется шестнадцатеричная система счисления. Существуют два формата MAC-адресов: 0000.Oc12.3456 и OO-OO-Oc-12-34-56.

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

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

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

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

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

Интерфейс сети Ethernet/802.3

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

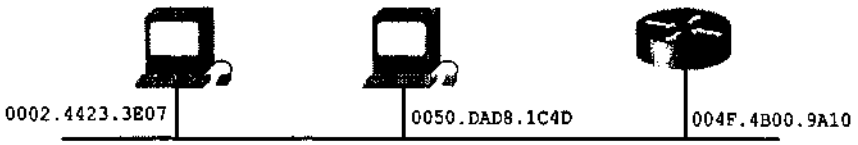


Рис. 1.5. Для указания на то, что на маршрутизаторе используется интерфейс 802.3, в операционной системе Cisco Internetwork Operating System (IOS) применяется специальная аббревиатура — перед типом интерфейса ставится буква E, за которой следует номер интерфейса (например, как данном случае, 0)

Сетевой уровень

На сетевом уровне эталонной модели OSI используются несколько протоколов.

- **Протокол IP** обеспечивает маршрутизацию дейтаграмм с **негарантированной доставкой (best-effort delivery)** без установки логического соединения (connectionless). Этот протокол не интересуется содержанием дейтаграмм; он лишь ищет наилучший способ направить дейтаграмму к месту ее назначения.

- **Протокол управляющих сообщений в сети Internet (Internet Control Message Protocol, ICMP)** обеспечивает возможность управления и отправки сообщений.

- **Протокол преобразования адресов (Address Resolution Protocol, ARP)** определяет адрес уровня канала связи по известному IP-адресу.

- **Обратный ARP (reverse ARP, RARP)** определяет сетевой адрес устройства в ситуациях, когда известен адрес канального уровня.

IP-адресация и подсети

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

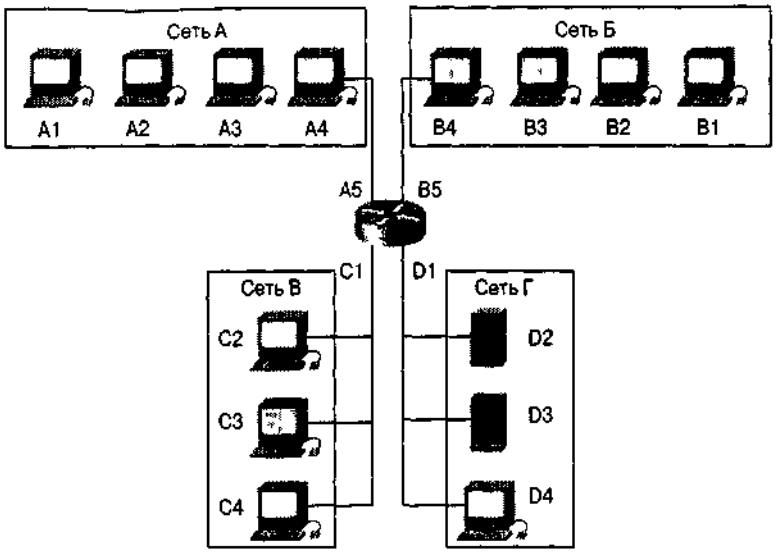


Рис. 1 6 Каждая сеть имеет свой адрес и все ее хосты имеют свои индивидуальные адреса

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

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

Определение пути

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

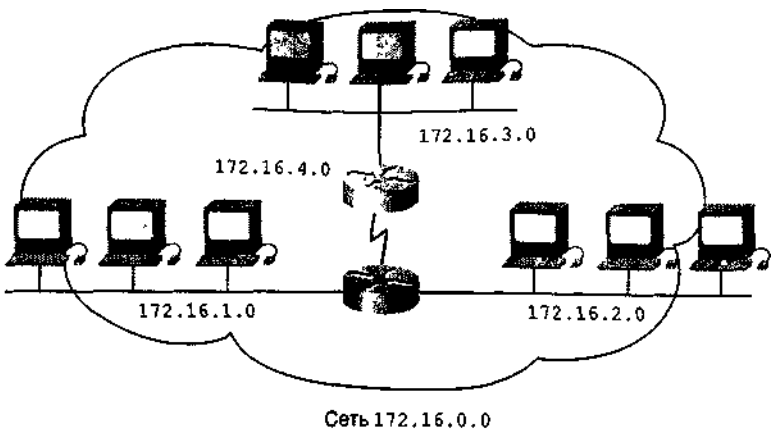


Рис. 1.7. Маршрутизаторы определяют сеть-получатель, используя адрес подсети и ограничивая тем самым поток данных по другим сегментам сети

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

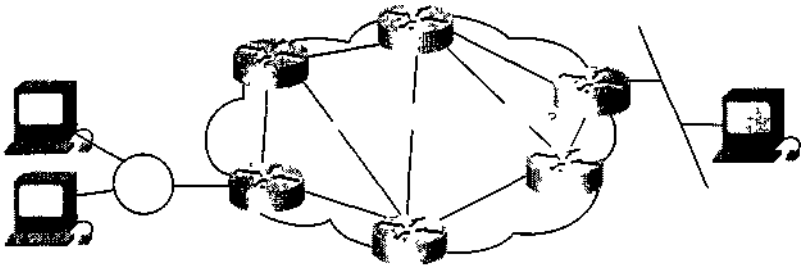


Рис. 1.8. Процедура определения пути позволяет маршрутизатору оценить возможные пути к месту назначения и выбрать наиболее предпочтительный способ обработки пакета

Обмен информацией о путях

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

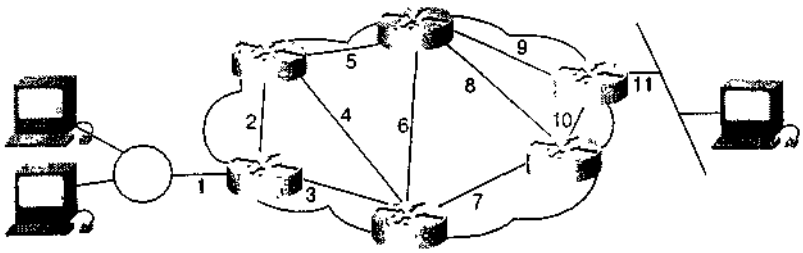


Рис. 1.9. Адрес должен содержать информацию о пути между точками передающей среды, используемыми для передачи пакетов от источника к пункту назначения

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

Сеть	Хост
1	1
	2
	3
2	1
3	1

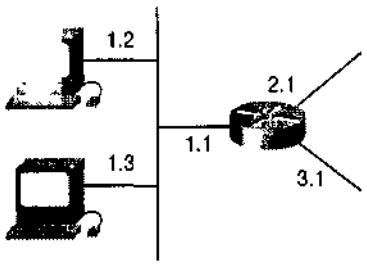


Рис. 1.10. Большинство схем адресации, использующих сетевой протокол, используют какую-либо форму адреса хоста или узла

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

Протокол ICMP

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

- Destination unreachable (Пункт назначения недостижим).
- Time exceeded (Превышено время ожидания).
- Parameter problem (Проблема с параметром).
- Source quench (Подавление источника).
- Redirect (Перенаправить).
- Echo (Эхо-запрос).
- Echo reply (Эхо-ответ).
- Timestamp (Запрос времени).
- Timestamp reply (Ответ на запрос о времени).
- Information request (Информационный запрос).
- Information reply (Ответ на информационный запрос).
- Address request (Запрос об адресе).
- Address reply (Ответ на запрос об адресе).

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

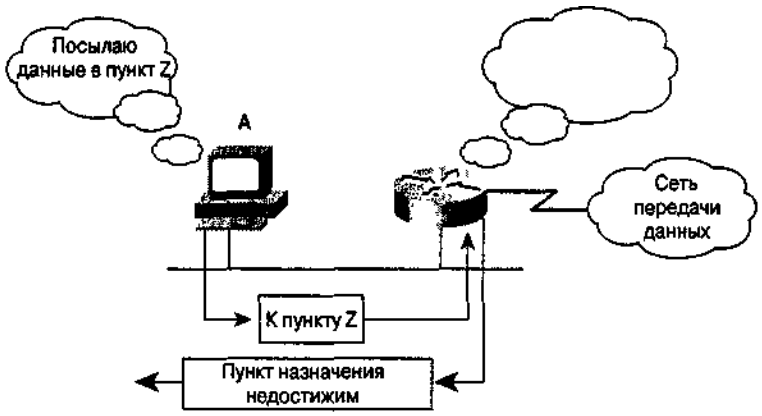


Рис. 1.11. Маршрутизатор отправляет сообщение: "Destination unreachable" ("Пункт назначения недостижим"), указывающее на то что он не может получить доступ к хосту, порту или сети, куда направлен пакет

Протокол ARP

Для осуществления коммуникации в сети Ethernet станция-источник должна знать IP- и MAC-адреса станции-получателя. После того как станция-отправитель определила IP-адрес станции-получателя, Internet-протокол источника использует таблицу ARP для нахождения соответствующего MAC-адреса получателя.

Если Internet-протокол находит в своей таблице IP-адрес получателя, соответствующий его MAC-адресу, то он связывает их и использует для инкапсуляции данных, после чего пакет пересылается через сетевую среду и получается станцией-адресатом.

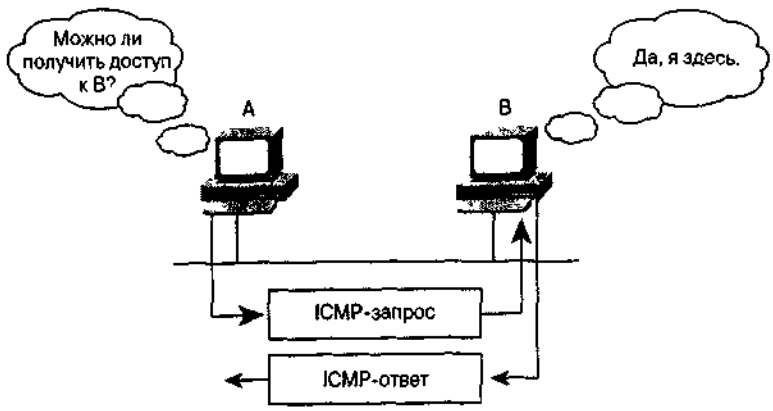


Рис. 1.12. Результатом выполнения команды ping *может стать и получение других lCMP-сообщений, таких как "Destination unreachable" ("Пункт назначения недостижим") или "Time exceeded" ("Истекло время ожидания ")*

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

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

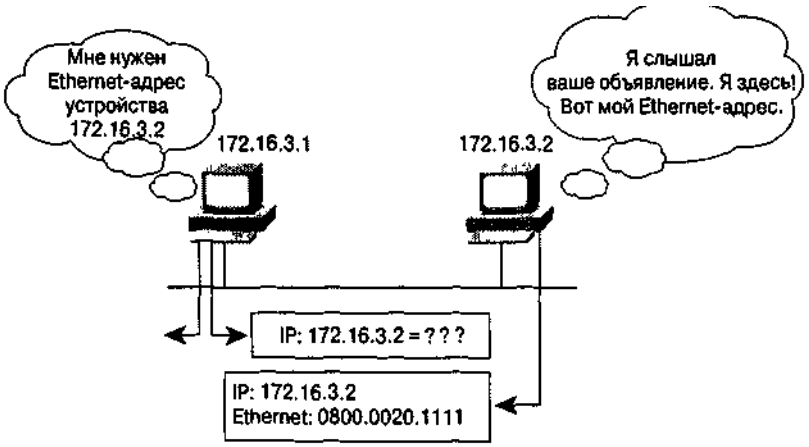


Рис. 1.13. Локальный ARP преобразует адрес путем анализа маски подсети

Маршрутизация

Сетевой уровень должен вступать во взаимные отношения с различными нижними уровнями. Маршрутизатор должен уметь обрабатывать пакеты, инкапсулированные во фреймы нижних уровней, не меняя адресации третьего уровня для данного пакета.

На рис. 1.14 изображен пример такой маршрутизации от одной LAN к другой. В данном случае потоку данных от хоста 4 Ethernet-сети 1 требуется найти путь к хосту 5 сети 2.

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

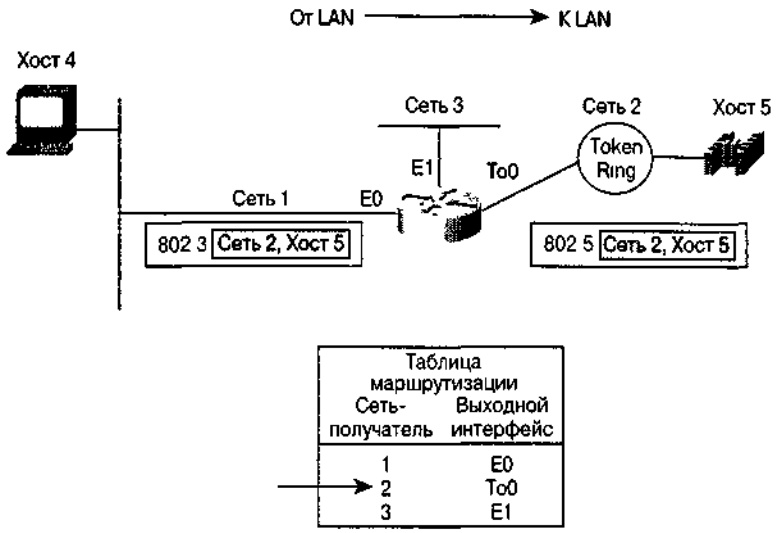


Рис. 1.14. Нахождение наилучшего пути хостами LAN зависит от маршрутизатора и его согласованной сетевой адресации

Операции маршрутизатора

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

коммутации.

Сеть-получатель	Направление и порт маршрутизатора
1.0	1.1
2.0	2.1
3.0	3.1

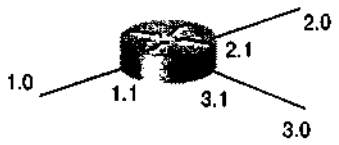


Рис. 1.15. Маршрутизатор передает пакет в следующую сеть по заданному пути, а сетевую часть адреса использует для выбора пути

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

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

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

Сравнение динамической и статической маршрутизации

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

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

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

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

Пример маршрута по умолчанию

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

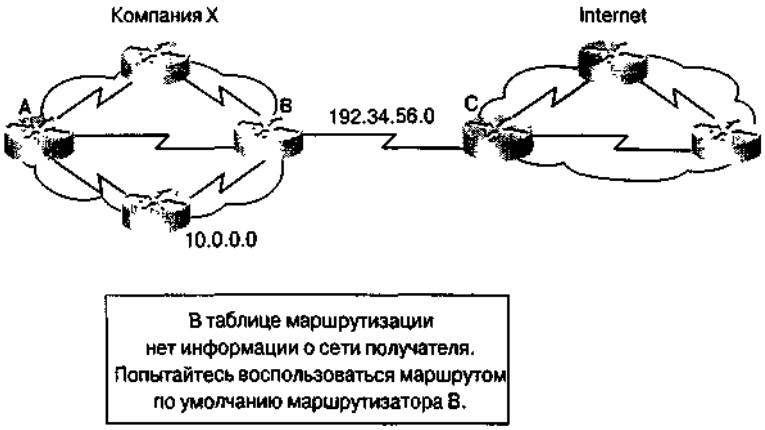


Рис. 1.16. Маршруты по умолчанию могут быть установлены заданной сетевым администратором статической конфигурацией. Вместо поддержания конкретной информации о топологии сети каждый маршрутизатор компании X проинформирован о маршруте по умолчанию и может получить доступ к любому неизвестному пункту назначения, направив пакет в Internet

Маршрутизируемые протоколы и протоколы маршрутизации

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

Маршрутизируемый протокол — это любой сетевой протокол, который в своем адресе сетевого уровня содержит достаточно информации для того, чтобы направить пакет от хоста к хосту, опираясь на схему адресации. Маршрутизируемый протокол определяет формат и характер использования полей внутри пакета. При этом пакет обычно направляется оі одной конечной системы к другой. Примером маршрутного протокола является IP.

Протокол маршрутизации — это протокол, который поддерживает маршрутизируемый протокол, предоставляя ему механизмы совместного использования информации по маршрутизации. Сообщения маршрутизирующих протоколов перемещаются между маршрутизаторами. Маршрутизирующий протокол позволяет маршрутизаторам обмениваться информацией друг с другом с целью поддержки таблиц маршрутизации и внесения в них изменений. Примерами протоколов маршрутизации типа TCP/IP являются протоколы: **Routing Information Protocol (RIP), Interior Gateway Protocol (IGRP), Enhanced Interior Gateway Routing Protocol (Enhanced IGRP) и Open Shortest Path First (OSPF).**

Протоколы маршрутизации

Эффективность динамической маршрутизации зависит от выполнения маршрутизатором

двух своих основных функций.

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

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

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

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

IP-протоколы маршрутизации

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

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

Типы протоколов маршрутизации

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

Конвергенция

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

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

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

Дистанционно-векторная маршрутизация

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

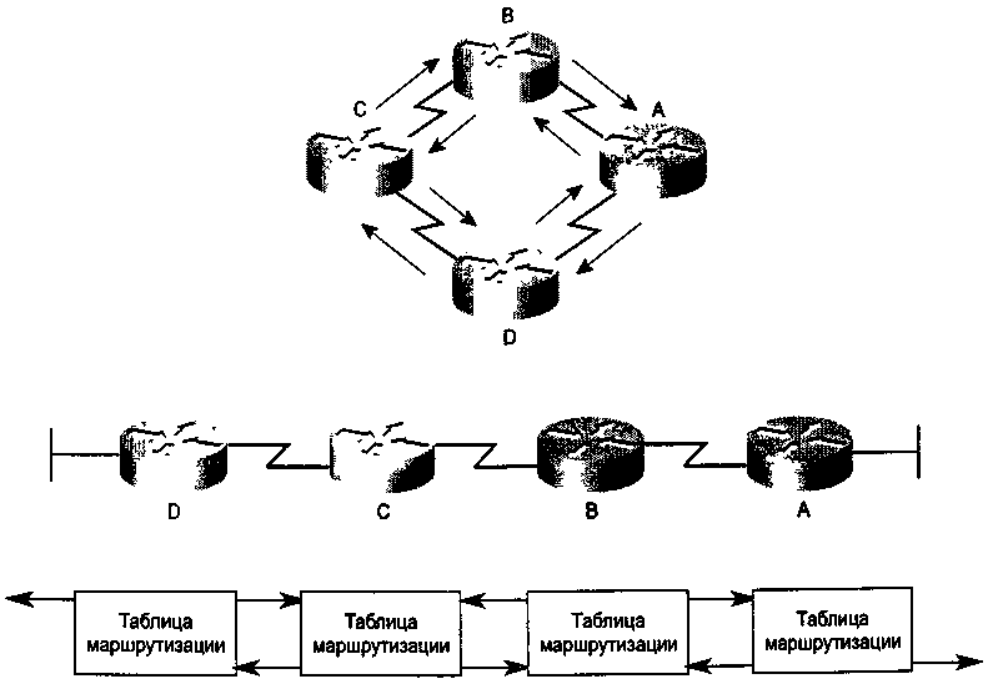


Рис 1 17 Регулярный обмен информацией между маршрутизаторами отображает изменения в то пологий сети

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

Маршрутизация состояния канала связи

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

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

Сравнение дистанционно-векторной маршрутизации и маршрутизации состояния канала связи

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

- Дистанционно-векторная маршрутизация получает все топологические данные из таблиц маршрутизации своих соседей. Маршрутизация состояния канала связи получает информацию о топологии всей сети путем накопления всех не обходимых LSA.
- При дистанционно-векторной маршрутизации наилучший путь определяется путем увеличения некоторого числового значения по мере перемещения таблиц

от одного маршрутизатора к другому. При маршрутизации состояния канала связи каждый маршрутизатор сам отдельно рассчитывает кратчайший путь к месту назначения.

- В большинстве протоколов дистанционно-векторной маршрутизации отображение изменений топологии происходит периодически по мере поступления таблиц изменений. Эти таблицы перемещаются от одного маршрутизатора к другому, что часто приводит к медленной конвергенции. В протоколах маршрутизации состояния канала связи внесение изменений вызывается изменениями в топологии. Относительно небольшие LSA, передаваемые всем остальным маршрутизаторам, обычно приводят к уменьшению времени конвергенции.

Конфигурирование IP-маршрутизации

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

Конфигурирование IP-адресов

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

Конфигурирование динамической маршрутизации

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

С перечисленных ниже команд маршрутизатора начинается процесс настройки системы маршрутизации.

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

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

Команда network	**Описание**
network *номер сети*	Указывает непосредственно подсоединенную сеть

Протокол RIP

Основными характеристиками протокола RIP являются следующие.

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

Для выбора RIP в качестве протокола маршрутизации используется команда router пр. Команда network назначает маршрутизатору MAC-адрес, к которому этот маршрутизатор непосредственно подсоединен. Процесс маршрутизации связывает интерфейс с соответствующим адресом и начинает обработку пакетов указанных сетях (рис. 1.18).

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

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

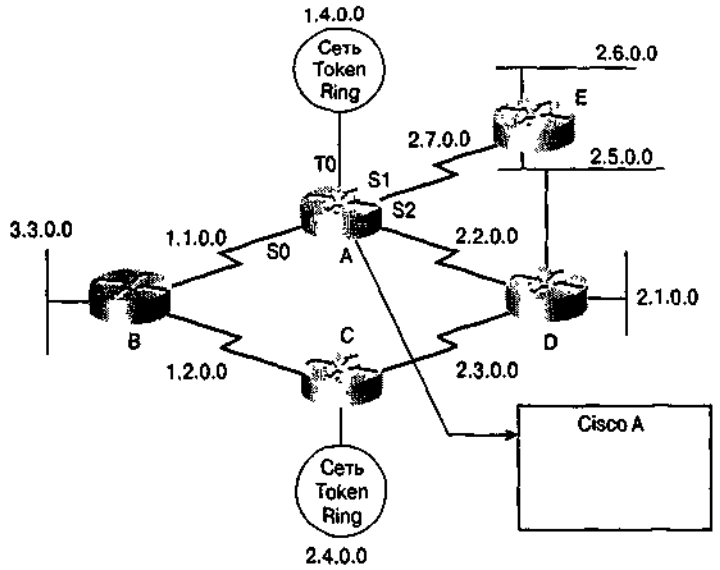


Рис. 1.18. Сообщения об изменениях маршрутизации позволяют маршрутизатору узнать текущую топологию сети

Транспортный уровень

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

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

Услуги транспортного уровня также позволяют пользователям запросить надежную транспортировку данных между хостом и пунктом назначения. Для обеспечения надежной транспортировки используется ориентированная на соединение связь между системами, которые обме-

ниваются информацией. Применение надежной транспортировки позволяет следующее.

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

Сегментирование приложений верхнего уровня

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

Установка соединения

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

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

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

Рис. 1.19. Для того чтобы началась передача данных, как передающая, так и принимающая стороны должны проинформировать свои операционные системы о том, что будет установлена связь

Передача данных

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

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

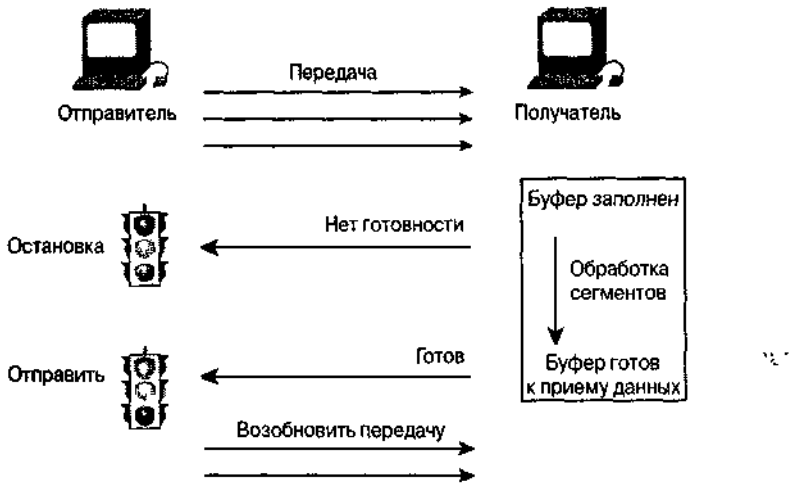


Рис. 1.20. Для того чтобы не допустить потери данных транспортный уровень может послать отправителю сигнал: "Не готов!"

Повышение надежности передачи путем создания окон

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

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

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

Способы подтверждения

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

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

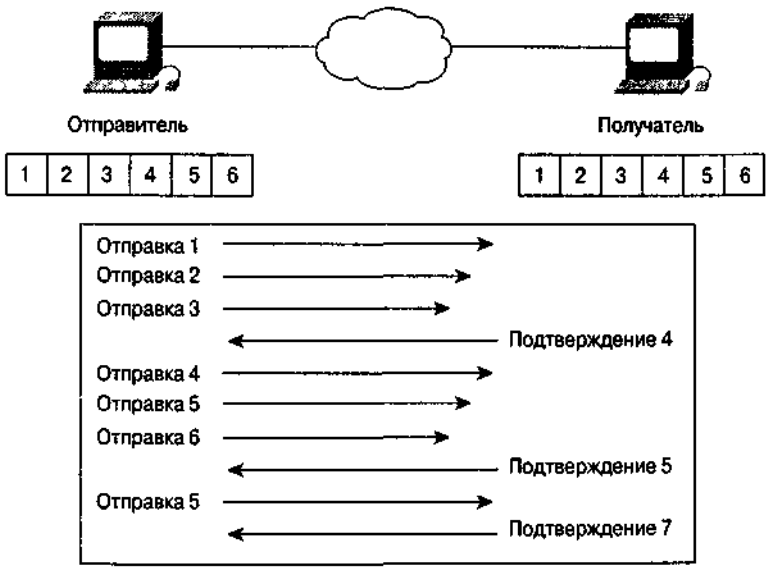


Рис. 1.21. Метод позитивного подтверждения требует, чтобы получатель обменивался информацией с источником путем отправки подтверждения при получении данных

Резюме

- За счет использования уровней Эталонная модель OSI упрощает обмен информацией между двумя компьютерами.
- Соответствующие протоколы каждого уровня обмениваются информацией, которую называют модулями данных протокола (PDU).
- Каждый уровень зависит от сервисных функций лежащего ниже него уровня Эталонной модели OSI. Нижний уровень использует инкапсуляцию для того, чтобы поместить PDU верхнего уровня в свое поле данных; после этого воз можно добавление заголовков и трейлеров, которые данный уровень использует для выполнения своих функций.
- Термин **Ethernet** часто используется по отношению ко всем CSMA/CD локальным сетям, которые работают в соответствии со спецификациями Ethernet, включая сеть IEEE 802.3.
- Каналы Ethernet и 802.3 обеспечивают транспортировку данных по физическому каналу, который соединяет какие-либо два устройства.
- Протокол IP обеспечивает негарантированную маршрутизацию дейтаграмм без установления логической связи. Сеть Ethernet не анализирует содержимое дейтаграмм, а лишь ищет способ передать дейтаграмму к ее месту назначения.
- Сообщения ICMP переносятся в IP-дейтаграммах и используются для передачи управляющих сообщений и сообщений об ошибках.
- Протокол АКР используется для преобразования известного IP-адреса в MAC-адрес с целью обеспечения возможности коммуникации в среде множественного доступа, например, такой как Ethernet
- При осуществлении коммутации маршрутизатор принимает пакет на одном интерфейсе и направляет его на другой.
- Протоколы маршрутизации обеспечивают наличие в адресе сетевого уровня достаточной информации для отправки пакета от одного хоста к другому, опираясь на схему адресации.
- Протокол маршрутизации поддерживает маршрутизируемый протокол, создавая при этом механизм совместного использования данных маршрутизации. Сообщения протоколов маршрутизации перемещаются между маршрутизаторами.
- Большинство протоколов маршрутизации относятся к одному из двух типов: дистанционно-векторные или протоколы состояния каналов связи.
- Маршрутизаторы должны быть способны обрабатывать пакеты, инкапсулированные в различные фреймы низкого уровня без изменения адресации 3-го уровня.
- Примерами IP-протоколов маршрутизации могут служить RIP, IGRP, OSPF и EIGRP.
- Службы транспортного уровня дают возможность пользователям запросить надежную транспортировку данных между источником и пунктом назначения.

Контрольные вопросы

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

1. Какой уровень эталонной модели OSI наилучшим образом описывает стандарты lOBaseT?

   A. Канальный.

   B. Сетевой.

   C. Физический.

   D. Транспортный.

2. Какое из приведенных ниже утверждений наилучшим образом описывает функции транспортного уровня эталонной модели OSI?

A. Он посылает данные, используя управление потоком.

B. Он обеспечивает наилучший путь для доставки.

C. Он определяет сетевые адреса.

D. Он делает возможной сетевую сегментацию.

3. Какая из следующих функций используется маршрутизатором для пересылки » пакетов данных между сетями?

A. Приложение и передающая среда.

B. Определение пути и коммутация.

C. Широковещание и обнаружение коллизий.

D. Никакая из упомянутых выше.

4. Какие из перечисленных ниже являются основными типами динамической маршрутизации?

A. Статический и по умолчанию.

B. TCP- и UDP-обмен.

C. Дистанционно-векторный и канальный.

D. Никакие из вышеперечисленных.

5. В случае, когда все маршрутизаторы в сети работают с одной и той же инфор мацией о топологии сети, то о сети говорят как о...

A. конвергированной.

B. формализованной.

C. реконфигурированной.

D. ничто из вышеперечисленного.

6. Опишите цель инкапсуляции данных

7. Опишите главную функцию транспортного уровня эталонной модели OSI.

8. Опишите цель использования протокола ICMP.

9. Опишите процедуру создания окон в протоколе TCP/IP.

10. Опишите главную функцию сетевого уровня эталонной модели OSI.

Основные термины

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

IP-адрес (IP-address). 32-разрядный адрес, назначаемый хосту в протоколе TCP/IP. IP-адрес принадлежит к одному из пяти классов (A, B, C, D или E) и представляется в десятичном формате в виде четырех октетов, разделенных точками. Каждый адрес состоит из номера сети, необязательного номера подсети и номера компьютера. Номера сети и подсети используются для

маршрутизации, а номер компьютера — для адресации уникального хоста в сети или подсети. Маска подсети используется для выделения информации о сети и подсети из IP адреса. IP-адрес также называется Internet-адресом (Internet address).

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

Динамическая маршрутизация(4упапис routing). Маршрутизация, которая автоматически подстраивается под топологию сети или под изменения в потоке данных. Также называется адаптивной маршрутизацией *(adaptive routing).*

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Подсеть (subnetwork). Часть базовой сети передачи данных.

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

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

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

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

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

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

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

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

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

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

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

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

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

Сетевой уровень (network layer). Третий уровень эталонной модели OSI. Уровень, на котором происходит маршрутизация. Обеспечивает соединение и выбор пути между двумя конечными системами. Примерно соответствует уровню контроля пути в модели SNA.

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

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

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

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

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

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

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

также метод получения разрешения на передачу.

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

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

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

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

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

Ключевые темы этой главы

- Рассматриваются различные проблемы, возникающие в локальных сетях, такие как:
  - коллизии
  - использование метода CSMA/CD
  - требования мультимедийных приложений к сети
  - нормальная латентность
  - расстояния и повторители
  - избыточное широковещание
- Описываются дуплексная передача и стандарт Fast Ethernet как два способа улучшения показателей LAN
- Анализируется влияние сегментации с использованием мостов, маршрутизаторов и коммутаторов на работу локальных сетей
- Описывается процесс коммутации
- Описывается коммутация в локальных сетях и ее преимущества
- Описывается протокол распределенного связующего дерева
- Обсуждаются достоинства виртуальных локальных сетей

Глава 2

Коммутация в локальных сетях

Введение

В настоящее время проектировщики сетей все чаще отказываются от использования мостов и концентраторов и при создании сети в первую очередь используют коммутаторы и маршрутизаторы В главе 1, "Эталонная модель OSI и маршрутизация", приведен обзор эталонной модели OSI и процесса планирования сети, а также рассмотрены требования к сети, связанные с использованием маршрутизации.

В настоящей главе обсуждаются проблемы, возникающие в локальных сетях, и воз-можные способы повышения их эффективности. Далее объясняется что такое переполнение LAN, описывается его влияние на производительность LAN и рассматриваются преимущества сегментации сети Кроме того, описываются достоинства и недостатки применения мостов, коммутаторов и маршрутизаторов для сегментации LAN, а также рассматривается влияние коммутации, маршрутизации и применения мостов на пропускную способность локальных сетей В заключение описываются сети Ethernet, Fast Ethernet, виртуальные сети и рассматриваются достоинства каждой из этих технологий.

Требования к сетям

Сегодняшние локальные сети становятся все более перегруженными и в них все чаще происходит переполнение. Кроме постоянно растущего числа пользователей есть и некоторые другие факторы, которые в совокупности потребовали расширения возможностей традиционных локальных сетей. Среди них можно выделить следующие.

• Центральные процессоры (CPU), работающие с большими, чем ранее, скоростями. В середине 80-х годов рабочей станцией, как правило, являлся персональный компьютер. В то время большинство персональных компьютеров могло выполнять 1 миллион инструкций в секунду (million instructions per second, MIPS) В настоящее время типичной для рабочих станций является скорость от 50 до 75 MIPS; при этом значительно возросла скорость выполнения операций ввода/вывода (I/O). В результате этих изменений всего лишь две рабочие станции могут исчерпать возможности локальной сети.

• Более скоростные операционные системы. Поскольку три наиболее часто используемые операционные системы (Windows, UNIX и Mac) являются многозадачными, пользователи могут начать несколько сетевых операций одновременно. После появления ОС Windows 95, расширявшей возможности операционных систем DOS/Windows и включающей многозадачность, пользователи персональных компьютеров повысили свои требования к сетевым ресурсам.

• Приложения, интенсивно использующие сеть. Использование **приложений типа** клиент/сервер, таких как World Wide Web, постоянно растет. Приложения такого типа позволяют администраторам централизовать обработку информации, облегчая ее хранение и защиту.

Приложения типа клиент/сервер освобождают пользователя от забот по поддержке информации и от расходов на достаточно емкий жесткий диск для ее сохранения. Учитывая значительный финансовый выигрыш, который дают приложения типа клиент/сервер, в будущем следует ожидать еще более широкого их распространения.

Интерфейс сетей типа Ethernet/802.3

Наиболее известной средой локальных сетей является **Ethernet.** Этот тип сети используется для обмена данными между сетевыми устройствами, такими как компьютеры, принтеры и файловые серверы. Как показано на рис. 2.1, в сетях Ethernet все устройства подсоединены к одной и той же передающей среде. В среде Ethernet используется метод **широковещания** фреймов данных для передачи и получения данных во всех узлах, подсоединенных к общей передающей среде.

На эффективность работы локальных сетей Ethernet/802.3 могут негативно повлиять несколько факторов.

- Широковещательный характер передачи фреймов данных.
- Метод множественного доступа с контролем несущей и обнаружением коллизий (carrier sense multiple access collision detect, CSMA/CD), который в каждый конкретный момент позволяет передавать данные только одной станции.
- Возможность возникновения затора в сети в связи с возросшими требованиями к ширине полосы пропускания со стороны мультимедийных приложений, таких как видео и Internet.
- Латентность (задержка распространения) фреймов во время прохождения передающей среды 1-го уровня LAN и 1-го, 2-го и 3-го уровней сетевых устройств.
- Увеличение расстояний между устройствами сети Ethernet/802.3 за счет применения повторителей на 1-м уровне.

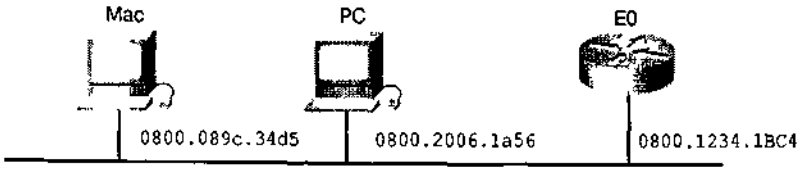


Рис. 2.1. В сетях Ethernet используется технология совместного доступа к среде для передачи данных между устройствами

Сеть Ethernet, использующая CSMA/CD и общую передающую среду, может поддерживать скорости передачи до 10 Мбит/с. CSMA/CD представляет собой метод доступа, при котором в каждый конкретный момент может передавать только одна станция. Целью Ethernet является обеспечение негарантированной доставки и предоставление всем устройствам, подключенным к общей среде, равного права на передачу. Как показано на рис. 2.2, одной из присущих CSMA/CD проблем является возможность возникновения коллизий.

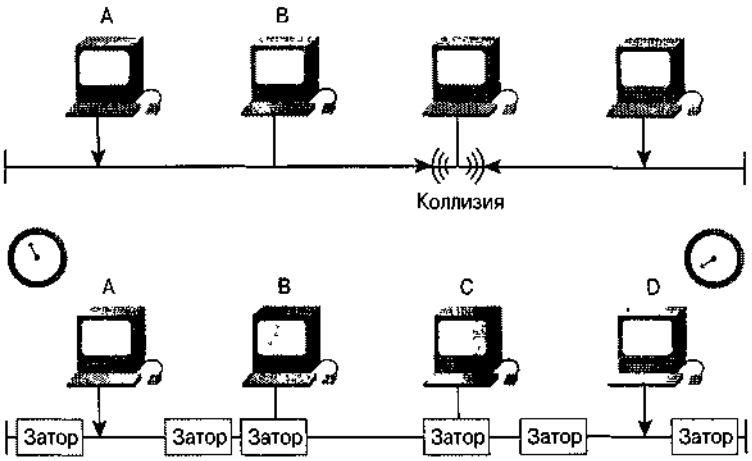


Рис. 2.2. CSMA/CD представляет собой метод доступа, который в каждый конкретный момент времени позволяет передавать лишь одной станции, что уменьшает вероятность коллизий

Полудуплексный Ethernet

Ethernet представляет собой **полудуплексную (half-duplex)** технологию. Каждый хост Ethernet перед отправкой данных проверяет сеть на предмет происходящей в ней передачи данных; если идет передача, то отправка данных этого хоста откладывается. Однако после этой отсрочки два или более хостов могут вновь начать передачу одновременно, что приводит к коллизии (столкновению). Если происходит коллизия, то хост переходит в состояние ожидания и позже пытается вновь вести передачу. По мере того как к сети подключаются все новые хосты, вероятность коллизий возрастает.

Возможности локальной сети могут быть исчерпаны вследствие того, что пользователи работают с интенсивно загружающим сеть программным обеспечением, таким как приложения типа клиент/сервер, которые обращаются к хостам чаще и в течение более длительного периода времени, чем обычные приложения. Физическое соединение, используемое устройствами локальной сети Ethernet, обеспечивает создание нескольких каналов, что делает возможным обмен информацией между несколькими устройствами.

Затор в сети и ширина полосы пропускания

Технологический прогресс приводит ко все большему увеличению скорости и мощности персональных компьютеров и рабочих станций. Сочетание более мощных компьютеров/рабочих станций и интенсивно использующих сеть приложений вызвало потребность в увеличении пропускной способности сети (называемой также **шириной полосы пропускания** или просто **полосой пропускания, bandwidth),** большей чем 10 Мбит/с, которую предоставляют сети совместного пользования Ethernet/802.3.

В сегодняшних сетях значительно возрастает объем передачи больших графических файлов, видеофильмов и мультимедийных приложений, а также быстро растет количество пользователей. Все эти факторы еще больше увеличивают нагрузку на пропускную способность сетей Ethernet, составляющую 10 Мбит/с .

По мере того как все большее количество потребителей совместно используют файлы большого объема и все чаще обращаются к файловым серверам, увеличивается вероятность затора (congestion) в сети. Это приводит к увеличению срока ожидания ответа и времени передачи файлов, что делает деятельность пользователей менее продуктивной. Для того чтобы уменьшить вероятность затора, необходимо увеличить ширину полосы пропускания или более эффективно использовать уже имеющуюся. Далее в настоящей главе описываются методы поиска такого рода решений

Латентность

Латентностью (latency) (иногда ее называют **задержкой распространения, propagation delay)** называется время, которое требуется фрейму или пакету данных для того, чтобы дойти от станции-источника или узла до пункта назначения в сети. Поскольку локальная сеть Ethernet использует метод CSMA/CD для обеспечения негарантированной доставки, система должна иметь некоторую латентность для обнаружения коллизий и обсуждения прав на передачу по сети.

Латентность зависит не только от расстояния и количества устройств. Например, если две рабочие станции разделены тремя коммутаторами, то латентность системы оказывается меньшей, чем если бы их разделяли два маршрутизатора. Промежуточные устройства, такие, например, как коммутаторы, значительно увеличивают эффективность работы сети,

Время передачи по сети Ethernet

Временем передачи называется время, которое требуется фрейму или пакету (данные помещаются в пакет или фрейм) для перемещения **от канального уровня (data link layer) до физического уровня (physical layer)** т.е. до физического кабеля сети. В табл. 2.1 приведено время передачи для четырех пакетов различного размера.

Таблица 2.1. Время передачи в **Ethernet**

Размер пакета в байтах	Время передачи в микросекундах
64	51,2
512	410
1000	800
1518	1214

Каждому Ethernet-биту для передачи предоставляется окно в 100 не. Один **байт** (byte) равен 8 **битам (bit)** Следовательно, для передачи одного байта требуется, как минимум, 800 не. Фрейму размером 64 байта для передачи требуется 51200 не или51,2 мкс (64 бита умноженные на 800 не дают 51200 не, а 51200, поделенные на 1000, дают 51,2 микросекунды). Время передачи пакета размером 1000 байт от первой рабочей станции на сервер или на вторую рабочую станцию составляет 800 микросекунд вследствие латентности устройств сети.

Расширение совместно используемой передающей среды LAN путем использования повторителей

Расстояние, на котором может работать локальная сеть, ограничено в связи с **затуханием (attenuation)** сигнала. Термин "затухание" означает, что сигнал ослабляется (затухает) при прохождении по сети. Затухание вызывается сопротивлением кабеля или другой передающей среды. **Повторителем (repeater)** в сети Ethernet называется сетевое устройство физического уровня, которое усиливает или регенерирует сигнал. Использование Ethernet-повторителя позволяет удлинить рабочее расстояние LAN и увеличить количество пользователей, как показано на рис. 2.3. Однако использование повторителей требует также разрешения вопросов широковещания, возникновения коллизий и в целом оказывает отрицательное воздействие на общую эффективность LAN с общей передающей средой.

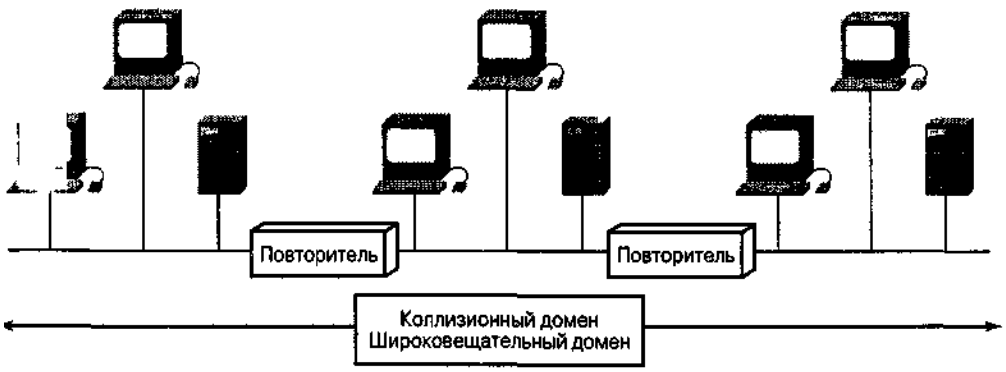


Рис. 2.3. Ethernet-повторитель позволяет вести только одну передачу в каждый конкретный момент; он соединяет все узлы в один коммуникационный канал и передает одни и те же данные на все порты следующего повторителя

Повторитель с несколькими портами называется также **концентратором, или хабом (hub).** В локальных сетях с общей передающей средой, в которых используются концентраторы, имеются проблемы широковещания и коллизий, а общая ширина пропускания локальной сети составляет 10 Мбит/с.

Повышение эффективности LAN

Эффективность LAN может быть повышена путем использования одного или двух из приведенных ниже решений:

- использование дуплексной топологии Ethernet;
- сегментация LAN

Дуплексный Ethernet

Дуплексный Ethernet (full-duplex) позволяет одновременно отправлять пакет и при этом получать другой Для осуществления одновременной передачи и приема требуются две пары кабелей и коммутируемое соединение между всеми узлами Такое соединение рассматривается как непосредственное, типа "точка-точка" и практически гарантирует отсутствие коллизий Поскольку оба узла могут передавать и получать данные в одно и то же время, вопрос об использовании полосы пропускания не обсуждается Дуплексный Ethernet может использовать существующую общую среду до тех пор, пока она удовлетворяет минимальным стандартам Ethernet:

Стандарт	Расстояние
10BaseT/1 OBaseTX	100 метров
10BaseFL	2 километра

Для осуществления одновременной передачи и приема каждому узлу требуется назначенный только ему **порт (port)** Для создания соединений типа "точка-точка" с использованием дуплексного метода могут использоваться стандарты lOBaseT, 100BaseT или 100Base FL Для обеспечения всех возможностей дуплексного метода на обоих концах требуются **сетевые адаптеры (network interface card,** NIC)

В этой конфигурации использование двух пар кабелей позволяет дуплексному Ethernet-коммутатору создать непосредственное соединение между передатчиком (TX) на одном конце цепи и приемником (RX) на другом конце При таком соединении двух станций образуется домен, свободный от коллизий, поскольку передача и прием данных происходят по отдельным, не конкурирующим между собой каналам

Ethernet обычно использует только 50-60% максимально возможной полосы пропускания в 10 Мбит/с по причине латентности и коллизий Дуплексный Ethernet предоставляет возможность использовать полосу пропускания на 100% в обоих направлениях Таким образом потенциально обеспечивается пропускная способность в 20 Мбит/с, из которых 10 Мбит/с используются для передачи и 10 Мбит/с для приема

Сегментация в LAN

Сеть может быть подразделена на участки меньшего размера, которые называют **сегментами (segment)** Каждый сегмент использует метод доступа CSMA/CD и поддерживает поток данных между пользователями этого сегмента На рис 2 4 приведен пример сегментированной Ethernet-сети В целом сеть состоит из 15 компьютеров (6 файл-серверов и 9 PC) Если разделить эту сеть на сегменты, то при коммуникации внутри сегмента на одни и те же 10 Мбит/с будет приходиться меньшее количество пользователей/устройств Как показано на рис 2 5, каждый

сегмент рассматривается как отдельный **коллизионный домен (collision domain)**

Разделив всю сеть на три сегмента, сетевой администратор может уменьшить вероятность переполнения внутри каждого из них При передаче данных внутри сегмента все пять устройств делят между собой полосу пропускания сегмента шириной 10 Мбит/с В сегментированной локальной сети Ethernet данные, прошедшие по сегменту, передаются в сетевую **магистраль (backbone)** с помощью **мостов (bridge), маршрутизаторов (router)** или **коммутаторов (switch)**

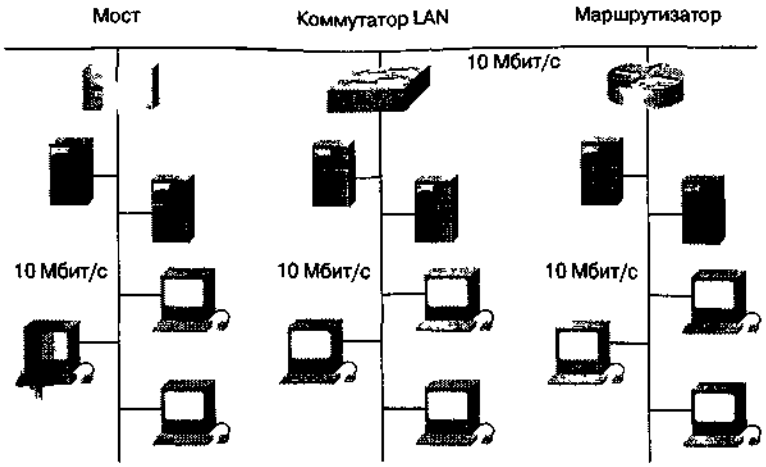


Рис 2 4 В несегментированной сети всем 15 устройствам пришлось бы использовать одну и ту же полосу пропускания в 10 Мбит/с и находиться в одном и том же коллизионном домене

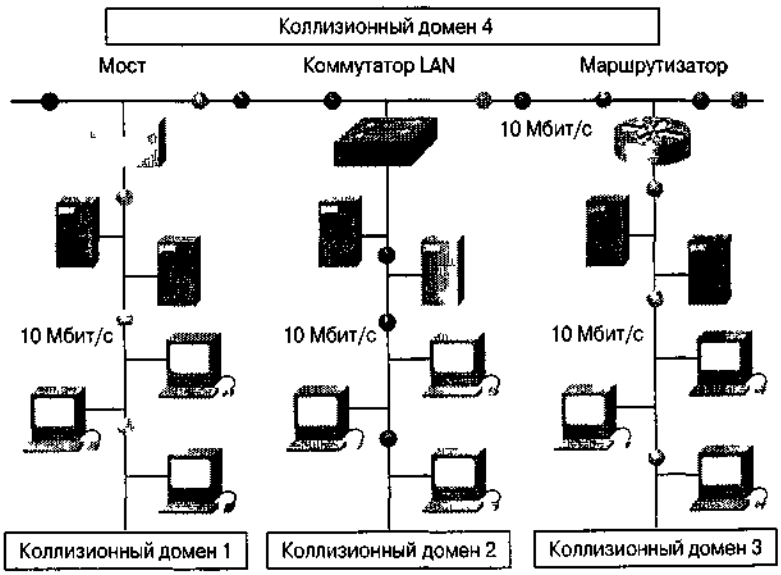


Рис 25 Магистральная сеть представляет собой отдельный коллизионный домен и использует CSMA/CD для осуществления негарантированной доставки данных из одного сегмента в другой

Сегментация с использованием мостов

Локальная сеть Ethernet, использующая для сегментации мосты, обеспечивает большую ширину пропускания в расчете на одного пользователя, поскольку на один сегмент приходится меньше пользователей И наоборот, локальные сети, в которых мосты не используются, обеспечивают меньшую полосу пропускания, поскольку в несегментированной LAN оказывается больше пользователей

Мосты "изучают" характер расположения сегментов сети путем построения адресных таблиц (рис. 2.6), в которых содержатся адреса всех сетевых устройств и сегментов, необходимых для получения доступа к данному устройству. Мосты являются устройствами 2-го уровня, которые направляют фреймы данных в соответствии с MAC-адресами фреймов (Media Access Control, MAC). Отметим, что мосты являются "прозрачными" для всех остальных устройств сети.

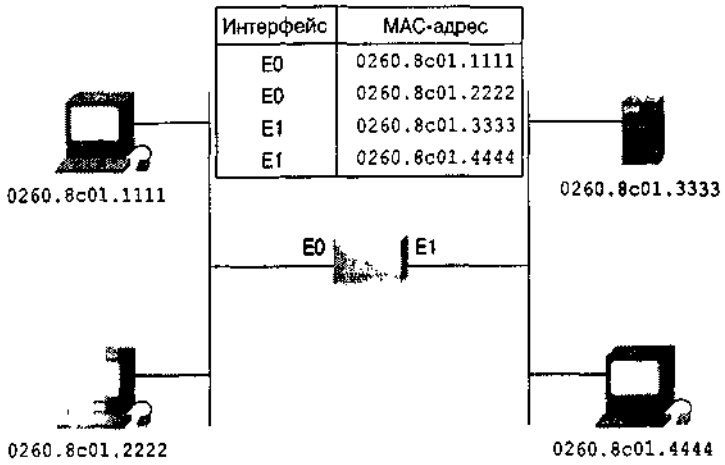


Рис. 2.6. Мост направляет дальше только фреймы, пункт назначения которых лежит вне данного сегмента

Мосты увеличивают латентность сети на 10-30%. Это увеличение латентности связано с тем, что мосту при передаче данных требуется дополнительное время на принятие решения. Мост рассматривается как устройство с функциями хранения и дальнейшей отправки, поскольку он должен проанализировать поле адреса пункта назначения фрейма, а затем решить, на какой **интерфейс (interface)** направить данный фрейм. Для выполнения этих операций требуется некоторое время, что замедляет процесс передачи и увеличивает латентность.

Сегментация с использованием маршрутизаторов

Маршрутизаторы представляют собой более современные устройства, чем обычные мосты. Мост является пассивным элементом сети и действует на уровне канала связи. Маршрутизатор действует на **сетевом уровне (network layer)** и в своих решениях относительно направления данных между сегментами опирается на адреса протокола сетевого уровня. Как показано на рис. 2.7, маршрутизаторы дают наивысший уровень сегментации, направляя данные на концентратор, к которому подсоединены рабочие станции. Маршрутизатор принимает решение о выборе сегмента для передачи данных, анализируя адрес пункта назначения, содержащийся в пакете данных, и используя **таблицу маршрутизации (routing table)** для выработки направляющих инструкций.

Для того, чтобы определить наилучший путь следования пакета к пункту назначения маршрутизатору требуется изучить полученный пакет. Этот процесс требует времени. Протоколы, требующие для каждого пакета **подтверждения (acknowledgement)** адресатом его получения (известные как **протоколы, ориентированные на подтверждение, acknowledgement-oriented protocols),** имеют сниженную на 30—40% производительность.

Протоколы, требующие минимального подтверждения (протоколы **скользящего окна, sliding-window protocols),** вызывают потерю пропускной способности на 20—30%. Это связано с уменьшением потока данных между отправителем и получателем (т.е. меньшего количества подтверждений).

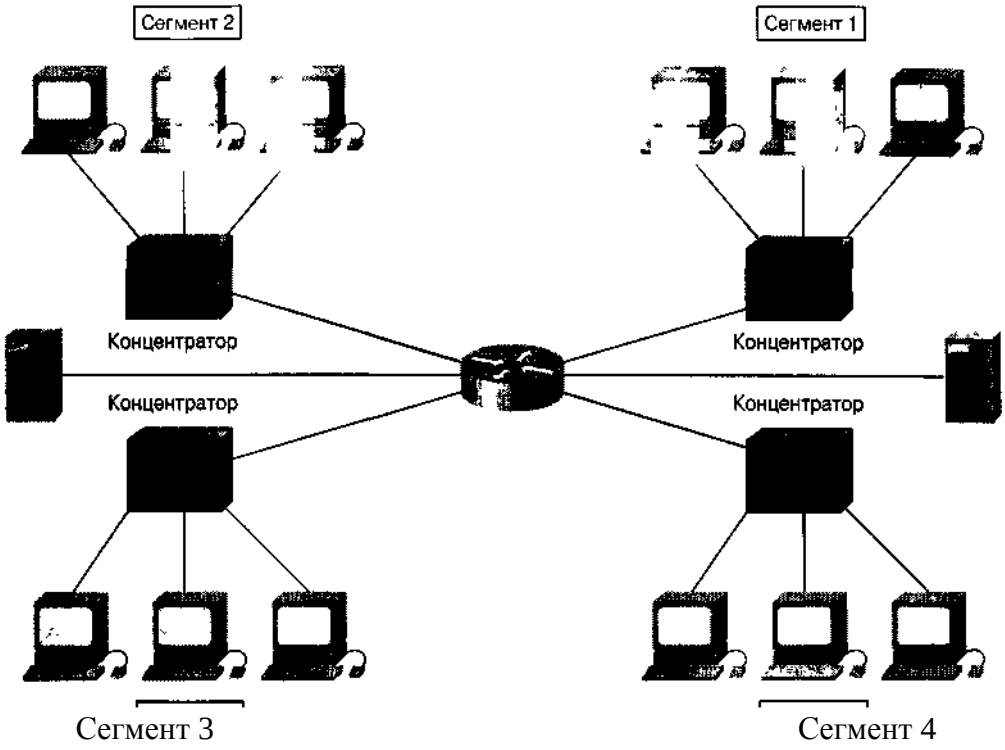


Рис. 2.7. Принцип сегментации с использованием маршрутизаторов

Сегментация с использованием коммутаторов

Использование **коммутации** (switching) в локальных сетях смягчает проблемы, связанные с недостаточной шириной полосы пропускания и с возможностью сетевых заторов, которые могут возникать, например, между несколькими PC и удаленным файл-сервером. Как показано на рис. 2.8, коммутатор разделяет локальную сеть на сегменты, т.е. делит единый коллизионный домен на отдельные домены, свободные от коллизий. Хотя LAN-коммутатор устраняет возможность коллизий между доменами, хосты, находящиеся внутри сегмента, по-прежнему остаются в одном коллизионном домене. Вследствие этого все узлы, подключенные к коммутатору, могут получить широковещательный сигнал всего от одного узла.

Технология коммутируемого Ethernet (Switched Ethernet) базируется на типовом Ethernet. При ее использовании каждый узел непосредственно соединен с одним из портов коммутатора или с сегментом, который, в свою очередь, соединен с одним из портов коммутатора. Таким образом на коммутаторе создается соединение с полосой пропускания 10 Мбит/с между каждым узлом и соответствующим сегментом. Компьютер, непосредственно соединенный с коммутатором, имеет собственный коллизионный домен и полную полосу пропускания в 10 Мбит/с.

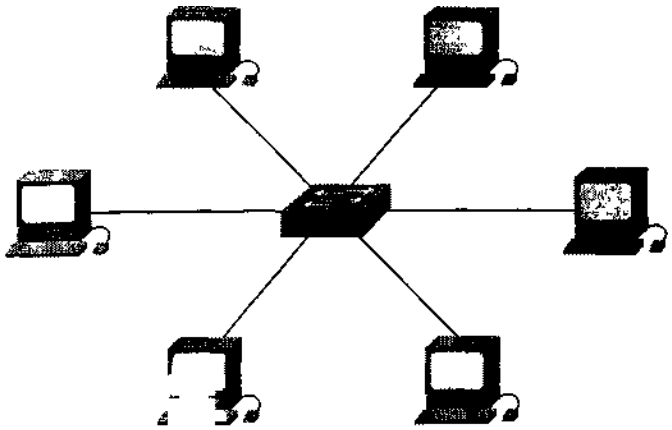


Рис. 2.8. LAN-KL і иутатор представляет собой высокоскоростной мост с несколькими портами, каждый из которых предназначен для одного узла или сегмента LAN

Локальная сеть, использующая топологию (topology) коммутируемого Ethernet, ведет себя так, как если бы она имела только два узла — узел отправителя и узел получателя. Этим двум узлам предоставляется полоса пропускания в 10 Мбит/с. Вследствие этого практически вся полоса пропускания может быть использована для передачи данных. За счет более эффективного использования полосы пропускания коммутируемый Ethernet обеспечивает более высокую скорость передачи, чем обычный Ethernet. В коммутируемом Ethernet доступная ширина полосы пропускания может достигать величины, близкой к 100%.

Коммутация в сети Ethernet увеличивает доступную полосу пропускания путем создания выделенных сегментов (т.е. соединений типа "точка-точка") и объединения этих сегментов в виртуальную сеть внутри коммутатора. Виртуальная сеть существует только тогда, когда двум узлам требуется обменяться информацией. Этим объясняется название виртуальный канал (virtual circuit) — он существует только при необходимости и создается внутри коммутатора.

Обзор применения коммутаторов и мостов

Коммутация представляет собой технологию, которая снижает вероятность переполнения в сетях Ethernet, Token Ring и FDDI (распределенный интерфейс передачи данных по оптоволоконным каналам, Fiber Distributed Data Interface) за счет уменьшения потока данных и увеличения ширины полосы пропускания. Коммутаторы часто используются в качестве замены концентраторов и предназначены для работы с существующими кабельными инфраструктурами. Они могут быть установлены без нарушения работы уже существующих сетей.

В настоящее время все виды коммутационного оборудования при обмене данными выполняют две основные операции.

- Коммутация фреймов данных. Она осуществляется при поступлении фрейма на входную точку в передающей среде и заключается в передаче его на выходную точку
- Поддержка операций по коммутации. Выполняя эту операцию, коммутатор создает и поддерживает таблицу коммутации.

Термин **мостовая технология (bridging)** относится к технологии, в которой устройство, известное как мост, соединяет два или более сегментов сети Ethernet. Мост передает дейтаграммы от источника в одном сегменте в пункт назначения в другом сегменте. Когда включается питание моста и начинается его функционирование, он исследует MAC-адреса поступающих дейтаграмм и создает таблицу известных пунктов назначения. Если мост обнаруживает, что пункт назначения дейтаграммы находится в том же самом сегменте, где и отправитель, то он отбрасывает эту дейтаграмму, поскольку в ее передаче нет необходимости.

Если мост обнаруживает, что получатель находится в другом сегменте, то он направляет дейтаграмму только в этот сегмент. Если мост не знает пункта назначения, то дейтаграмма рассылается во все сегменты, кроме сегмента отправителя (этот процесс называется **лавинной передачей, flooding).** Таким образом, первичное назначение моста состоит в ограничении движения потока данных определенными сегментами сети.

Как мосты, так и коммутаторы соединяют сегменты сети, используют MAC-адреса для определения сегмента, в который должна быть отправлена дейтаграмма, и уменьшают поток данных в сети. Преимущество коммутаторов состоит в том, что они работают значительно быстрее и могут выполнять дополнительные функции, такие как создание **виртуальных сетей (virtual** LAN, VLAN).

Латентность LAN-коммутаторов

Каждый коммутатор, используемый в локальной сети Ethernet, увеличивает ла-тентность сети. Однако правильный выбор метода коммутации позволяет нейтрализовать собственную латентность некоторых коммутаторов.

Коммутатор, находящийся между рабочей станцией и сервером, увеличивает время передачи на 21 микросекунду. Время передачи пакета размером 1000 байт составляет 800 микросекунд. Общее время передачи пакета с рабочей станции на сервер составляет 821 микросекунду (800+21=821). Рациональное использование коммутации выражается в том, что сразу считывается MAC-адрес пункта назначения и передача начинается до того, как весь пакет поступит на коммутатор. Это позволяет несколько скомпенсировать латентность коммутатора.

Коммутация 2-го и 3-го уровней

Существуют два метода коммутации фреймов данных — коммутация 2-го уровня и коммутация 3-го уровня. Коммутация состоит в получении приходящего фрейма на одном интерфейсе и отправке его через другой интерфейс. Для отправки пакета маршрутизаторы используют коммутацию 3-го уровня, в то время как коммутаторы используют для этого коммутацию 2-го уровня.

Различие между коммутацией 2-го и 3-го уровней состоит в типе информации, содержащейся внутри фрейма и используемой для определения нужного выходного интерфейса. При коммутации 2-го уровня фреймы коммутируются на основе MAC-адресов, а при коммутации 3-го уровня фреймы коммутируются на основе информации сетевого уровня.

В отличие от коммутации 3-го уровня, коммутация 2-го уровня не использует содержащуюся в пакете информацию сетевого уровня, а использует MAC-адрес пункта назначения, содержащийся внутри фрейма. Если он известен, то информация посылается по MAC-адресу пункта назначения. Коммутация 2-го уровня создает и поддерживает таблицу коммутации, в которой фиксируются MAC-адреса каждого порта или интерфейса.

Если коммутатору 2-го уровня не известен MAC-адрес пункта назначения, то производится широковещательная рассылка фрейма по всем портам сети для выяснения этого адреса. Если в результате такой рассылки фрейм достигает пункта назначения, то соответствующее устройство отсылает его обратно с указанием своего MAC-адреса, который добавляется коммутатором в его таблицу коммутации.

Адреса 2-го уровня задается производителем коммуникационного устройства. Эти уникальные адреса состоят из двух частей — кода производителя (manufacturing code, MFG) и уникального идентификатора. Каждому производителю его MFC-код назначается Институтом инженеров по электротехнике и электронике (Institute of Electrical and Electronic Engineers, IEEE). Уникальный идентификатор устройства задается производителем. Во всех сетях, кроме сетей системной сетевой архитектуры (Systems Network Architecture, SNA), пользователь не имеет или имеет мало возможностей влиять на адресацию 2-го уровня, потому что адреса 2-го уровня для конкретного устрой-

ства являются фиксированными, в то время как адреса 3-го уровня могут быть изменены. Адреса 2-го уровня образуют плоское (с отсутствием иерархии) адресное пространство, в котором каждый адрес уникален.

Коммутация 3-го уровня выполняется на сетевом уровне. При этом анализируется содержащаяся в пакете информация, после чего он направляется далее на основе адреса пункта назначения сетевого уровня. Коммутация 3-го уровня может сочетаться с маршрутизацией.

В большинстве случаев адрес 3-го уровня определяется сетевым администратором. Такие протоколы, как IP, IPX и AppleTalk используют адресацию 3-го уровня. Задавая адреса 3-го уровня, сетевой администратор создает локальные области, которым соответствует единый адресный блок (аналогичный почтовому адресу, состоящему из названия улицы, города, штата и страны). Каждой такой локальной области присваивается некоторый номер. Если пользователь переезжает в другое здание, то его конечные станции получают новые адреса 3-го уровня, но адреса 2-го уровня остаются теми же самыми.

Поскольку маршрутизаторы действуют на 3-м уровне эталонной модели OSI, они включены в иерархическую структуру адресации и сами создают ее. Следовательно, маршрутизированная сеть может связать логическую структуру адресации с физической инфраструктурой, например, посредством создания TCP/IP-подсетей или IPX-сетей для каждого сегмента. По этой причине поток данных в коммутированной (т.е. плоской) сети принципиально отличается от потока данных в маршрутизированной (т.е. иерархической) сети. Сети с иерархической структурой позволяют более гибко организовать поток данных, потому что они могут воспользоваться иерархией сети для определения оптимального пути и разделения широковещательных доменов.

Смысл коммутации 2-го уровня и 3-го уровня

Возросшая мощность процессоров и высокие требования приложений типа клиент/сервер и мультимедийных приложений вызвали потребность в большей ширине полосы пропускания в традиционных средах совместного пользования. Это побуждает проектировщиков сетей к замене в монтажных шкафах концентраторов на коммутаторы.

Для удовлетворения потребности в большей ширине полосы пропускания в локальных сетях коммутаторы 2-го уровня используют микросегментацию (microsegmentation). Это отчасти решает проблему, однако в настоящее время сетевые проектировщики столкнулись с возросшими требованиями к межсетевым коммуникациям.

Например, каждый раз, когда пользователь получает доступ к серверу и другим ресурсам, расположенным в различных подсетях, поток данных должен пройти через устройство 3-го уровня. Потенциально может образоваться затор, который угрожает нарушить работу сети. Для того чтобы избежать его возникновения, сетевой проектировщик может добавить дополнительные устройства 3-го уровня во всей сети, что снижает нагрузку на централизованные маршрутизаторы. Таким образом, коммутатор увеличивает ширину полосы пропускания, отделяя друг от друга коллизионные домены и избирательно направляя потоки данных на соответствующие сегменты сети.

Как LAN-коммутатор узнает адрес

Ethernet-коммутатор может узнать адрес каждого устройства в сети путем чтения адреса отправителя в каждом переданном пакете и отмечая порт, по которому пакет пришел на коммутатор. После этого коммутатор добавляет эту информацию к своей рассылочной базе данных. Адреса изучаются динамически. Это означает, что после чтения нового адреса он запоминается и хранится в **памяти, адресуемой по содержимому (content-addressed memory, CAM).** Если считан адрес отправителя, который отсутствует в CAM, то он запоминается и хранится для будущего употребления.

При каждой записи адреса в CAM отмечается момент его получения. Это позволяет хранить

адреса в течение определенного периода времени. При каждом обращении к адресу или поиске его в CAM его временная метка обновляется. Адреса, к которым не было обращений в течение определенного периода времени, удаляются из памяти. Посредством удаления устаревших адресов CAM поддерживает точную и функционально эффективную рассылочную базу данных.

Преимущества коммутации

Коммутаторы имеют много достоинств. LAN-коммутатор позволяет многим пользователям параллельно обмениваться информацией путем использования виртуальных цепей и выделенных сетевых сегментов в среде, свободной от коллизий. Таким способом достигается максимально возможная ширина полосы пропускания в общей передающей среде. Кроме того, переход к коммутируемой LAN весьма эффективен в финансовом отношении, поскольку позволяет вновь использовать существующее оборудование и кабели. В заключение следует добавить, что возможности коммутатора в сочетании с программным обеспечением для конфигурирования LAN предоставляют сетевому администратору гибкие средства управления работой сети.

Симметричная и асимметричная коммутация

Свойство симметрии при коммутации позволяет дать характеристику коммутатора с точки зрения ширины полосы пропускания для каждого его порта. Как показано на рис. 2.9, симметричный коммутатор обеспечивает коммутируемые соединения между портами с одинаковой шириной полосы пропускания, например, в случаях когда все порты имеют ширину полосы пропускания 10 Мбит/с или 100 Мбит/с.

Как показано на рис. 2.10, обеспечивает коммутируемые соединения между портами с различной шириной полосы пропускания, например, в случаях комбинации портов с шириной полосы пропускания 10 Мбит/с и 100 Мбит/с.

Асимметричная коммутация используется в случае наличия больших сетевых потоков типа клиент/сервер, когда многочисленные пользователи обмениваются информацией с сервером одновременно, что требует большей ширины пропускания для того порта коммутатора, к которому подсоединен сервер, с целью предотвращения затора на этом порте.

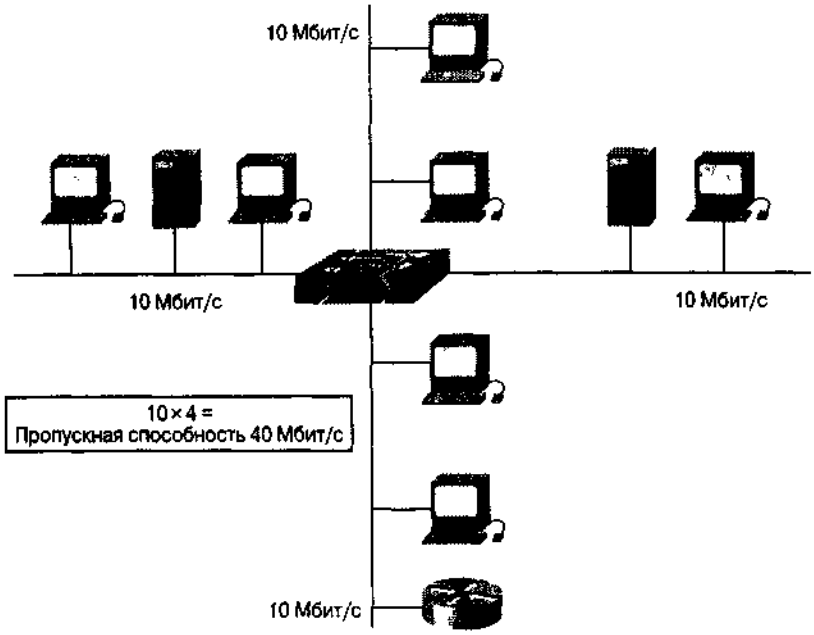


Рис. 2.9. Равномерное распределение потока данных по всей сети оптимизирует работу симметричного коммутатора

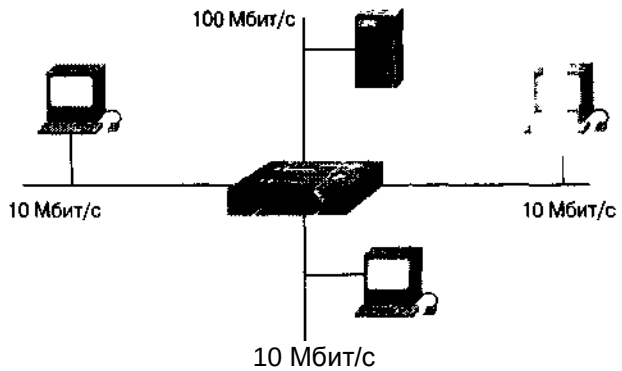


Рис. 2 10 Асимметричный коммутатор обеспечивает коммутируемые соединения между портами с шириной пропускания 10 Мбит/с и 100 Мбит/с

Как будет описано в следующем разделе, для того чтобы направить поток данных с порта 100 Мбит/с на порт 10 Мбит/с без опасности переполнения на последнем, асимметричный коммутатор должен иметь буфер памяти.

Буфер памяти

Для временного хранения пакетов и последующей их отправки по нужному адресу коммутатор может использовать **буфер памяти (memory buffer).** Так называется область памяти, в которой коммутатор хранит адреса пунктов назначения и передаваемые данные. Буфер памяти может использовать два метода хранения и отправки пакетов — буферизация по портам и буферизация с общей памятью.

При буферизации по портам пакеты хранятся в **очередях (queue),** которые связаны с отдельными входными портами. Пакет передается на выходной порт только тогда, когда все пакеты, находившиеся впереди него в очереди, были успешно переданы. При этом возможна ситуация, когда один пакет задерживает всю очередь из-за занятости порта его пункта назначения. Эта задержка может происходить даже в том случае, когда остальные пакеты могут быть переданы на откры-

тые порты их пунктов назначения.

При буферизации в общей памяти все пакеты хранятся в общем буфере памяти, который используется всеми портами коммутатора. Количество памяти, отводимой порту, определяется требуемым ему количеством. Такой метод называется **динамическим распределением буферной памяти.** После этого пакеты, находящиеся в буфере динамически распределяются по выходным портам. Это позволяет получить пакет на одном порте и отправить его с другого порта, не устанавливая его в очередь.

Коммутатор поддерживает карту портов, в которые требуется отправить пакеты. Очистка этой карты происходит только после того, как пакет успешно отправлен. Поскольку память буфера является общей, размер пакета ограничивается всем размером буфера, а не долей, предназначенной для конкретного порта. Это означает, что крупные пакеты могут быть переданы с меньшими потерями, что особенно важно при коммутации 10/100, т.е. когда порт с шириной полосы пропускания 100 Мбит/с должен отправлять пакеты на порт 10 Мбит/с.

Два метода коммутации

Для отправки фрейма через коммутатор могут быть использованы два метода:

• **Отправка с промежуточным хранением (store-and-forward).** Пакет должен быть получен полностью, прежде чем начнется отправка. При этом считываются ад реса пункта назначения и/или источника и перед отправкой используются фильтры. При получении фрейма проявляется латентность сети; эта латентность увеличивается для больших фреймов, поскольку для того, чтобы прочи тать весь фрейм, требуется больше времени. Вероятность обнаружения ошибок довольно высока, поскольку во время ожидания поступления всего фрейма имеется возможность поиска ошибок.

• **Сквозной метод (cut-through).** Коммутатор начинает считывать адрес пункта на значения и отправлять фрейм еще до полного его получения. Этот метод уменьшает латентность передачи, но имеет небольшую вероятность определе ния ошибок. Сквозная коммутация имеет две формы.

• Коммутация с быстрой отправкой (fast-forward switching) Коммутация с быстрой отправкой обеспечивает наименьшую латентность, поскольку отправка пакета начинается сразу после получения адреса пункта назначения. Поскольку при таком виде коммутации отправка начинается еще до полного получения пакета, возможны ситуации, когда пакет передается с ошибками Хотя такое происходит нечасто, а сетевой адаптер пункта назначения обычно отбрасывает пакеты с ошибками при получении, чрезмерный поток данных может оказаться в некоторых ситуациях неприемлемым. Для уменьшения числа пакетов, отправленных с ошибками, рекомендуется использовать метод коммутации без фрагментации. В режиме быстрой отправки латентность измеряется периодом времени от получения первого бита до его отправки, т.е. по принципу "первым пришел — первым ушел" (fust in, first out, FIFO).

• Коммутация без фрагментации (fragment-free switching). При коммутации без фрагментации отфильтровываются пакеты, попавшие в коллизию, которые составляют большинство ошибок при передаче, и только после этого начинается передача. В правильно работаюшей сети фрагменты, попавшие в коллизию должны иметь размер менее 64 байт. Пакеты размером более 64 байт являются действительными и обычно принимаются без ошибок. При коммутации без фрагментации пакет должен быть проверен на повреждение в результате коллизии до того, как он будет отправлен. При таком способе латентность также определяется принципом FIFO.

Латентность обоих способов коммутации определяется тем, когда коммутатор начинает отправку фрейма. Чем быстрее режим коммутации, тем меньше латентность коммутатора. Для ускорения отправки фрейма приходится сокращать время, отводимое на проверку ошибок. При этом качество проверки снижается, что может привести к большему количеству повторных передач.

Виртуальные сети (VLAN)

Коммутатор Ethernet физически сегментирует LAN на отдельные коллизионные домены. Однако каждый сегмент является частью одного широковещательного домена. Все сегменты коммутатора составляют один широковещательный домен. Это означает, что узел одного сегмента способен установить широковещательный режим на всех узлах всех сегментов.

Виртуальная сеть (virtual LAN, VLAN) представляет собой логическое объединение сетевых устройств или пользователей, не ограниченное одним физическим сегментом. Устройства или пользователи VLAN могут быть сгруппированы по выполняемым функциям, по принадлежности к одной организации, по характеру используемых приложений и т.д., независимо от их физического расположения в сегментах. VLAN создает единое широковещательное пространство, не ограниченное физическим сегментом, и его можно рассматривать как подсеть.

Создание VLAN производится в коммутаторе с помощью соответствующего программного обеспечения. VLAN не стандартизованы и требуют использования лицензионного программного обеспечения от производителя коммутатора.

Протокол распределенного связующего дерева

Главной функцией **протокола распределенного связующего дерева (Spanning-Tree Protocol, STP)** является создание дублирующих путей, в которых присутствуют мосты или коммутаторы, таким образом, чтобы не проявлялся эффект латентности, связанной с образованием в сети петель.

Мосты и коммутаторы принимают решения об отправке **однонаправленных фреймов (unicast frame)** на основе MAC-адреса пункта назначения, содержащегося во фрейме. Если MAC-адрес неизвестен, то устройство рассылает фрейм со всех портов, пытаясь достичь пункта назначения. Это делается также для всех широковещательных фреймов.

Алгоритм распределенного связующего дерева, реализованный в протоколе распределенного связующего дерева, предотвращает возникновение петель методом расчета устойчивой сетевой топологии распределенного связующего дерева. Для создания нечувствительной к ошибкам сети необходимо, чтобы между всеми узлами сети существовал путь без петель. Алгоритм распределенного связующего дерева используется для расчета такого пути. Древовидные фреймы, называемые **модулями данных мостового протокола (bridge protocol data units, BPDU)** отправляются и получаются всеми коммутаторами сети через равные промежутки времени и используются для создания топологии распределенного связующего дерева.

Коммутатор использует протокол распределенного связующего дерева во всех виртуальных сетях, основанных на технологиях Ethernet и **Fast Ethernet (быстрый Ethernet).** Этот протокол обнаруживает и разрывает петли путем перевода некоторых соединений в режим пассивного ожидания, который сменяется активным в случае разрыва активного соединения. В каждой сформированной виртуальной локальной сети работает свой экземпляр протокола распределенного связующего дерева для того, чтобы Ethernet-топологии всей сети отвечали производственным промышленным стандартам.

Различные состояния протокола распределенного связующего дерева

Протокол распределенного связующего дерева определяет несколько состояний виртуальной локальной сети.

- Блокировка — фреймы не отправляются, слышны BPDU.

- Прослушивание — фреймы не отправляются, прослушиваются фреймы.
- Анализ — фреймы не отправляются, изучаются адреса.
- Отправка — фреймы отправляются, изучаются адреса.
- Отключен — фреймы не отправляются, BPDU не слышны.

Для каждой VLAN состояние задается начальной конфигурацией, а при дальнейшей работе изменяется процедурами протокола STP. Состояние, затраты и приоритеты портов и виртуальных сетей можно определить с помощью команды `show spantree`. После того как установлено состояние "с порта на VLAN" протокол STP определяет, отправляет ли порт фреймы или блокирует их. Можно установить конфигурацию, при которой режим отправки протокола STP устанавливается сразу после установки соединения, а не в обычной последовательности: блокировка, прослушивание и последующая отправка. Возможность быстрого переключения состояний от блокировки к отправке вместо обычной последовательности переходных состояний полезна в ситуациях, когда требуется непосредственный доступ к серверу.

Резюме

- Появление более мощных компьютеров/рабочих станций и приложений, интенсивно использующих сеть, вызвало потребность в обеспечении полосы пропускания с шириной значительно большей, чем у типовой локальной сети Ethernet/802.3 LAN.
- Все большее количество пользователей используют сеть для совместной работы с большими файлами, обращаются к файловым серверам и к Internet, что часто приводит к переполнению сети.
- Сеть можно разделить на участки меньшего размера, называемые сегментами. Каждый сегмент представляет собой отдельный коллизионный домен.
- В сегментированной локальной сети Ethernet данные, пройдя по сегментам, направляются в сеть с помощью мостов, коммутаторов или маршрутизаторов.
- При использовании топологии коммутируемого Ethernet создается сеть, которая ведет себя так, как если бы она имела только два узла — передающий и принимающий.
- Коммутатор делит локальную сеть на микросегменты, создавая тем самым из единого коллизионного пространства несколько свободных от коллизий доменов.
- Коммутаторы обеспечивают высокую скорость передачи за счет чтения MAC-адреса пункта назначения (адреса 2-го уровня), во многом так же, как это делают мосты. Это значительно увеличивает скорость отправки пакетов.
- Ethernet-коммутация увеличивает доступную ширину полосы пропускания путем создания выделенных сегментов (соединений типа "точка-точка") и соединения этих сегментов в виртуальную сеть внутри коммутатора.
- В зависимости от ширины полосы пропускания каждого из портов коммутация может быть симметричной или асимметричной.
- Асимметричный коммутатор локальной сети обеспечивает коммутацию между портами с различной шириной полосы пропускания, например, 10 Мбит/с и 100 Мбит/с.
- Прохождение фрейма через коммутатор может происходить в двух режимах — в сквозном режиме и в режиме с промежуточным хранением.
- Виртуальная локальная сеть (VLAN) представляет собой логическое объединение нескольких пользователей или сетевых устройств, которое не ограничивается одним физическим сегментом.

• Главной функцией протокола распределенного связующего дерева является создание дублирующих путей с мостами или коммутаторами без увеличения латентности, которое может произойти из-за образования петель.

Контрольные вопросы

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

1. Какой из приведенных ниже методов широковещания используется передающей средой Ethernet для передачи и получения данных от всех узлов сети?
A. Пакеты.
B. Фреймы данных.
C. Сегменты.
D. По 1 байту.

2. Каково минимальное время, требуемое для передачи одного байта данных в сети Ethernet?
A. 100 наносекунд.
B. 800 наносекунд.
C. 51200 наносекунд.
D. 800 микросекунд.

3. Что из перечисленного ниже характеризует микросегментацию сети?
A. Выделенные пути между хостами отправителя и получателя.
B. Несколько путей передачи данных внутри коммутатора.
C. Одновременная видимость всего потока данных в сетевом сегменте?
D. Первый и второй варианты.

4. Коммутаторами Ethernet являются...
A. Повторители с несколькими портами на 1 уровне.
B. Концентраторы с несколькими портами на 2 уровне.
C. Маршрутизаторы с несколькими портами на 3 уровне.
D. Мосты с несколькими портами на 2 уровне.

5. Для чего оптимизируется асимметричная коммутация?
A. Для потока данных сети в случае, когда "быстрый" порт коммутатора подсоединен к серверу.
B. Для равномерного распределения потока данных в сети.
C. Для коммутаторов без буфера памяти.
D. Первый и второй варианты.

6. При_____коммутации коммутатор проверяет адрес получателя и сразу начинает отправку пакета, а при _____ коммутации коммутатор получает фрейм полностью перед последующей его отправкой.
A. С промежуточным хранением; симметричной.
B. Сквозной; с промежуточным хранением.
C. С предварительным хранением; сквозной.
D. С буфером памяти; сквозной.

7. Протокол распределенного связующего дерева позволяет...
A. маршрутизаторам обмениваться информацией о состоянии канала.
B. коммутаторам обмениваться информацией о количестве переходов.
C. мостам обмениваться информацией третьего уровня.
D. использовать дополнительные пути, без отрицательных эффектов от образования петель,

8. Опишите различие между сквозной коммутацией и коммутацией с промежуточным хранением.

9. Опишите дуплексный и полудуплексный режимы работы сети Ethernet.

10. Назовите основную функцию протокола распределенного связующего дерева.

Основные термины

Bridging. Технология, в которой мост соединяет два или более сегмента локальной сети.

Ethernet. Среда с общим доступом (локальная сеть с шинной топологией), поддерживающая номинальную скорость передачи данных до 10 Мбит/с, и использующая метод доступа CSMA/CD.

Fast Ethernet. Спецификации Ethernet для скоростей до 100 Мбит/с. Fast Ethernet предлагает десятикратную, по сравнению с lOBaseT, скорость, сохраняя при этом такие характеристики, как формат фрейма, механизмы MAC и MTU. Подобное сходство позволяет использовать в сетях Fast Ethernet существующие управляющие механизмы и приложения для сетей типа lOBaseT. Fast Ethernet базируется на расширении спецификации IEEE 802.3.

Unicast. Сообщение направленное единственному адресату.

Байт (byte). Ряд последовательных двоичных чисел, которые действуют как единое целое (например, байт, состоящий из 8 битов).

Бит (bit). Число в двоичной системе исчисления. Равно нулю или единице.

Буфер памяти (memory buffer). Область памяти, в которой коммутатор хранит передаваемые данные и адреса получателей.

Виртуальная локальная сеть (virtual LAN, VLAN). Группа устройств в локальной сети, которые сконфигурированы (с использованием управляющего программного обеспечения) таким образом, что они могут обмениваться информацией, как если бы они были соединены одним кабелем. В действительности они располагаются в разных сегментах локальной сети. Поскольку виртуальные сети основываются на логическом, а не физическом соединении, они являются чрезвычайно гибкими.

Виртуальный канал (virtual circuit). Логический канал, создаваемый для того, чтобы гарантировать надежную связь между двумя сетевыми устройствами. Виртуальный канал определяется парой VPI/VCI и может быть либо постоянным (PVC), либо коммутируемым (SVC). Виртуальные каналы используются в протоколах Frame Relay и X.25. В ATM виртуальный канал иногда обозначается аббревиатурой VC *(virtual channel).*

Дуплексная сеть Ethernet (full-duplex Ethernet). Сеть, обеспечивающая возможность одновременной двусторонней передачи данных между передающей и принимающей станцией.

Задержка распространения (propagation delay). Время, которое требуется данным, чтобы пройти по сети от источника до адресата. Также называется *временем задержки (latency).*

Затухание (attenuation). Ослабление коммуникационного сигнала.

Интерфейс (interface). 1. Соединение между двумя системами или устройствами. 2. В терминологии маршрутизации — сетевое соединение.

Коллизионный домен (collision domain). В сети Ethernet участок сети, в котором распространяются столкнувшиеся фреймы. Повторители и концентраторы не предотвращают распространение коллизий, а коммутаторы, мосты и маршрутизаторы создают отдельные коллизионные домены, которые локализуют область коллизий.

Коллизия (collision). В сети Ethernet коллизии происходят в результате одновременной передачи фреймов с двух узлов. При встрече в передающей среде фреймы обоих узлов сталкиваются и повреждаются.

Коммутатор (switch). Сетевое устройство, которое фильтрует, перенаправляет и рассылает фреймы на основе адресов пункта назначения каждого из них. Коммутаторы выполняют операции на уровне канала связи эталонной модели OSI.

Коммутация (switching). Процесс принятия входящего фрейма на одном интерфейсе и отправки его через другой.

Коммутация без буферизации пакетов (cut-through). Вид коммутации, при использовании которой данные проходят через коммутатор следующим образом: начало пакета появляется на ис-

ходящем порту до того, как пакет закончит прохождение входящего порта. Устройство, использующее этот вид коммутации, читает, обрабатывает и начинает передачу пакета сразу, как только узнает адрес и порт пункта назначения. Коммутация без буферизации пакетов известна также под названием *непрерывная коммутация (on-the-fly packet switching)* или *коммутация "на лету"*.

Коммутация без фрагментации (fragment-free switching). Методика коммутации, при которой до начала перенаправления отбрасываются столкнувшиеся фрагменты. Большинство из них являются поврежденными пакетами.

Коммутация с быстрой отправкой (fast-forward switching). Пакет перенаправляется немедленно после считывания адреса пункта назначения.

Коммутация с промежуточным хранением пакетов (store-and-forward). Методика коммутации пакетов, при которой фреймы полностью обрабатываются до отправки на порт передачи. Этот процесс включает в себя вычисление CRC и проверку адреса пункта назначения. Кроме того, фреймы должны временно храниться до тех пор, пока не появятся сетевые ресурсы для отправки сообщения (например, неиспользуемые каналы).

Концентратор (hub). Устройство, служащее центром сети с топологией типа "звезда" Также называется *многопортовым повторителем (multipart repeater).*

Лавинная передача (flooding). Передача мостом дейтаграмм всем сегментам кроме сегмента-источника.

Латентность или время ожидания (latency). Задержка между временем отправления запроса на доступ в сеть и временем получения разрешения на передачу.

Магистраль (mackbone). Соединяет все компоненты сети и обеспечивающая связь между ними.

Маршрутизатор (router). Устройство сетевого уровня, которое использует одну или несколько метрик для определения оптимального пути прохождения потока данных. Маршрутизаторы перенаправляют пакеты из одной сети в другую, основываясь на информации сетевого уровня. Иногда называются *шлюзами (gateway),* хотя это название все более устаревает.

Метод множественного доступа с контролем несущей и обнаружением коллизий (carrier sense multiple access collision detect, CSMA/CD). Механизм доступа, в котором устройства, готовые к отправке данных, сначала проверяют канал на наличие в нем передачи. Если она не обнаружена в течение заданного периода времени, устройство может начать передачу. Если два устройства передают одновременно, происходит коллизия, которая регистрируется устройствами, вовлеченными в конфликт. Для разрешения конфликта передача с этих устройств на некоторое время задерживается Сети Ethernet и IEEE 802.3 используют CSMA/CD.

Микросегментация (microsegmentation). Разделение сети на более мелкие сегменты. (Обычно осуществляется для увеличения полосы пропускания сетевых устройств)

Модуль данных мостового протокола (bridge protocol data unit, BPDU). Пакет приветствия протокола распределенного связующего дерева, посылаемый в интервалы времени, определенные конфигурацией протокола, для обмена информацией между мостами.

Мост (bridge). Устройство, которое соединяет два сегмента сети, использующих один протокол связи, и передает пакеты от одного сегмента к другому. Мосты работают на канальном уровне (второй уровень) эталонной модели OSI. Мост фильтрует, перенаправляет или рассылает широковещанием входящий фрейм, используя его MAC- адрес.

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

Память, адресуемая по содержимому (content-addressed memory, CAM). Память, которая поддерживает точную рабочую базу данных для последующей отправки пакетов.

Перегрузка (congestion). Поток данных, превышающий пропускную способность сети.

Повторитель (repeater). Устройство, которое восстанавливает и распространяет электрические сигналы между двумя сегментами сети.

Подтверждение (acknowledgment). Уведомление, посланное от одного сетевого устройства другому, чтобы подтвердить, что произошло некоторое событие (например, получение сообщения).

Иногда используется аббревиатура АСК

Полудуплексная сеть Ethernet (half-duplex Ethernet). Сеть, обеспечивающая возможность передачи данных между передающей и принимающей станцией в каждый конкретный момент только в одном направлении.

Порт (port). Интерфейс сетевого устройства (например, маршрутизатора). Разъем на распределительной панели, в который вставляется штекер такого же размера, например, штекер RJ-45. Чтобы соединить компьютеры, подключенные к распределительной панели, используются распределительные шнуры. Такая схема называется перекрестным соединением (кроссировка);она позволяет функционировать локальной сети.

Приложение типа клиент/сервер (client/server application). Приложение, которое хранится централизованно на сервере и используется рабочими станциями. За счет подобной организации облегчается обслуживание и защита приложений.

Протокол распределенного связующего дерева (Spanning-Tree Protocol). Мостовой протокол, который использует алгоритм распределенного связующего дерева и тем самым .позволяет мосту динамически обходить петли в топологии сети путем построения соответствующего дерева. Мосты обмениваются BPDU-сообшениями для нахождения петель, а затем удаляют эти петли, отключая выбранные интерфейсы мостов. Понятие Spanning-Tree Protocol обозначает два одноименных протокола: протокол стандарта ШЕЕ 802 1 и более ранний протокол Digital Equipment Corporation, на котором он основан. Версия IEEE поддерживает домены мостов и позволяет мосту построить беспетельную топологию в расширенной LAN. В целом версия IEEE предпочтительнее, чем разработка Digital.

Сегмент (segment). Участок сети, ограниченный мостами, маршрутизаторами или коммутаторами.

Сетевой адаптер (network interface card, NIC) Плата, обеспечивающая коммуникационные возможности компьютерных систем.

Сетевой уровень (network layer). Третий уровень эталонной модели OSI. Уровень, на котором происходит маршрутизация Обеспечивает соединение и выбор пути между двумя конечными системами Примерно соответствует уровню контроля пути в SNA модели.

Скользящее окно (sliding window). Окно, размер которого согласовывается динамически во время TCP-сеанса.

Таблица маршрутизации (routing table). Таблица, хранящаяся в маршрутизаторе или другом сетевом устройстве, которая содержит маршруты к определенным пунктам назначения в сети и, в некоторых случаях, метрики, связанные с этими маршрутами.

Топология (topology). Физическое расположение узлов сети и передающей среды внутри предприятия.

Узел (node). Конечная точка сетевого соединения. Общая точка двух или более линий в сети. Узлами могут быть процессоры, контроллеры или рабочие станции. Различные типы узлов, используемые для маршрутизации и для исполнения других функций, соединяются каналами и служат точками управления сетью. Термин *"узел "* иногда применяется по отношению к любому устройству, имеющему доступ в сеть. Слова "узел" и "устройство" часто взаимозаменяемы.

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

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

Ширина полосы пропускания , или полоса пропускания (bandwidth). Разность между наибольшими и наименьшими частотами, доступными для сетевых сигналов. Также номинальная

пропускная способность данной сетевой среды или протокола.

Широковещательный пакет (broadcast). Пакет данных, переданный всем узлам в сети. Идентифицируется широковещательными адресами.

Ключевые темы этой главы

- Объясняется, что представляет собой **виртуальная локальная сеть (virtual local access network, VLAN)**
- Объясняются причины появления виртуальных сетей и описываются их достоинства
- Описывается роль, которую играют коммутаторы в создании виртуальных сетей
- Описываются процессы фильтрации, идентификации фреймов и использования фреймовых тегов в виртуальных сетях
- Описывается совместное использование коммутаторов и концентраторов
- Перечисляются и описываются три метода разработки, виртуальных сетей

Глава 3

Виртуальные локальные сети

Введение

В"главе 2, "Коммутация в локальных сетях", обсуждались проблемы, которые мо-іуг возникать в локальных сетях, и возможные способы повышения эффективности и \ работы Были описаны достоинства и недостатки различных видов сегментации — с использованием **мостов (bridges), коммутаторов (switches) и маршрутизаторов (routers),** а также влияние коммутации, использования мостов и маршрутизации на пропускную способность сети В заключение были кратко описаны достоинства быстрого Ethernet и **виртуальных локальных сетей (virtual local-area network,** VLAN) Настоящая глава представляет собой введение в теорию виртуальных локальных сетей и их коммутируемых конфигураций, в ней также сравниваются традиционные конфигурации локальных сетей с коммутируемыми конфигурациями и обсуждаются преимущества использования коммутируемой архитектуры в локальных сетях

Обзор виртуальных локальных сетей

Как показано на рис 3 1, виртуальная локальная сеть представляет собой логическое объединение устройств или пользователей Объединение их в группу может производиться по выполняемым функциям, используемым приложениям, по отделам и т.д. , независимо от их физического расположения в **сегментах (segment)** Конфигурирование виртуальной сети производится на коммутаторе программным путем Виртуальные сети не стандартизированы и требуют использования программного обеспечения от производителя коммутатора

Существующие конфигурации локальных сетей совместного использования

Конфигурация типичной локальной сети определяется физической инфраструктурой соединения устройств, образующих сеть. Группировка пользователей осуществляется исходя из расположения их компьютеров по отношению к **концентратору (hub),** и основывается на структуре кабелей, ведущих к монтажному шкафу. Маршрутизатор, связывающий между собой все концентраторы, обычно осуществляет сегментацию сети и действует как широковещательный брандмауэр (broadcast firewall), в то время как сегменты, созданные коммутаторами, таким свойством не обладают. Такой тип сегментации при группировке не учитывает взаимосвязи рабочих групп и требования к ширине полосы пропускания. Вследствие этого они используют один и тот же сегмент и в равной степени претендуют на одну и ту же полосу пропускания, хотя требования к ней для различных групп и подразделений могут значительно различаться.

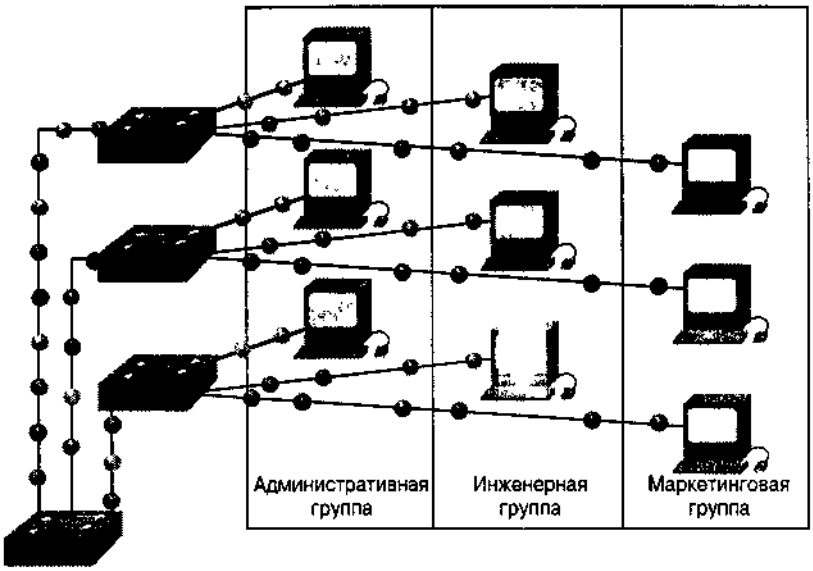


Рис. 3.1. Виртуальная сеть представляет собой группу устройств или пользователей, не ограниченную физическим сегментом сети

Сегментация с использованием архитектуры коммутаторов

Локальные сети все чаще подразделяют на рабочие группы, которые, будучи соединены через общие магистрали, образуют топологию виртуальной локальной сети. Виртуальная сеть логически сегментирует физическую инфраструктуру сети на отдельные подсети (в Ethernet они называются широковещательными доменами, broadcast domain). В образовавшейся виртуальной сети широковещательные фреймы коммутируются только между портами (port) этой сети.

В первоначальных реализациях виртуальных сетей использовалась разметка портов, которая объединяла в широковещательный домен устройства группы, выбираемые по умолчанию. Современные требования включают в себя необходимость расширения сферы действия виртуальной сети на всю сеть. Такой подход позволяет объединить географически разделенных пользователей посредством создания виртуальной локальной сети. Конфигурация виртуальной сети осуществляет скорее логическое, чем физическое объединение.

В настоящее время большинство устанавливаемых сетей обеспечивают весьма ограниченную логическую сегментацию. Как правило, пользователи группируются на основе соединений с совместно используемым концентратором и на распределении портов маршрутизатора между концентраторами. Такая топология обеспечивает сегментацию только между концентраторами, которые обычно расположены на разных этажах, а не между пользователями, компьютеры которых подсоединены к одному концентратору. Это накладывает физические ограничения на сеть и на возможности группировки пользователей. Некоторые виды сетевой архитектуры предоставляют возможность группировки, однако их возможности конфигурировать логически определенные рабочие группы ограничены.

Виртуальные сети и физические границы

В локальных сетях, содержащих коммутирующие устройства, использование технологии виртуальных сетей представляет собой эффективный и экономически выгодный способ объединения пользователей сети в рабочие группы независимо от их физического расположения. На

рис. 3.2 проиллюстрированы различия между сегментацией в виртуальной сети и в обычной локальной сети. Главными среди них являются следующие.

- Виртуальные сети работают на 2-м и 3-м уровнях эталонной модели OSI.
- Обмен информацией между виртуальными сетями обеспечивается маршрутизацией 3-го уровня.
- Виртуальная сеть предоставляет средство управления широковещанием.
- Включение пользователей в виртуальную сеть производится сетевым администратором.
- VLAN позволяет повысить степень защиты сети путем задания сетевых узлов, которым разрешено обмениваться информацией друг с другом.

Использование технологии виртуальных сетей позволяет сгруппировать порты коммутатора и подсоединенные к ним компьютеры в логически определенные рабочие группы следующих типов.

- Сотрудники одного отдела.
- Группа сотрудников с пересекающимися функциями.
- Различные группы пользователей, совместно использующих приложения или программное обеспечение.

Можно сгруппировать порты и пользователей в рабочую группу на одном коммутаторе или на нескольких соединенных между собой коммутаторах Группируя порты и пользователей вокруг нескольких коммутаторов, можно создать инфраструктуру сети в одном здании, в нескольких соединенных между собой зданиях или даже сеть большой области, как показано на рис. 3.3.

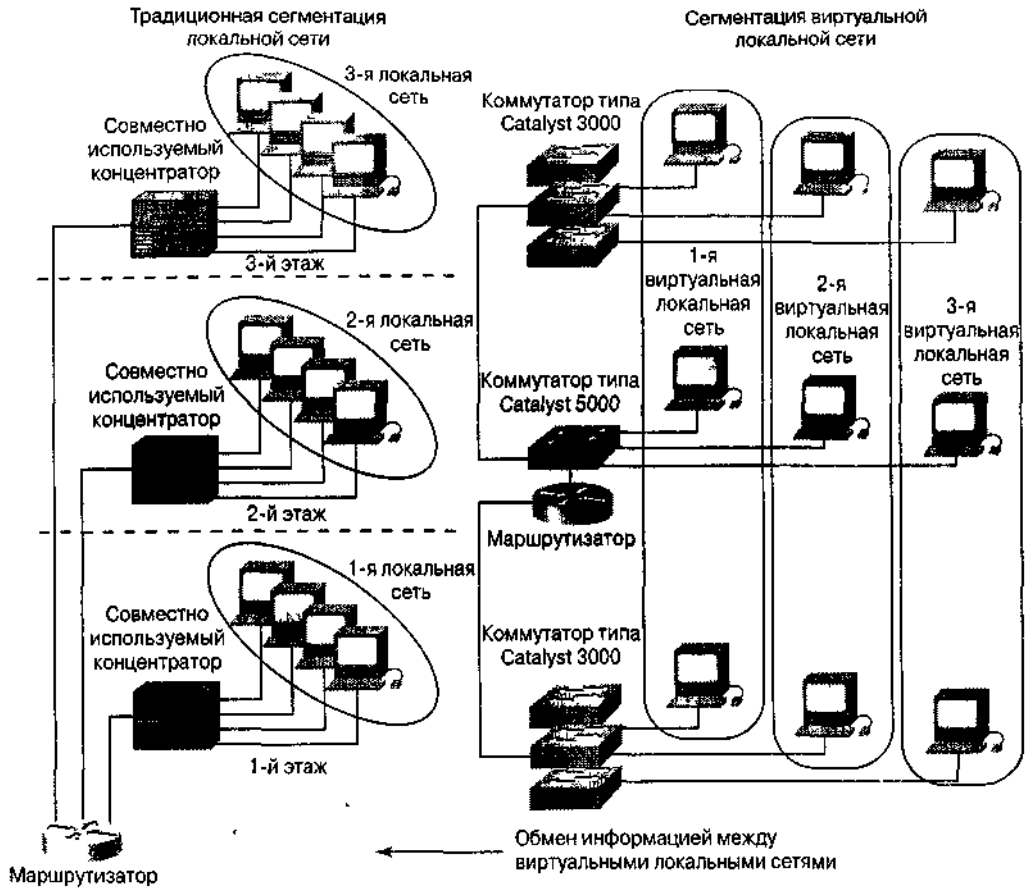


Рис 3 2 В коммутируемой сети создание виртуальной сети обеспечивает сегментацию и организационную гибкость

Транспортировка информации виртуальных сетей по корпоративной магистрали

Важной особенностью архитектуры виртуальных сетей является их способность передавать информацию между взаимосвязанными коммутаторами и маршрутизаторами, подключенными к корпоративной магистрали. Такая транспортировка делает возможным обмен информацией в рамках всего предприятия Благодаря транспортировке исчезают физические границы между пользователями, повышается гибкость конфигурационных решений при перемещении пользователей в другое место и становятся доступными механизмы, обеспечивающие взаимосвязанную работу компонентов магистральной системы

Магистраль обычно служит местом сбора больших потоков данных. Она также передает конечному пользователю информацию виртуальной сети и выполняет идентификацию коммутаторов, маршрутизаторов и непосредственно подсоединенных к магистрали серверов. В магистрали обычно используются мощные широкополосные каналы, обеспечивающие передачу потоков данных по всему предприятию

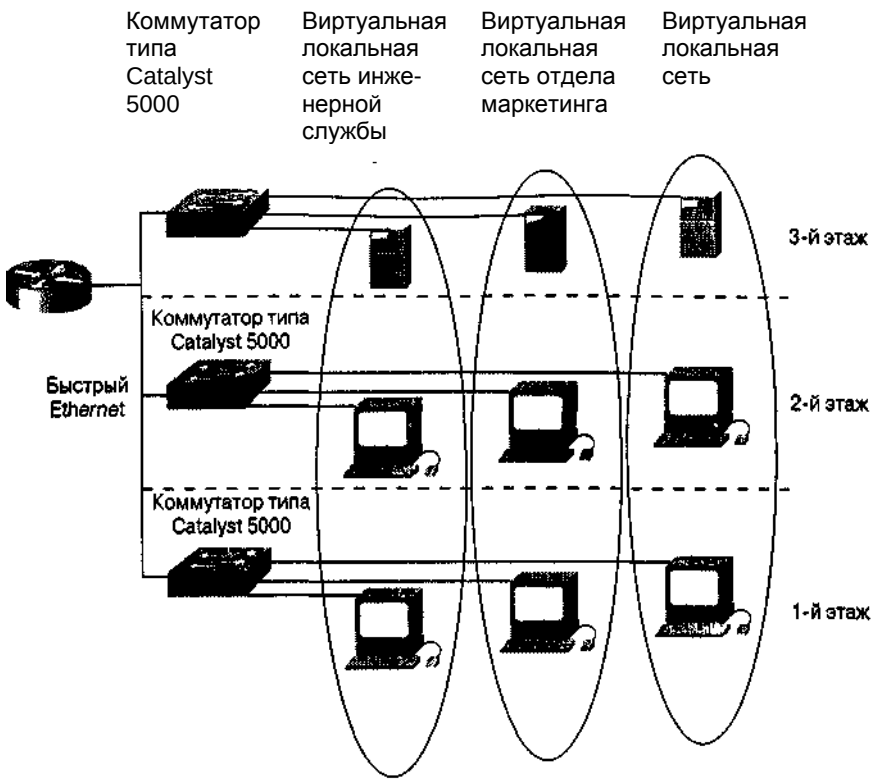


Рис 3.3. Использование виртуальных сетей позволяет ликвидировать ограничения на обмен информацией между рабочими группами

Маршрутизаторы в виртуальных сетях

Роль маршрутизаторов в виртуальных сетях отличается от их роли в обычных локальных сетях, заключающейся в создании брандмауэров (firewall), в управлении широковещанием, а также в обработке и распределении информации о маршрутах.

Маршрутизаторы остаются необходимыми и в коммутируемых архитектурах, в которых создана конфигурация виртуальной сети, поскольку они обеспечивают обмен информацией между логически определенными рабочими группами. Маршрутизаторы обеспечивают устройствам виртуальной сети доступ к совместно используемым ресурсам, таким как серверы и хосты. Они также обеспечивают связь с другими частями сети, которые логически сегментированы на осно-

ве традиционного подхода, основанного на выделении подсетей, или требуют доступа к удаленным серверам через каналы распределенных сетей Обмен информацией на 3-м уровне, осуществляемый в коммутаторе или обеспечиваемый извне, является необходимым элементом любой высокопроизводительной коммутационной архитектуры

Внешние маршрутизаторы могут быть с высокой финансовой эффективностью интегрированы в коммутируемую архитектуру путем использования одного или нескольких высокоскоростных магистральных соединений. Как правило, используются соединения FDDI, Fast Ethernet или ATM, которые обладают следующими преимуществами.

- Увеличенная пропускная способность соединений между коммутаторами и маршрутизаторами.
- Использование всех физических портов маршрутизатора, требуемых для обмена информацией между VLAN.
- Архитектура виртуальной локальной сети не только обеспечивает логическую сегментацию, но и значительно увеличивает эффективность работы сети.

Конфигурация коммутируемой сети

Проблемы, связанные с совместным использованием локальных сетей и появление коммутаторов побуждают к замене традиционных конфигураций локальных сетей на конфигурации коммутируемых виртуальных сетей. Эти коммутируемые конфигурации отличаются от традиционных конфигураций локальных сетей следующими особенностями.

- Коммутаторы устраняют физические ограничения, возникающие вследствие совместного использования концентратора, поскольку они логически группируют пользователей и порты всего предприятия. Вместо концентраторов в монтажных шкафах устанавливаются коммутаторы. Они не требуют изменений в расположении кабелей (или требуют незначительных) и могут полностью заменить совместно используемый концентратор с выделенными для каждого пользователя портами.
- Коммутаторы могут быть использованы для создания виртуальных сетей осуществляющих сегментацию. В традиционных конфигурациях локальных сетей сегментация осуществляется маршрутизаторами.

Коммутаторы являются основными компонентами, обеспечивающими обмен данными в виртуальных сетях. Как показано на рис. 3.4, в виртуальной сети они выполняют жизненно важные функции, являясь для устройств конечной станции точкой входа в среду коммутации, а также обеспечивают обмен данными в рамках всего предприятия.

Каждый коммутатор обладает способностью принимать решения о фильтрации и отправке фреймов (frame) на основе метрики виртуальной сети, определяемой сетевыми администраторами, а также способностью передавать эту информацию другим коммутаторам и маршрутизаторам сети.

Наиболее общими подходами к логической группировке пользователей в отдельные виртуальные сети являются фильтрация фреймов и их идентификация. Оба этих подхода характеризуются тем, что каждый фрейм исследуется при получении или отправке его коммутатором. Основываясь на наборе правил, определяемом администратором, коммутаторы определяют, куда будет передан фрейм, будет ли он фильтроваться или передаваться широковещательно. Эти механизмы контроля могут применяться администратором централизованно (с использованием программного обеспечения для управления сетью) и легко реализуются во всей сети.

При фильтрации фреймов исследуется индивидуальная информация каждого фрейма. Для каждого коммутатора создается таблица фильтрации; это обеспечивает высокий уровень административного контроля, поскольку становится возможным исследование многих атрибутов каждого фрейма. В зависимости от типа коммутатора локальной сети (LAN switch) группировка может производиться на основе адресов управления доступом к передающей среде (Media Ac-

cess Control address) или на основе протокола (protocol) сетевого уровня. Коммутатор сравнивает фильтруемые фреймы с элементами таблицы фильтрации и на этой основе предпринимает соответствующее действие.

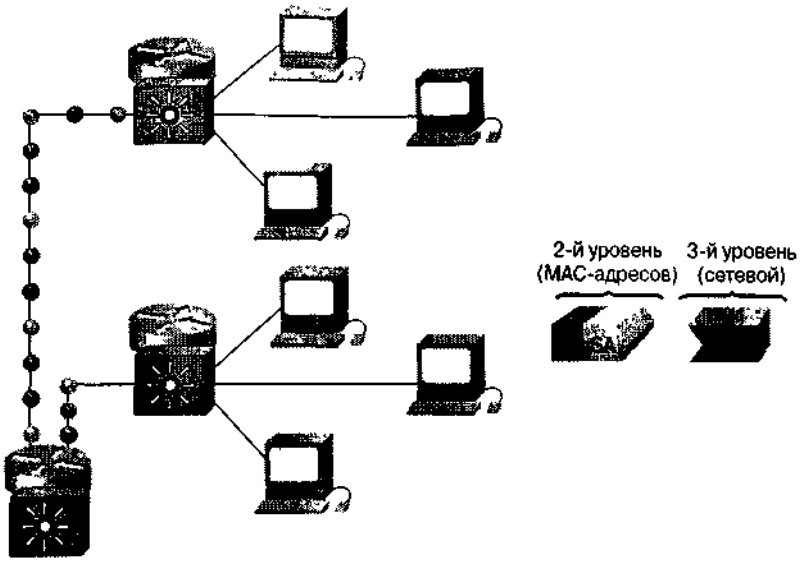


Рис. 3.4. Коммутаторы могут использоваться для группировки пользователей, портов или логических адресов в группы по интересам

Первоначально виртуальные сети базировались на фильтрах, а группировка пользователей основывалась на таблице фильтрации. Расширение такой модели было затруднительным, поскольку для каждого фрейма приходилось выполнять поиск в таблице фильтрации.

При использовании тегов (tag) каждому фрейму назначается уникальный, определяемый пользователем идентификатор. Такой метод был избран отделом стандартов **Института инженеров по электротехнике и электронике (Institute of Electrical and Electronic Engineers, IEEE)** по той причине, что он допускает расширяемость сети. Использование фреймовых тегов получает все большее признание в качестве стандартного механизма распределения портов; по сравнению с фильтрацией фреймов он обеспечивает большие возможности **расширения (scalability)** сети в пределах предприятия. Стандарт IEEE 802. lq регламентирует использование фреймовых тегов в качестве способа реализации виртуальной сети.

Использование фреймовых тегов при проектировании виртуальных сетей представляет собой подход, специально разработанный для коммутируемых коммуникаций. При использовании тегов в заголовок каждого фрейма при его отправке по сетевой магистрали помещается уникальный идентификатор. Этот идентификатор считывается и анализируется каждым коммутатором перед его широковещательной передачей или перед отправкой на другие коммутаторы, маршрутизаторы или устройства конечных станций. При выходе фрейма из сетевой магистрали и перед отправкой на конечную станцию коммутатор удаляет этот идентификатор из фрейма. Процесс идентификации фреймов происходит на 2-м уровне эталонной модели OSI и не требует большой обработки или обмена служебными сообщениями.

Различные варианты реализации виртуальных сетей

Виртуальная сеть представляет собой коммутируемую сеть, в которой выполнено логическое сегментирование по исполняемым функциям, используемым приложениям или по принадлежности пользователей к определенному отделу, вне зависимости от физического расположения, их компьютеров Каждый порт коммутатора может быть включен в виртуальную сеть. Все порты, включенные в одну виртуальную сеть принимают широковещательные сообщения, в то вре-

мя как порты, в нее не включенные, этих сообщений не принимают. Это повышает эффективность работы сети в целом. В последующих разделах обсуждаются три способа реализации виртуальных сетей, которые могут быть использованы для включения портов коммутаторов в виртуальную сеть: с центральным портом, статический и динамический.

Виртуальные сети с центральным портом

В виртуальных сетях с центральным портом (port-centric VLAN) все узлы виртуальной сети подключены к одному и тому же интерфейсу маршрутизатора. На рис. 3.5 показано семейство пользователей виртуальной сети, подключенных к порту маршрутизатора. Такое подключение облегчает работу администратора и повышает эффективность работы сети, поскольку:

- в виртуальной сети легко выполняются административные действия;
- повышается безопасность при обмене информацией между виртуальными сетями;

пакеты не "просачиваются" в другие домены.

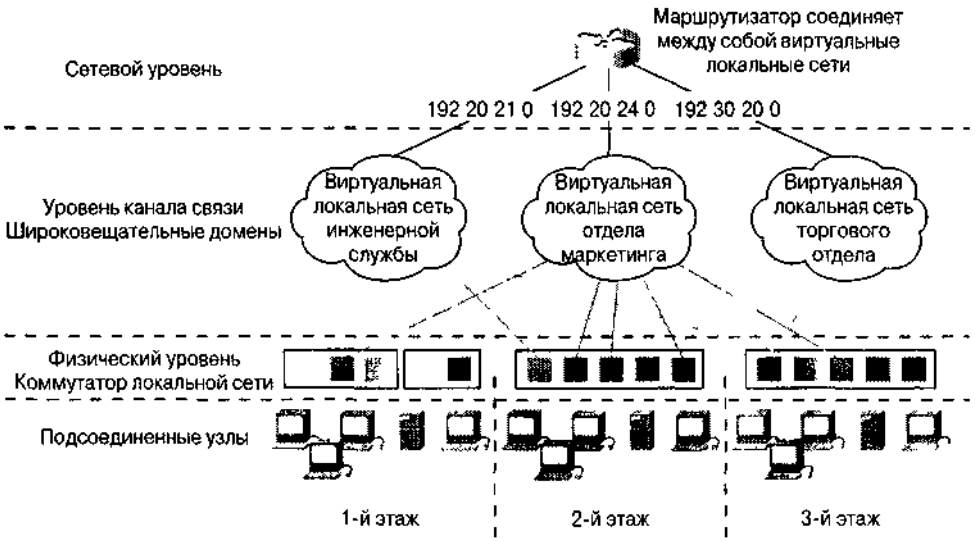


Рис. 3.5. В виртуальных сетях с центральным портом легко осуществляется контроль за всеми пользователями сети Все узлы, подключенные к одному и тому же порту, должны находиться в одной виртуальной сети

Статические виртуальные сети

Статическая виртуальная сеть (Static VLAN) представляет собой совокупность портов коммутатора, статически объединенных в виртуальную сеть. Эти порты поддерживают назначенную конфигурацию до тех пор, пока она не будет изменена администратором. Хотя для внесения изменений статические виртуальные сети требуют вмешательства администратора, к их достоинствам можно отнести высокий уровень безопасности, легкость конфигурирования и возможность непосредственного наблюдения за работой сети Статические виртуальные сети эффективно работают в ситуациях, когда необходимо контролировать переезды пользователей и вносить соответствующие изменения в конфигурацию.

Динамические виртуальные сети

Динамические виртуальные сети (dynamic VLAN) представляют собой логическое объединение портов коммутатора, которые могут автоматически определять свое расположение в виртуальной сети. Функционирование динамической виртуальной сети основывается на MAC-

адресах, на логической адресации или на типе протокола пакетов данных. При первоначальном подключении станции к неиспользуемому порту коммутатора соответствующий коммутатор проверяет MAC-адрес в базе данных управления виртуальной сетью и динамически устанавливает соответствующую конфигурацию на данном порте. Основными достоинствами такого подхода является уменьшение объема работ в монтажном шкафу при добавлении нового пользователя или при переезде уже существующего и централизованное извещение всех пользователей при добавлении в сеть неопознанного пользователя. Основная работа в этом случае заключается в установке базы данных в программное обеспечение управления виртуальной сетью и в поддержания базы данных, содержащей точную информацию обо всех пользователях сети.

Достоинства виртуальных сетей

В качестве достоинств виртуальных сетей можно выделить следующие их особенности.

- Использование виртуальных сетей позволяет значительно экономить средства, затрачиваемые на решение вопросов, связанных с переездом в другое место, с появлением новых пользователей и с внесением изменений в структуру сети
- Виртуальные сети позволяют обеспечить контроль над широковещанием.
- Они позволяют обеспечить защиту информации в рабочих группах и во всей сети.
- Виртуальная сеть позволяет сэкономить средства за счет использования уже существующих концентраторов.

Добавление новых пользователей, их переезд и изменение расположения

Современные компании находятся в состоянии непрерывной реорганизации. В среднем 20—40% работников физически меняют свое расположение каждый год. Эти переезды, добавления новых пользователей и изменения структуры сети представляют собой страшную головную боль сетевых менеджеров и вызывают большую часть расходов, связанных с поддержанием работы сети Многие переезды требуют изменения прокладки кабелей и почти все переезды требуют изменения адресации станций и установки новой конфигурации маршрутизаторов и концентраторов

Виртуальные сети представляют собой эффективный механизм управления этими изменениями и уменьшения расходов, связанных с установкой новой конфигурации концентраторов и маршрутизаторов Пользователи виртуальной локальной сети могут совместно использовать одно и то же сетевое адресное пространство (т е. IP-подсеть) независимо от их физического расположения Если пользователь виртуальной сети переезжает из одного места в другое, оставаясь внутри той же самой виртуальной сети и оставаясь подключенным к тому же самому порту коммутатора, то его сетевой адрес не изменяется. Изменение положения пользователя требует всего лишь подключения его компьютера к одному из портов коммутатора и включения этого порта в прежнюю виртуальную сеть, как показано на рис 3 6.

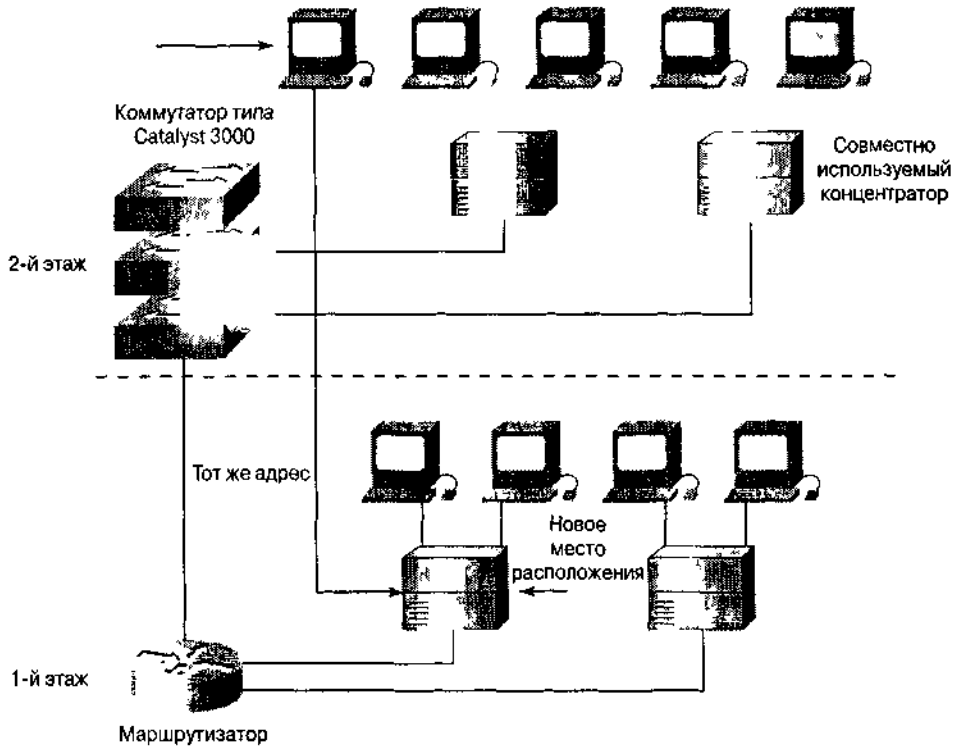


Рис 3.6. Коммутаторы, способные создавать виртуальные сети, значительно упрощают решение проблем, связанных с изменением схемы прокладки кабелей, конфигурации сети, с переездом пользователя в другое место, а также задач отладки при повторном подсоединении пользователя к сети

Виртуальные сети обладают значительными преимуществами перед обычными локальными сетями, поскольку они требуют меньших изменений при прокладке кабелей, при установке конфигурации сети и уменьшают время, требуемое для отладки.

Конфигурация маршрутизаторов остается при этом неизменной; сам по себе переезд пользователя из одного места в другое, если пользователь остается в той же самой виртуальной сети, не требует изменения конфигурации маршрутизатора.

Управление широковещанием

Потоки широковещательных сообщений циркулируют в каждой сети. Частота появления широковещательных сообщений зависит от типа приложения, типа серверов, количества логических сегментов и характера их использования. Хотя многие приложения за последние годы были модифицированы таким образом, чтобы уменьшить число посылаемых ими широковещательных сообщений, разрабатываемые в настоящее время новые мультимедийные приложения интенсивно используют широковещание и **множественную (групповую) адресацию (multicast).**

Для предотвращения проблем, связанных с широковещанием, необходимо принимать превентивные меры. Одной из наиболее эффективных мер является сегментирование сети с помощью брандмауэров для того, чтобы в максимальной степени уменьшить влияние проблем, возникших в одном сегменте, на другие части сети. В этом случае, несмотря на наличие проблем широковещания в одном из сегментов, остальная часть сети оказывается защищенной брандмауэром, в качестве которого обычно используется маршрутизатор. Сегментация с помощью брандмауэров обеспечивает надежность и минимизирует поток широковещательных служебных сообщений, обеспечивая тем самым большую пропускную способность для потоков данных

приложений.

Если между коммутаторами нет маршрутизаторов, то широковещательные сообщения (передачи 2-го уровня) передаются на все коммутируемые порты. Такую конфигурацию обычно называют **плоской сетью (flat network);** при этом вся сеть представляет собой один широковещательный домен. Преимущества плоской сети заключаются в небольшом времени ожидания и высокой производительности, а также в легкости администрирования. Недостатком такой сети является ее повышенная чувствительность к широковещательному потоку через коммутаторы, порты и магистральные каналы.

Виртуальные сети представляют собой эффективный механизм расширения сферы действия брандмауэров (маршрутизаторов) на среду коммутации и защиты сети от потенциально опасных проблем широковещания. Кроме того, виртуальные сети сохраняют все преимущества, предоставляемые коммутацией.

Брандмауэры создаются путем логического объединения портов или пользователей в отдельные группы виртуальной сети как на отдельных коммутаторах, так и в группе соединенных коммутаторов. Как показано на рис. 3.7, широковещательные сообщения одной виртуальной сети не передаются за ее пределы и, наоборот, на прилегающие порты не поступают широковещательные сообщения от других виртуальных сетей. Такой тип конфигурации существенно уменьшает общий широковещательный поток, освобождает полосу пропускания для потока данных пользователей и снижает общую чувствительность сети к **широковещательной лавине (broadcast storm)**

Чем меньше группа виртуальной сети, тем меньше количество пользователей, которые получают широковещательные сообщения, распространяемые внутри какой-либо группы. Группировка пользователей виртуальной сети может также выполняться на основе типа используемых приложений или типа широковещательных сообщений, поступающих от приложений. Можно поместить пользователей, совместно использующих приложения с высокой широковещательной активностью, в одну группу и распределить приложение по всей сети предприятия.

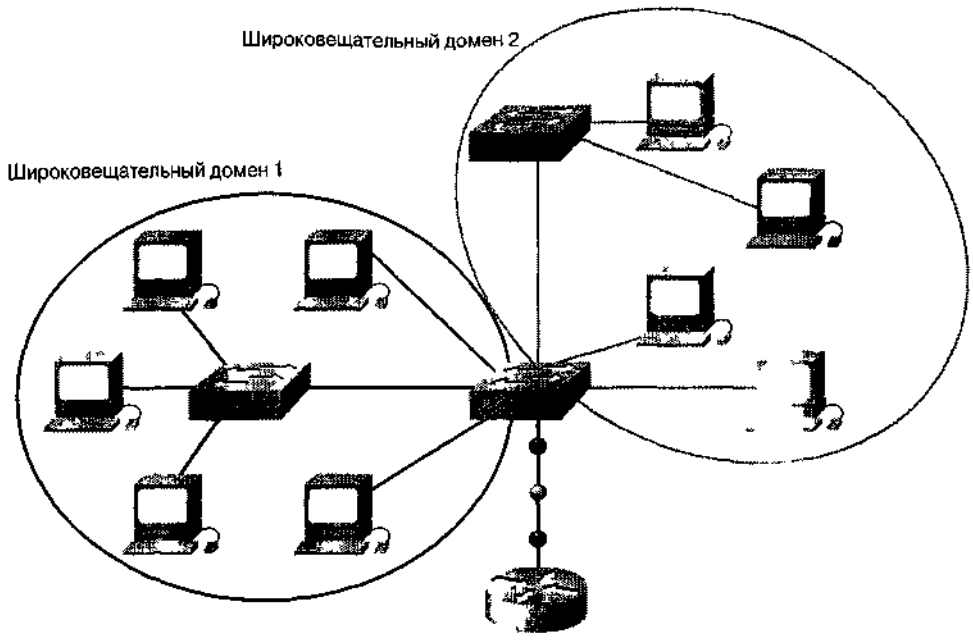


Рис 3.7. Ограничивая количество портов коммутатора внутри виртуальной сети и количество пользователей, подключенных к этим портам, можно легко управлять размером широковещательного домена

Обеспечение большей безопасности сети

За последние годы сфера использования локальных сетей значительно расширилась. По се-

тям часто передаются конфиденциальные данные. Защита конфиденциальной информации требует ограничения доступа к сети. Проблема, вызванная совместным использованием локальных сетей, состоит в том, что в такую сеть можно относительно легко проникнуть Подключившись к активному порту, вторгшийся без разрешения в сеть пользователь получает доступ ко всем данным, передаваемым по сегменту. При этом чем больше группа, тем больше потенциальная угроза несанкционированного доступа.

Одним из эффективных в финансовом отношении и легко административно реализуемых методов повышения безопасности является сегментация сети на большое количество широковещательных групп, как показано на рис. 3.8. Это позволяет сетевому администратору:

- ограничить количество пользователей в группе виртуальной сети;
- запретить другим пользователям подсоединение без предварительного получения разрешения от приложения, управляющего виртуальной сетью;
- установить конфигурацию всех неиспользуемых портов в принимаемое по умолчанию состояние низкой активности VLAN.

Реализовать сегментацию такого типа относительно просто. Порты коммутатора группируются на основе типа приложений и приоритетов доступа. Приложения и ресурсы, доступ к которым ограничен, обычно размещаются в защищенной группе виртуальной сети. Маршрутизатор ограничивает доступ в эту группу в соответствии с конфигурацией коммутаторов и маршрутизаторов. Ограничения доступа могут основываться на адресах станций, типах приложений или типах протоколов.

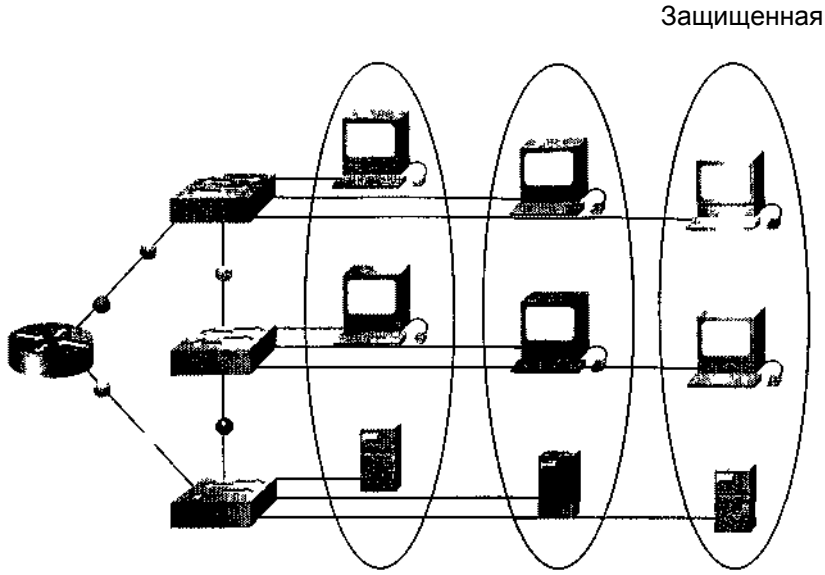


Рис 3.8. Виртуальные сети позволяют использовать брандмауэры, ограничить доступ индивидуальных пользователей и уведомляют сетевого менеджера о несанкционированном вторжении в сеть

Обеспечить большую безопасность можно путем использования **списков управления доступом (access control list, ACL),** которые описаны в главе 6, "Списки управления доступом (ACL)" Они особенно полезны при обмене информацией между отдельными локальными сетями В защищенной виртуальной сети маршрутизатор ограничивает доступ к сетевой информации посредством задания соответствующей конфигурации коммутаторов и маршрутизаторов. Ограничения доступа могут основываться на адресах станций, типах приложений, типах протоколов или даже на времени суток

Экономия финансовых средств за счет использования уже существующих концентраторов

За последние несколько лет сетевые администраторы установили большое количество концентраторов. Многие из этих устройств заменяются ныне новыми. Поскольку сетевые приложения требуют все большей полосы пропускания и большей эффективности непосредственно на рабочем месте, эти концентраторы по-прежнему исполняют полезные функции во многих существующих сетях. Сетевые менеджеры могут сэкономить средства, подсоединяя уже существующие концентраторы к коммутаторам

Как показано на рис 3 9, каждый сегмент концентратора, соединенный с коммутатором, может быть назначен только одной группе виртуальной сети. Если какую-либо станцию необходимо перевести в другую виртуальную сеть, то эта станция должна быть заново подсоединена к соответствующему концентратору.

Взаимные связи между коммутаторами позволяют выполнять обмен информацией между коммутирующими портами и автоматически определять соответствующие принимающие сегменты. Чем больше групп создается на совместно используемом концентраторе, тем выше степень **микросегментации (microsegmentation)** и тем большей гибкостью обладает виртуальная сеть при объединении отдельных пользователей в группы.

Путем подсоединения концентраторов к коммутаторам можно установить конфигурацию, при которой концентраторы являются частью архитектуры виртуальной сети. При этом становится возможным совместное использование потоков данных и сетевых ресурсов, непосредственно подсоединенных к коммутирующим портам виртуальной сети.

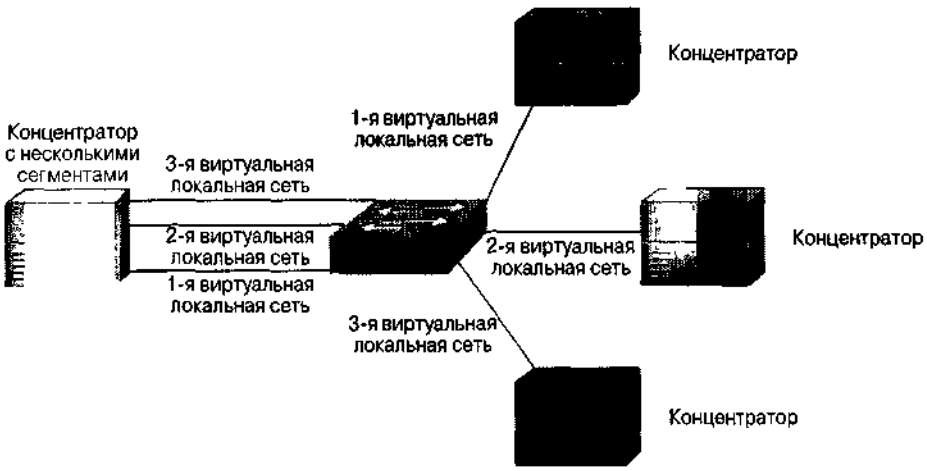


Рис. 3 9 Соединение концентраторов и коммутаторов предоставляет возможность сегментации виртуальной сети

Резюме

- Коммутатор Ethernet предназначен для физической сегментации локальной сети, в результате которой образуются отдельные коллизионные домены (collision domain).
- Обычная локальная сеть конфигурируется в соответствии с физической инфраструктурой сети.
- В локальных сетях, использующих коммутирующие устройства, создание виртуальной сети представляет собой эффективный в финансовом и производственном отношении способ группировки пользователей сети в виртуальные рабочие группы независимо от их физического расположения.

- Виртуальные сети функционируют на 2-м и 3-м уровнях эталонной модели OSI.
- Важной особенностью архитектуры VLAN является ее способность передавать информацию между взаимосвязанными коммутаторами и маршрутизаторами, подсоединенными к корпоративной магистрали.
- Проблемы, возникающие при совместном использовании локальных сетей и коммутаторов, побуждают к замене традиционных конфигураций локальных сетей коммутируемыми конфигурациями виртуальных сетей.
- Наиболее общими подходами при осуществлении логической группировки пользователей в отдельные виртуальные сети являются фильтрация фреймов, использование фреймовых тегов и идентификация фреймов.
- Существуют три основных типа виртуальных сетей: сети с центральным портом, статические виртуальные сети и динамические виртуальные сети.
- Среди достоинств виртуальных сетей можно выделить следующие.
- Использование виртуальных сетей позволяет уменьшить административные затраты, связанные с решением вопросов переезда, добавления новых пользователей и изменений в структуре сети.
- Они обеспечивают управление широковещанием.
- Виртуальные сети обеспечивают защиту информации в рабочих группах и во всей сети.
- Виртуальные сети позволяют сэкономить средства за счет использования уже существующих концентраторов.

Контрольные вопросы

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

1. Опишите преимущества виртуальных сетей.
2. Какое влияние оказывает использование виртуальных сетей на широковещание в традиционных локальных сетях?
3. Каковы три основных способа реализации виртуальных сетей?
4. Какова цель использования фреймовых тегов в виртуальных сетях?
5. Термин *расширяемая микросегментация* означает следующее.
   A. Возможность расширения сети без создания коллизионных доменов.
   B. Возможность подключения большого числа хостов к одному коммутатору.
   C. Возможность широковещания сразу на большое количество узлов.
   D. Все вышеупомянутое.
6. Коммутаторы, которые являются ключевым элементом виртуальных сетей, дают возможность выполнить следующее.
   A. Сгруппировать пользователей, порты или логические адреса в виртуальной сети.
   B. Принять решения о фильтрации и отправке фреймов.
   C. Выполнять обмен информацией между коммутаторами и маршрутизаторами.
   D. Все перечисленное.
7. Каждый сегмент_____, подсоединенный к порту _____, может быть назначен только одной виртуальной сети.
   A. Коммутатора; концентратора.
   B. Концентратора; маршрутизатора.
   C. Концентратора; коммутатора.
   D. Локальной сети; концентратора.

8. Что из перечисленного ниже *не является* достоинством статической виртуальной сети?

A. Защита сети от несанкционированного доступа.

B. Легкость установки конфигурации.

C. Легкость наблюдения за работой сети.

D. Автоматическое обновление конфигурации портов при добавлении новых станций.

9. Что из перечисленного ниже *не является* характерным признаком виртуальной сети?

A. ID-порт и MAC-адрес.

B. Протокол.

C. Приложение.

D. Все перечисленные понятия являются характерными признаками виртуальной сети.

10. Что из перечисленного ниже является положительным результатом использования виртуальной сети?

A. Отсутствует необходимость конфигурирования коммутаторов.

B. Можно управлять широковещанием.

C. Можно защитить конфиденциальную информацию.

D. Могут быть преодолены физические границы, препятствующие объединению пользователей в группы.

Основные термины

Адрес управления доступом к передающей среде или MAC-адрес (Media Access Control, MAC). Шестибайтовое число, представляющее собой стандартизированный адрес канального уровня, необходимый каждому порту или устройству, подключенному к локальной сети. Устройства сети используют эти адреса для нахождения определенных портов, а также для создания и обновления таблиц маршрутизации и структур данных. MAC-адреса контролируются IEEE. Они также называются аппаратными адресами, адресами MAC-уровня или физическими адресами.

Брандмауэр (firewall). Один или несколько маршрутизаторов или серверов доступа, выполняющих роль буфера между частной и общей сетью. Использует список управления доступом (ACL) и другие средства для обеспечения безопасности частной сети.

Виртуальная сеть (virtual LAN, VLAN). Группа устройств в локальной сети, которые сконфигурированы (с использованием управляющего программного обеспечения) таким образом, что они могут обмениваться информацией, как если бы они были подключены к одному кабелю. В действительности они могут быть расположены в разных сегментах локальной сети. Структура таких сетей является чрезвычайно гибкой, поскольку она базируется не на физическом, а на логическом соединении устройств.

Виртуальная сеть с центральным портом (port-centric VLAN). Виртуальная сеть, все узлы которой присоединены к одному порту коммутатора.

Групповая или многоадресная передача (multicast). При таком способе передачи пакеты копируются и рассылаются по нескольким адресам, которые указаны в адресном поле пакета.

Динамическая виртуальная сеть (dynamic VLAN). Виртуальная сеть, создаваемая на основе MAC-адресов, логических адресов или на типе протокола пакетов данных.

Институт инженеров по электротехнике и электронике (Institute of Electrical and Electronic Engineers, IEEE). Профессиональная организация, чья деятельность включает в себя разработку коммуникационных и сетевых стандартов. Сетевые стандарты ШЕЕ для локальных сетей в настоящее время являются общепринятыми.

Коллизионный домен (collision domain). В сети Ethernet — область сети, в которой распространяются столкнувшиеся фреймы. Повторители и концентраторы позволяют коллизиям распространяться по сети, а коммутаторы, мосты и маршрутизаторы их останавливают.

Коммутатор (switch). Сетевое устройство, которое фильтрует, перенаправляет и рассылает фреймы на основе MAC-адреса их пункта назначения. Коммутатор выполняет операции на канальном уровне эталонной модели OSI.

Концентратор (hub). Аппаратное или программное обеспечение, объединяющее несколько независимых, но соединенных между собой модулей сети или сетевого оборудования. Концентраторы могут быть активными (усиливающими сигналы, проходящие через них) или пассивными (такие концентраторы не усиливают, а просто пропускают сигналы через себя).

Маршрутизатор (router). Устройство сетевого уровня, использующее одну или несколько метрик для нахождения оптимального пути прохождения потока данных по сети. Маршрутизаторы перенаправляют потоки данных от одной области сети в другую, используя для этого информацию сетевого уровня. Иногда называются *шлюзами (gateway),* хотя это название все более и более устаревает.

Микросегментация (microsegmentation). Разделение сети на более мелкие сегменты. (Обычно осуществляется для увеличения полосы пропускания сетевых устройств).

Плоская сеть (flat network). Сеть, в которой между коммутаторами нет маршрутизаторов и представляющая собой один широковещательный домен. В такой сети широковещательные пакеты и сообщения канального уровня посылаются каждому коммутируемому порту.

Порт (port). Интерфейс сетевого устройства (например, маршрутизатора).

Протокол (protocol). Формальное описание набора соглашений и правил, которые определяют обмен информацией между устройствами в сети.

Расширяемость (scalability). Способность сети увеличиваться без каких-либо существенных изменений ее базовой структуры.

Сегмент (segment). Участок сети, ограниченный мостами, маршрутизаторами или коммутаторами.

Сетевой коммутатор (LAN **switch).** Коммутатор локальной сети. Высокоскоростной коммутатор, перенаправляющий пакеты между сегментами сети. Большинство коммутаторов локальной сети изменяют направления движения потоков данных, анализируя MAC-адреса, содержащиеся в пакетах. Коммутаторы локальных сетей подразделяются на категории, в соответствии с используемым методом коммутации: с буферизацией или без буферизации пакетов. Примером коммутатора локальной сети может служить модель Cisco Catalyst 5000.

Список управления доступом (access control list, ACL). Набор ограничительных и разрешающих директив в конфигурации маршрутизатора Cisco, для управления передачей и отправкой с него информации (например, для предотвращения отправки пакетов с некоторым адресом с указанного интерфейса маршрутизатора).

Статическая виртуальная сеть (static VLAN). Виртуальная сеть, в которой конфигурация портов коммутатора не изменяется.

Фрейм (frame). Логически сгруппированная информация, посылаемая через передающую среду в виде блока данных канального уровня. Этот термин часто используется по отношению к заголовку и трейлеру, окружающим данные пользователя, содержащиеся в блоке, и используемым для синхронизации и определения ошибок. Термины *дейтаграмма, сообщение, пакет* и *сегмент (datagram, message, packet, segment)* также используются для описания логически сгруппированных блоков информации на разных уровнях эталонной модели OSI и в различных технологических циклах.

Широковещательная лавина (broadcast storm). Нежелательная множественная широковещательная передача, возникающая одновременно во всех сегментах сети. Широковещательная лавина использует всю возможную полосу пропускания и обычно вызывает простои сети.

Широковещательный домен (broadcast domain). Группа устройств, каждое из которых принимает широковещательные фреймы, отправленные с любого узла этой группы. Широковещательные домены обычно ограничиваются маршрутизаторами, поскольку маршрутизаторы не отправляют широковещательные фреймы.

Широковещательный пакет (broadcast packet). Пакет данных, переданный всем узлам в сети. Характеризуется особыми широковещательными адресами.

Ключевые темы этой главы

- Объясняются цели проектирования локальных сетей
- Описываются проблемы, возникающие при проектировании локальных сетей
- Описывается методология проектирования сетей
- Описан процесс подбора и анализа сетевого оборудования
- Описан процесс проектирования первого уровня (передающие среды и топология)
- Описан процесс проектирования второго уровня (коммутация)
- Описан процесс проектирования третьего уровня (маршрутизация)
- Описана документация для физической и логической реализации сетей

Глава 4

Проектирование локальных сетей

Введение

В главе 3, "Виртуальные локальные сети", описывались локальные сети (LAN, VLAN) и коммутируемое сетевое взаимодействие, сравнивались традиционные локальные сети общего доступа с коммутируемыми сетями. В предыдущей главе также обсуждались преимущества использования архитектуры коммутируемых виртуальных локальных сетей. Несмотря на усовершенствования в области эффективности оборудования и повышение возможностей передающих сред, процесс проектирования сетей становится все более сложным Намечается тенденция к использованию более сложных сред, включая различные носители и межсетевые соединения за пределами управляемой сети, контролируемой одной организацией. В процессе проектирования важно постоянно помнить о совокупности этих факторов, поскольку тщательное проектирование сети может уменьшить трудности, связанные с ростом и развитием сетевой среды

Тщательное проектирование сети является важнейшей предпосылкой ее быстрой и устойчивой работы. Если при проектировании сети допущены ошибки, то может возникнуть множество непредвиденных проблем и возможность ее роста окажется под угрозой Процесс проектирования требует глубокого анализа конкретной ситуации. В настоящей главе приведен обзор процесса проектирования локальных сетей. Кроме того, в ней описываются цели, проблемы и методология проектирования, а также процесс разработки топологии локальных сетей

Вашингтонский проект: проектирование сети

Предполагается, что знания, полученные при чтении этой книги будут применяться для проектировании сети учебного округа. Этот вымышленный учебный округ расположен в городе Фениксе, штат Аризона В округе идет процесс проектирования и реализации сети, в которую войдут локальные сети каждой школы и распределенная сеть, обеспечивающая обмен данными между ними.

В этой главе начинается процесс проектирования локальной сети. Поскольку основные концепции и требования читателю уже знакомы, их можно применить на практике. В процессе проектирования необходимо обеспечить выполнение следующих требований.

- Предполагается, что сеть будет обслуживать различные рабочие группы — группы персонала школ и группы учащихся. Это логическое разделение станет основной идеей проекта и потребует использования виртуальных локальных сетей. Такие сети, например, придется использовать для того, чтобы отделить компьютеры администраторов от студенческих компьютеров.
- Частью этого проекта является также обеспечение доступа к Internet с любого компьютера школьного округа.
- Необходим ряд серверов для облегчения интерактивной автоматизации всех административных и обучающих функций.
- Поскольку данная реализация сети будет функционировать как минимум 7-10 лет, необходимо принять во внимание возможность 100% роста локальных сетей.
- Полоса пропускания канала к каждому хосту должна составлять не менее 1 Мбит/с, а к каждому серверу не менее 100 Мбит/с.
- Допускается использовать в сети только два маршрутизируемых протокола: TCP/IP и Novell IPX.

Цели проекта локальной сети

Проектирование сети может оказаться сложной задачей. Проектирование сети включает в себя нечто большее, чем просто создание связи между компьютерами. Для того, чтобы сеть была управляемой и расширяемой требуется учесть множество особенностей. Чтобы спланировать надежную и расширяемую сеть, проектировщик должен осознавать, что каждый из основных компонентов сети предъявляет к ней свои особые требования. Даже сеть, содержащая всего 50 узлов маршрутизации, может создать целый комплекс проблем, которые ведут к непредсказуемым результатам. А попытка разработать и построить сеть, включающую тысячи узлов, может вызвать еще более сложные проблемы.

Первым шагом в планировании сети является определение и документирование целей проекта. Названные цели являются специфическими для каждой организации или конкретной ситуации. Однако следующие требования характерны для большинства проектов.

- **Функциональность.** Прежде всего, сеть должна работать. Это означает, что она должна предоставить пользователям возможность удовлетворения их производственных потребностей. Сеть должна обеспечить связь пользователей друг с другом и с приложениями с соответствующей требованиям скоростью и надежностью.
- **Расширяемость.** Сеть должна обладать способностью к росту. Это означает, что первоначально реализованная сеть должна увеличиваться без каких-либо существенных изменений общего устройства.
- **Адаптируемость.** Сеть должна быть разработана с учетом технологий будущего и не должна включать элементы, которые в дальнейшем ограничивали бы внедрение технологических новшеств.
- **Управляемость.** Сеть нужно сконструировать так, чтобы облегчить текущий контроль и управление для обеспечения стабильности ее работы.

Аспекты, указанные выше, являются специфическими для одних типов сетей и более общими для других типов. В настоящей главе рассказывается как учесть эти требования в процессе проектирования.

Компоненты сетевого проекта

С появлением в последние годы высокоскоростных технологий, таких как ATM (режим асинхронной передачи) и более сложных архитектур локальных сетей, использующих коммутацию и виртуальные локальные сети, многие организации стали обновлять свои локальные сети, планировать и внедрять новые.

Для конструирования локальных сетей под высокоскоростные технологии и мультимедийные приложения проектировщику необходимо учитывать следующие важнейшие аспекты общего проектирования сетей.

- Функции и размещение серверов.
- Определение коллизий.
- Сегментация.
- Соответствие широкополосных и широковещательных доменов.

Эти вопросы обсуждаются в следующих разделах.

Функции и размещение серверов

Одним из ключевых моментов успешного проектирования является правильное понимание функций серверов и особенностей их размещения в сети. Серверы предоставляют доступ к файлам, печать, связь и службы приложений, таких как обработка текстов. Серверы чаще используются не в качестве рабочих станций, а работают под управлением специализированных операционных систем, таких как NetWare, Windows NT, UNIX и Linux. В настоящее время каждый сервер обычно выделяется для выполнения одной функции, например, функции почтового или файлового сервера.

Серверы можно разделить на два отдельных класса: **серверы предприятия (enterprise servers) и серверы рабочих групп (workgroup servers).** Сервер предприятия поддерживает всех пользователей сети, предоставляя им различные службы, такие как электронная почта или служба доменных имен (DNS), как показано на рис. 4.1. Поскольку серверы электронной почты и DNS выполняют централизованные функции, они могут понадобиться каждому члену организации (например, такой как Вашингтонский учебный округ). С другой стороны, сервер рабочей группы обслуживает определенную группу пользователей и предлагает им такие службы, как обработка текстов или совместный доступ к файлам, то есть функции, которые могут понадобиться только некоторым группам пользователей.

Серверы предприятия должны размещаться в **главной распределительной станции (main distribution facility, MDF).** В этом случае поток данных на серверы предприятия будет идти только к MDF, не проходя через остальные сети. В идеальном случае серверы рабочих групп следует размещать в **промежуточных распределительных станциях (intermediate distribution facilities, IDF),** по возможности ближе к пользователям, использующим приложения этих серверов. Для этого необходимо непосредственно соединить серверы с MDF или IDF. Если расположить серверы рабочих групп близко к пользователям, то поток данных будет проходить по инфраструктуре сети прямо к IDF, не затрагивая других пользователей в этом сегменте. Внутри MDF и IDF коммутаторы второго уровня должны иметь для этих серверов ширину полосы пропускания не менее 100 Мбит/с.

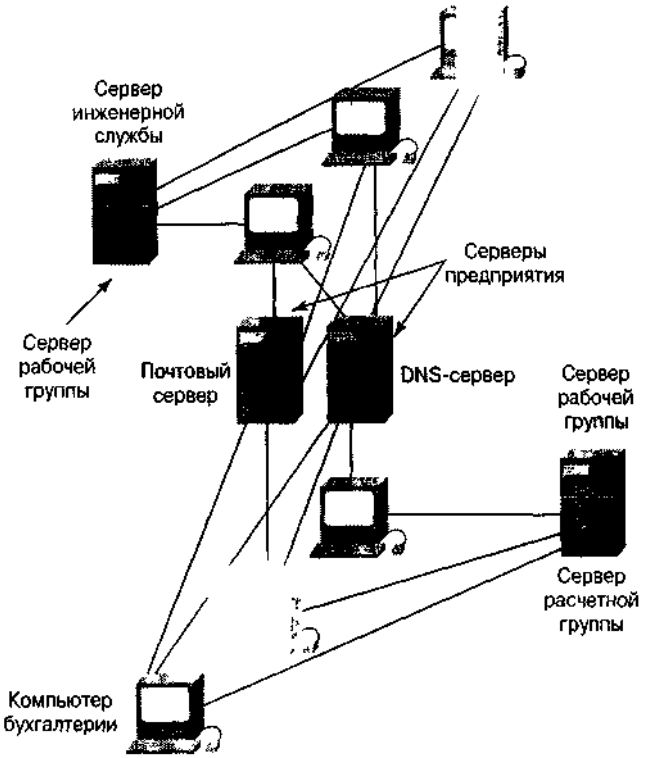


Рис. 4.1. Одно из отличий между серверами предприятий и рабочих групп состоит в том, что серверы предприятий включают в себя необходимые службы

Вашингтонский проект: размещение и функции серверов

Следует разделить файловые серверы проекта на серверы предприятия и серверы рабочих групп, а затем разместить их в сети согласно ожидаемому характеру потока данных пользователей и исполняемым функциям.

- **Серверы DNS и электронной почты.** В каждой узловой точке должен находиться DNS-сервер, чтобы поддерживать отдельные школы, обслуживаемые из этой точки. Каждая школа также должна иметь компьютер для DNS и служб электронной почты (так называемый локальный почтовый офис), обслуживающий всех студентов и сотрудников этой школы.
- **Административный сервер.** В каждой школе должен быть административный сервер для аттестации и проведения экзаменов учащихся, контроля посещаемости и выполнения других административных функций. Этот сервер должен использовать семейство протоколов TCP/IP и быть доступным только для преподавателей и сотрудников школы.
- **Библиотечный сервер.** В округе реализуются автоматизированная система библиотечной информации и поисковая система для интерактивного обучения и для исследовательских целей. Этот сервер должен использовать TCP/IP в качестве протокола третьего и четвертого уровня эталонной модели OSI Сервер предназначен для всех пользователей находящихся на территории любой школы округа.

- **Сервер приложений. Все** компьютерные приложения, такие как текстовые редакторы и электронные таблицы, должны размещаться на центральном сервере каждой школы.
- **Другие серверы.** Любые другие серверы, установленные в школах, должны рассматриваться как серверы отделов (рабочих групп) и размещаться в соответствии с потребностями доступа к ним групп пользователей. В качестве примера можно привести сервер с обучающим приложением для определенной школы.

Сети intranet

Intranet представляет собой одну из типичных конфигураций локальных сетей. Web-серверы в сети intranet отличаются от публичных Web-серверов тем, что без соответствующего разрешения и пароля получить доступ к сети intranet какой-либо организации невозможно. Сети intranet спроектированы таким образом, что доступ к ним имеют только пользователи, имеющие право доступа к внутренней сети организации. Внутри intranet устанавливаются Web-серверы, а броузеры используются в качестве общего средства доступа к информации, например, к финансовым, графическим или текстовым данным, хранящимся на этих серверах.

Введение технологии intranet является лишь одним из многих факторов, обусловленных использованием приложений и параметрами конфигурации и вызывающих потребность в увеличении полосы пропускания. Поскольку полоса пропускания сетевой магистрали должна быть расширена, сетевым администраторам необходимо также рассмотреть возможность приобретения мощных рабочих станций для более быстрого доступа к intranet. Новые рабочие станции и серверы должны быть снабжены сетевыми адаптерами 10—100 Мбит/с для обеспечения большей конфигурационной гибкости, которая позволит сетевым администраторам выделять необходимую полосу пропускания отдельным станциям.

Обнаружение коллизий

Для того, чтобы уменьшить количество коллизий и конкуренцию за доступ к носителям, в процессе проектирования следует принять взвешенные решения при выборе и размещении сетевых устройств. Под конкуренцией понимается чрезмерное число коллизий в сетях Ethernet, вызванное с большим количеством запросов многих устройств к ресурсам сети. Число широковещательных рассылок становится чрезмерным, когда слишком много клиентов обращаются к службам, когда слишком много серверных пакетов предлагают службы или происходят многочисленные **обновления таблицы маршрутизации (routing update),** а также в случае наличия большого количества широковещательных сообщений протоколов, например, протокола преобразования адресов (ARP).

Узел сети Ethernet получает доступ к среде, конкурируя с другими устройствами. В случае увеличения количества узлов, подключенных к общей среде возникает ситуация, когда, эти узлы пытаются передавать все большее и большее количество сообщений и шансы одного узла выиграть эту борьбу значительно уменьшаются, в результате чего сеть "захлебывается". То, что конкуренция, как метод доступа, не допускает расширения и не позволяет сети увеличиваться, является главным недостатком сетей Ethernet.

Как показано на рис. 4.2, количество коллизий растет с увеличением потока данных в сети с общим доступом. И хотя коллизии являются обычными явлениями в сетях Ethernet, чрезмерное их число уменьшает доступную полосу пропускания (иногда весьма значительно). В большинстве случаев фактически доступная полоса уменьшается примерно на 35—40% по сравнению с

номинальной (10 Мбит/с). Это явление можно ликвидировать путем сегментации сети с использованием мостов, коммутаторов или маршрутизаторов.

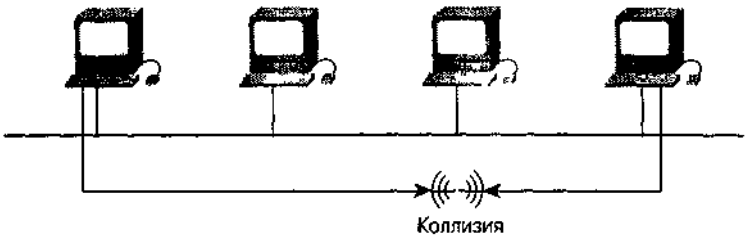


Рис. 4.2. В сети с шинной топологией коллизии уменьшают доступную полосу пропускания

Сегментация

Под **сегментацией (segmentation)** понимается процесс разделения одного коллизионного домена на два или более, как показано на рис. 4.3. Мосты и коммутаторы второго (канального) уровня можно использовать для сегментации сети с логической шинной топологией и для создания разделенных коллизионных доменов. В результате увеличивается доступная полоса пропускания для отдельных станций. Вся сеть с шинной топологией по-прежнему представляет собой широковещательный домен, поскольку мосты и коммутаторы пересылают широковещательные пакеты, хотя и не распространяют коллизии (рис. 4.3).

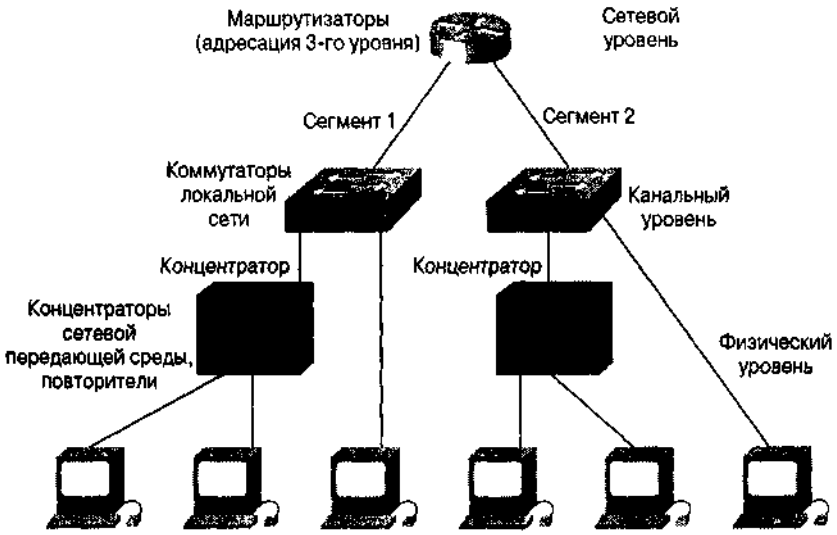


Рис. 4.3. Для сегментации сети используются маршрутизаторы и коммутаторы

Все широковещательные рассылки от любого хоста видны остальным хостам в том же широковещательном домене, что необходимо для обеспечения возможности установления соединения. Расширяемость широкополосного домена зависит от общего потока данных, а расширяемость широковещательного домена — от общего широковещательного потока. Важно помнить, что мосты и коммутаторы пересылают широковещательный (FF-FF-FF-FF-FF) поток, в то время как маршрутизаторы обычно этого не делают.

Широкополосный и широковещательный домены

Под широкополосным доменом понимаются все устройства, связанные с одним портом моста или коммутатора. В случае Ethernet-коммутатора широкополосный домен называется также **коллизионным доменом.** Коммутатор может создать по одному широкополосному домену на каждом порте. Как показано на рис. 4.4, все рабочие станции одного широкополосного домена конкурируют за полосу пропускания своей локальной сети. Весь поток данных с любого хоста широкополосного домена виден всем остальным хостам. В коллизионном домене сети Ethernet, две станции могут начать передачу одновременно, что вызывает коллизию.

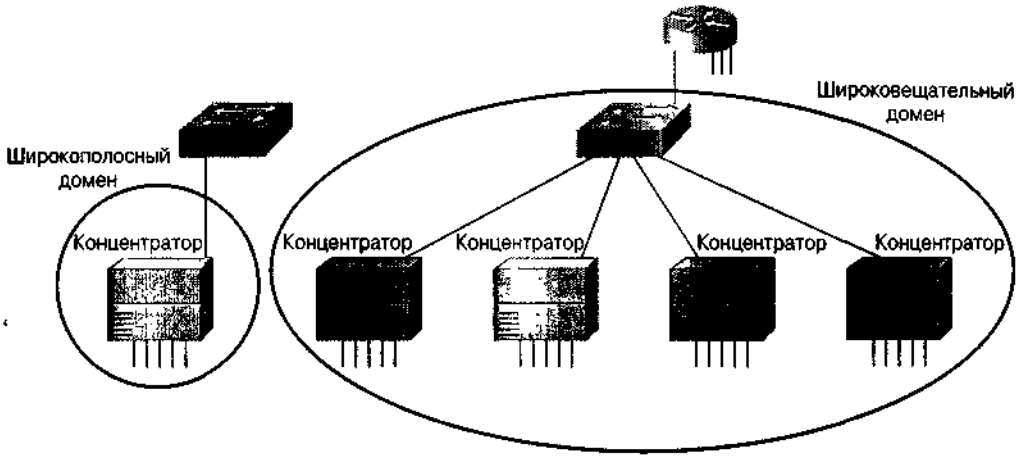


Рис. 4.4. Коллизионный домен имеет общую полосу пропускания, а широковещательный домен виден всей подсети

Методология проектирования сети

Чтобы локальная сеть была эффективной и удовлетворяла потребностям пользователей, она должна быть спроектирована и реализована в результате тщательно спланированной последовательности действий, включающих следующее .

1. Сбор требований и ожиданий пользователей.
2. Анализ собранных требований.
3. Проектирование структуры 1-го, 2-го и 3-го уровней локальной сети (т. е. топологии сети).
4. Документирование логической и физической реализации сети.

Эти действия описываются в приведенных ниже разделах.

Сбор требований

На первом этапе проектирования сети следует собрать данные о структуре организации. Эта информация должна включать в себя данные об истории и текущем состоянии организации, о планируемом росте, о методах управления, офисных системах, а также мнения членов персонала, которые будут использовать локальную сеть. Необходимо ответить на следующие вопросы: кто будет пользователем локальной сети? Каков уровень его навыков, и как он относится к компьютерам и компьютерным приложениям?

Ответы на эти и подобные вопросы помогут определить требования к дополнительному обучению и количество специалистов, необходимое для поддержки данной локальной сети.

Вашингтонский проект: понимание потребностей заказчика

Первое и главное — необходимо понять заказчика. В случае проекта Вашингтонского учебного округа необходимо встретиться с основными пользователями сети, определить их географическое расположение, используемые в настоящее время приложения и планы на будущее, а также решить, кто сможет быть главным помощником при проектировании сети. После завершения сбора данных об организационной структуре округа необходимо:

- определить, как перемещается информация в округе;
- выяснить, где хранятся общедоступные данные и кто их использует;
- выяснить, необходим ли доступ к данным, которые находятся за пределами округа,
  например, в Internet;
- определить вопросы и проблемы, требующие решения.

В идеальном случае процесс сбора информации помогает определить и прояснить проблемы, стоящие перед проектировщиком. Следует также определить, существуют ли в организации уже установленные правила. Объявлены ли какие-либо данные как критичные? Объявлены ли какие-либо операции как критичные? (Критичные данные и операции рассматриваются в качестве ключевых для бизнеса, а доступ к ним является критически важным для ежедневно выполняемых дел.) Какие протоколы можно использовать в сети? Существуют ли ограничения на типы рабочих станций?

Далее следует определить, кто в данной организации обладает полномочиями на установление адресации, назначение имен, на установку конфигурации и планирование топологии. В некоторых компаниях имеется центральный департамент **управления информационными системами** (УИС) (Management **Information** Systems, MIS), который отвечает за решение этих вопросов. В других компаниях департамент УИС очень мал и поэтому полномочия передаются отделам. При этом также следует уделить особое внимание оценке ресурсов предприятия и имеющихся ограничений. Ресурсы организации, которые могут повлиять на реализацию новой локальной сети, подразделяются на две основные категории: компьютерное программное и аппаратное обеспечение и человеческие ресурсы. Нужно документально зафиксировать существующее программное и аппаратное обеспечение организации и то, которое потребуется в будущем. Каким образом в настоящее время эти ресурсы связаны и предоставляются ли они для совместного доступа? Какими финансовыми ресурсами обладает данная организация? Ответ на эти вопросы поможет оценить издержки и рассчитать бюджет локальной сети. Проектировщику следует также убедиться в правильном понимании им того, насколько эффективны сети, уже существующие на предприятии.

Анализ требований

Следующий шаг при конструирования сети — анализ собранных на предыдущем этапе тре-

бований пользователей к будущей сети. С течением времени пользователи сети, как правило, повышают свои требования. Например, чем больше появляется доступных голосовых и видеоприложений, тем большими становятся требования к увеличению пропускной способности сети.

Еще одной задачей данного этапа является оценка требований пользователей. Конечно, мало пригодна сеть, которая не способна предоставить своим пользователям необходимую и точную информацию. Поэтому необходимо предпринять соответствующие действия для удовлетворения информационных требований организации и ее работников.

Вашингтонский проект: доступность

Выясните, что означает для заказчика понятие *доступности. В* случае проекта Вашингтонского учебного округа необходимо провести детальный анализ текущих задач и тех, которые появятся в дальнейшем. Анализ требований, предъявляемых к сети, включает в себя анализ производственных и технических целей округа.

Необходимо ответить на следующие вопросы.

- Какие приложения будут устанавливаться?
- К каким новым сетям потребуется доступ?
- В каком случае проект можно будет считать успешно реализованным?

Доступность и поток данных в сети

Полезность сети определяется ее доступностью. На доступность влияют многие факторы, включая следующие.

- Пропускная способность.
- Время отклика.
- Доступ к ресурсам.

У каждого заказчика есть свое определение **доступности.** Например, может возникнуть необходимость передавать голосовые или видеоданные по сети. Однако подобные службы требуют полосы пропускания большей, чем имеющаяся в сети или магистрали. В этом случае доступность можно увеличить путем добавления ресурсов, но такой путь значительно увеличивает стоимость. В процессе сетевого проектирования необходимо искать способы обеспечения большей доступности с наименьшими затратами.

Вашингтонский проект: определение сетевой нагрузки

До разработки структуры сети и приобретения оборудования необходимо определить сетевую нагрузку в Вашингтонском учебном округе.

Кроме того, при анализе технических требований округа, следует оценить поток данных, вызываемый приложениями, в размере и количестве пакетов (например, в байтах в секунду, что позволит оценить время, необходимое для передачи этих файлов по сети). Некоторые виды использования сети могут генерировать большой поток данных и, следовательно, вызывать перегрузку сети в следующих устройствах и службах.

- Internet-доступ.
- Загрузка программного обеспечения с удаленного сайта.

- Передача изображений или видеоинформации.
- Доступ к центральной базе данных.
- Обращения к файловым серверам отделов.

Следует также оценить нагрузку на сеть при максимальном количестве одновременно работающих пользователей и во время запуска регулярных сетевых служб, таких как резервное копирование на файловом сервере.

Проектирование сетевой топологии

Следующий шаг после определения всех требований к сети — принятие решения по выбору удовлетворяющей нужды пользователей, топологии локальной сети. В этой книге рассматриваются **звездообразная (star topology)** и расширенная звездообразная топологии. Как следует из рис. 4.5, звездообразная и расширенная звездообразная топологии используют технологию сетей Ethernet 802.3 — метод множественного доступа с контролем несущей и обнаружением коллизий (CSMA/CD). В этой книге рассматривается звездообразная топология CSMA/CD по причине ее доминирующего положения в индустрии.

Звездообразная топология

Расширенная звездообразная топология

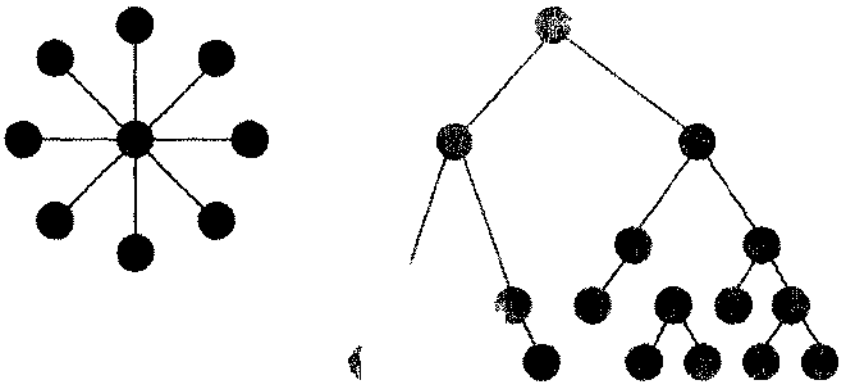


Рис. 4.5. Звездообразная и расширенная звездообразная топологии являются весьма стабильными и поэтому наиболее распространенными моделями сетей

Как показано на рис. 4.3, главные компоненты локальной сети могут быть разделены между тремя уровнями эталонной модели OSI — сетевым, канальным и физическим. Эти компоненты обсуждаются в приведенных ниже разделах.

Проектирование топологии физического уровня

В этом разделе исследуется звездообразная и расширенная звездообразная топология.

Вашингтонский проект: быстродействие и расширение

Для проекта Вашингтонского учебного округа необходимо подобрать компоненты сетевого уровня с достаточным быстродействием и возможностью расширения. Как известно, физический уровень определяет путь, по которому данные передаются между узлом-источником и узлом-адресатом. Следовательно, тип передающей среды и выбранная топология помогут определить, какой объем данных и насколько быстро сможет проходить по сети.

Прокладка кабелей

Физические кабели — один из наиболее важных компонентов, выбираемых при проектировании сети. Решение этой задачи включает в себя выбор типа используемого кабеля (обычно медный или оптоволоконный) и его общей структуры. Кабельная среда физического уровня включает в себя такие типы, как **неэкранированная витая пара пятой категории (Category 5 unshielded twisted-pair, UTP) и оптоволоконный кабель (fiber-optic cable).** При прокладке кабеля следует руководствоваться стандартом EIA/TIA 568 для размещения и соединения проводных схем.

В дополнение к ограничениям на протяженность кабеля, необходимо тщательно оценить сильные и слабые стороны различных кабельных топологий, поскольку эффективность сети прежде всего зависит от качества ее основного кабеля. Большая часть проблем, возникающих в сети, связана с проблемами физического уровня. Если планируются какие-либо значительные изменения в сети, то следует сделать полный анализ состояния кабеля для определения зон, в которых требуется обновление и замена кабеля.

При проектировании новой сети или повторной прокладке кабеля, необходимо учитывать, что высокоскоростные технологии, такие как Fast Ethernet, ATM и Gigabit Ethernet должны использовать, как минимум, оптоволоконный кабель в качестве магистрали и вертикальных соединений и кабель пятой категории UTP для горизонтальных соединений. Обновление кабеля должно иметь приоритет перед другими необходимыми изменениями. Предприятие должно обеспечить полное и безусловное соответствие этих систем строгим промышленным стандартам, таким как спецификации TIA/EIA 568.

Стандартом EIA/TIA 568 определяется, что каждое устройство, подключенное к сети, должно быть соединено горизонтальным кабелем с центральной точкой, как показано на рис. 4.6. Это требование должно выполняться в том случае, когда все станции, которым необходим доступ в сеть, находятся в радиусе 100 метров для кабеля пятой категории UTP Ethernet, как указывается в стандарте EIA/ IA 568. В табл. 4.1 перечислены типы кабелей и их характеристики.

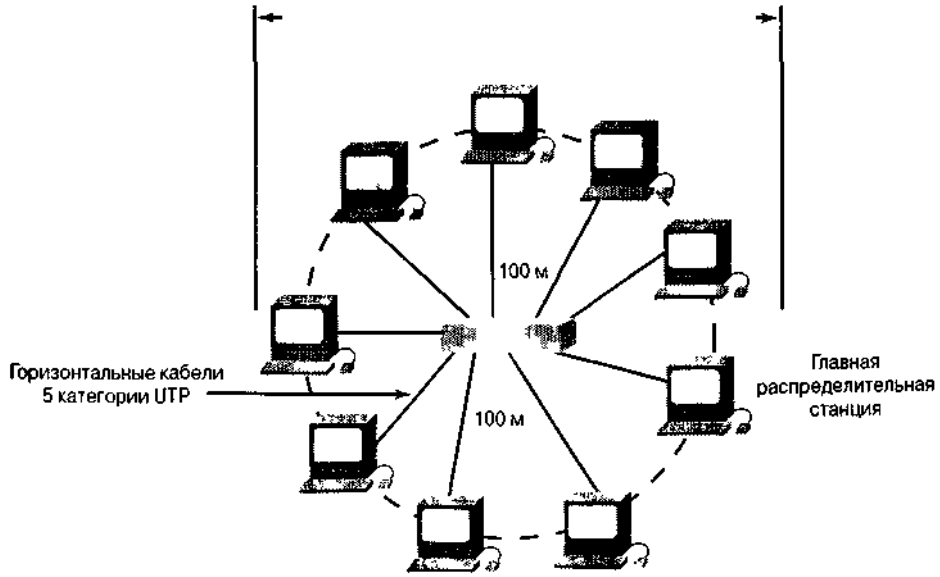


Рис. 4 6 Для реализации малых сетей может потребоваться лишь один монтажный шкаф в центре "звезды"

Таблица 4.1. Характеристики типов кабелей и параметры стандарта IEEE 802.3

Скорость передачи	10 Мбит/с	10 Мбит/с	100 Мбит/с	100 Мбит/с
Метод передачи сигналов	Базовая полоса	Базовая полоса	Базовая полоса	Базовая полоса
Тип носителя	Кабель пятой категории UTP	Оптоволоконный кабель	Кабель пятой категрии UTP	Многомодовое волокно
Максимальная длина	100 метров	2000 метров	100 метров	400 метров

Звездообразная топология

В простой звездообразной топологии с одним монтажным шкафом, показанной на рис. 4.7, ГРС включает одну или более горизонтальных **кросс-соединительных (horizontal cross-connect, HCC)** коммутационных панелей. Кабели горизонтальных коммутационных панелей используются для соединения горизонтальной проводки (физический уровень) с портами коммутатора локальной сети (канальный уровень). Восходящий порт коммутатора (который не похож на остальные порты, поскольку не имеет перекрестных соединений) подсоединен к Ethernet-порту маршрутизатора сетевого уровня посредством кабеля связи. В этой точке конечный хост имеет физическое соединение с портом маршрутизатора.

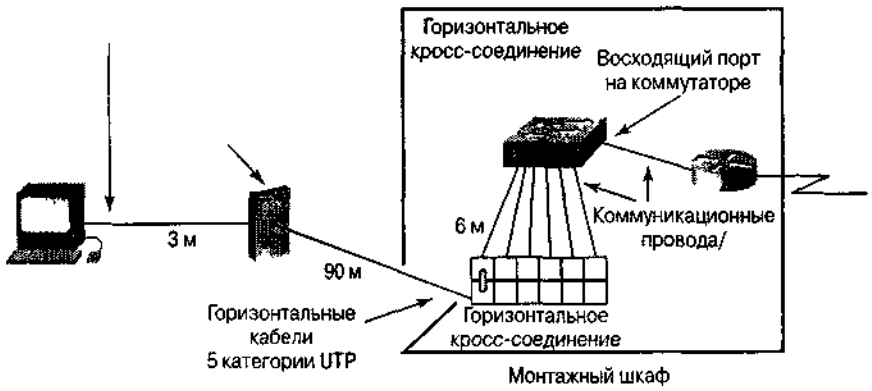


Рис. 4.7. Количество горизонтальных кабельных трасс и размер (количество портов) горизонтальных коммутационных панелей должны быть определены в соответствии с требованиями пользователей.

Вашингтонский проект: дренажная область

Следует сделать обзор пользовательских требований проекта для определения ожиданий пользователей относительно числа горизонтальных кабельных трасс к каждой комнате, которая попадает в дренажную область (catchment area) ГРС или ПРС.

Расширенная звездообразная топология

В крупных сетях обычной практикой является установка более чем одного монтажного шкафа. Это происходит в случае, если имеются подключаемые компьютеры, находящиеся за пределами 100-метрового ограничения длины кабеля пятой категории UTP Ethernet. Путем установки нескольких монтажных шкафов создается множество дренажных областей. Вторичные монтажные шкафы подключаются к ПРС (рис. 4.8). В стандартах EIA/TIA 568 указывается, что ПРС должны подключаться к ГРС с использованием **вертикальной прокладки кабеля (vertical cabling).** Этот вид прокладки называется также **магистральным (backbone cabling).**

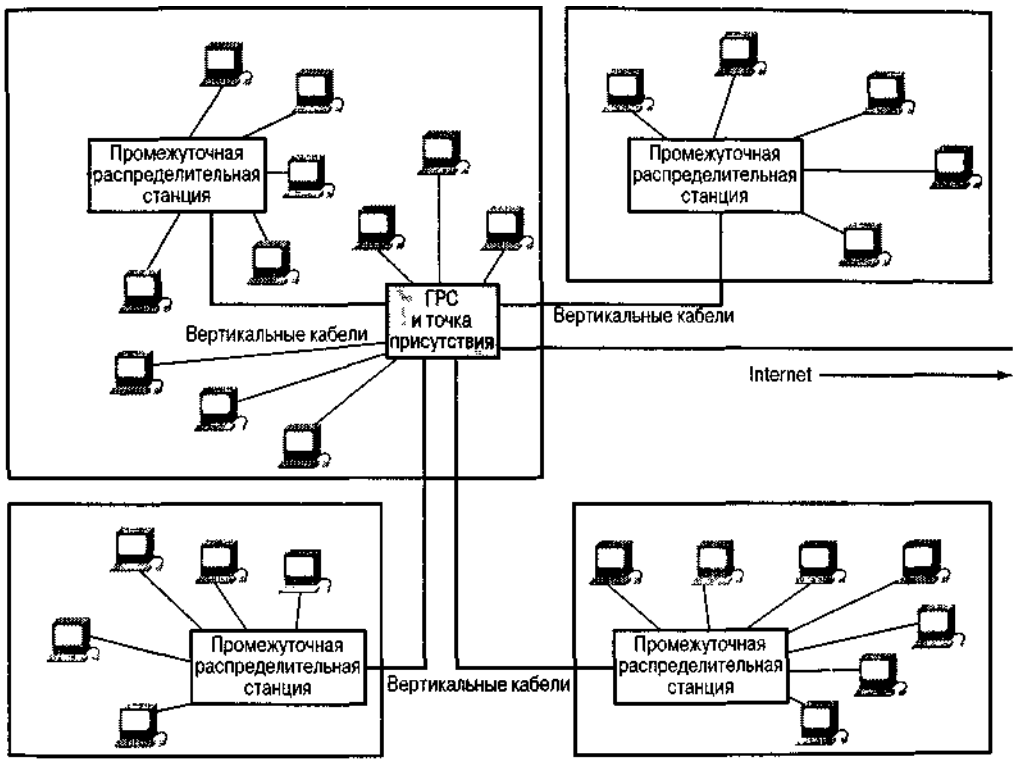


Рис. 4.8. Расширенная звездообразная топология в зданиях студенческого городка

Как показано на рис. 4.9, **вертикальное кросс-соединение (vertical cross-connect,**VCC) используется для подключения разных ПРС к центральной ГРС. Поскольку длина вертикальных кабелей обычно превышает 100-метровое ограничение для пятой категории UTP, в вертикальных кросс-соединениях применяются оптоволоконные кабели (рис. 4.10).

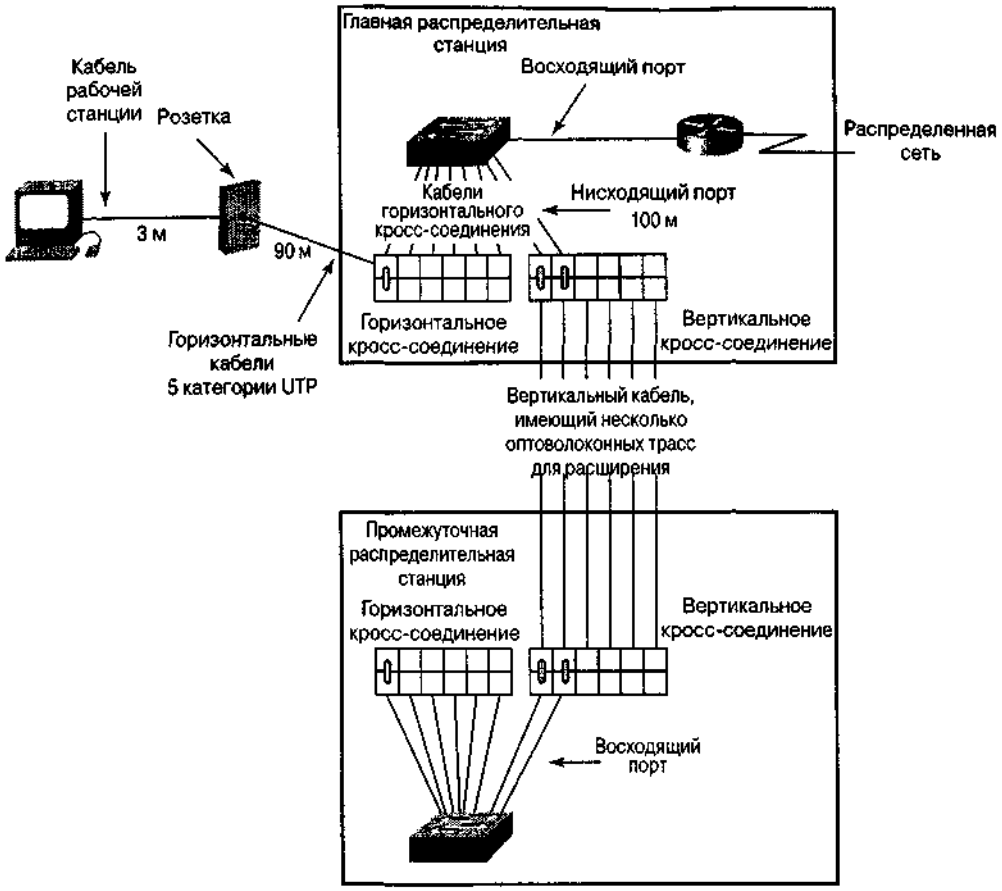


Рис 4.9 Основное отличие между ГРС и ПРС — это появление дополнительной коммутационной панели, которая может быть вертикальным кросс-соединением

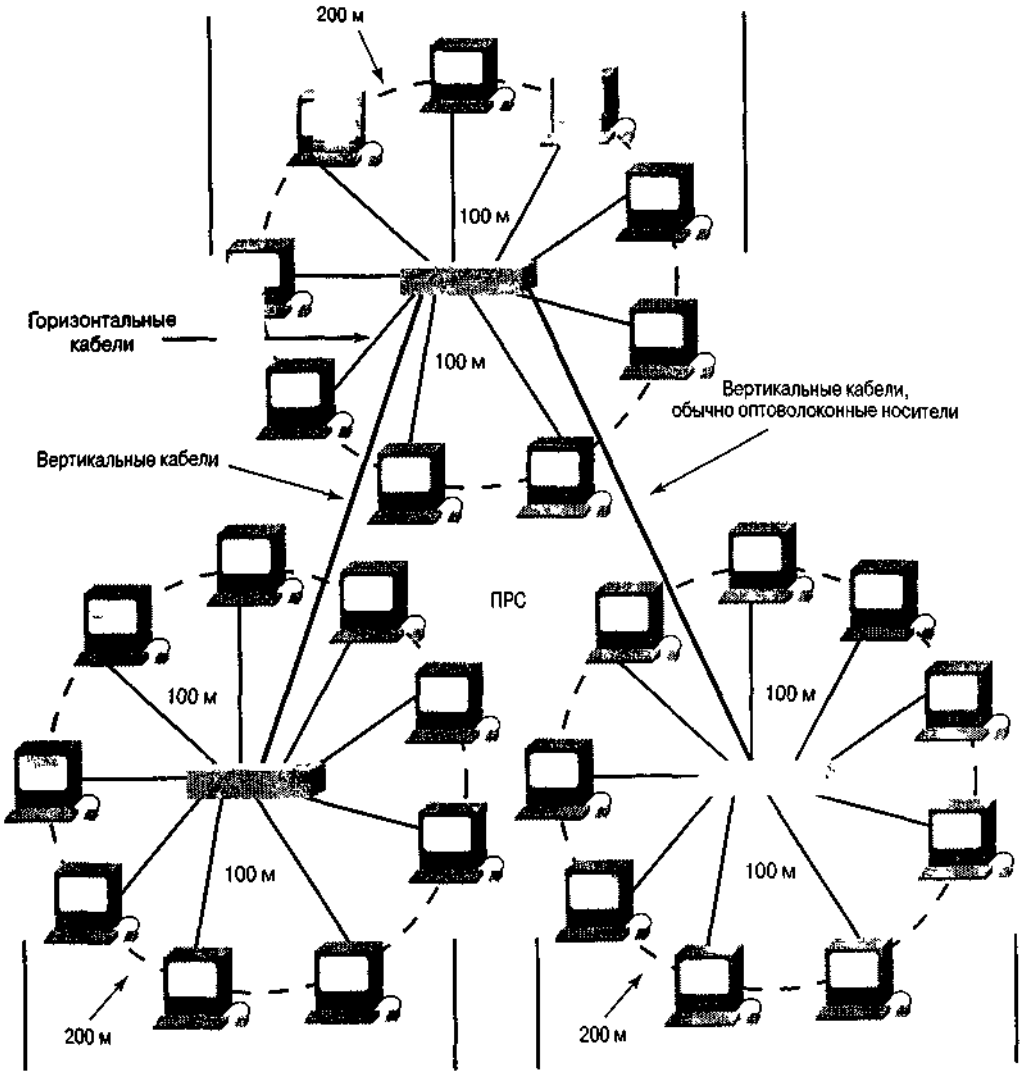


Рис. 4.10.. Все вертикальные кабели подсоединяются к ГРС для создания одного сегмента локальной сети

Вашингтонский проект: скорости соединения

В проектируемой сети весь поток данных между ПРС и ГРС будет перемещаться по вертикальному кабелю Следовательно, это соединение нужно проектировать как самое скоростное Все данные, проходящие по сети округа, будут проходить по этому каналу, поэтому он должен иметь полосу пропускания не менее 100 Мбит/с

Fast Ethernet — вертикальный кабель от ГРС к ПРС

Fast Ethernet — это Ethernet, улучшенный до пропускной способности 100 Мбит/с. Этот тип сети использует ориентированную на широковещание логическую шинную топологию **lOBaseT,** наряду с известным методом доступа CSMA/CD для управления доступом к передающей среде (MAC). В настоящее время стандарт Fast Ethernet включает в себя целый ряд различных стан-

дартов, основанных на медной паре (100BaseTX) и оптоволоконном кабеле (100BaseFX). Он используется для соединения ГРС и ПРС, как показано на рис. 4.11.

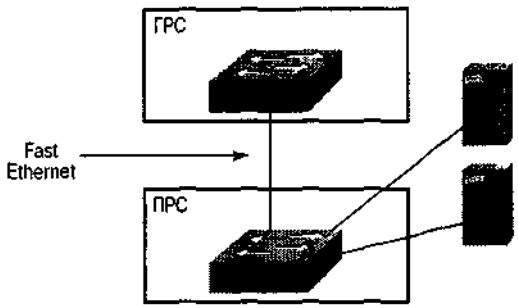


Рис 4.11. Fast Ethernet соединяет ГРС и ПРС, используя 100 Мбит/с полосу пропускания и технологию CSMA/CD

Документация 1 -го уровня

Как показано на рис. 4 12, логическая диаграмма представляет собой модель сетевой топологии без точного указания всех деталей прокладки кабеля. Логическая диаграмма — это основная карта локальной сети. Элементы логической диаграммы включают в себя следующее.

- Точное расположение монтажных шкафов ГРС и ПРС.
- Тип и количество кабеля для соединения ГРС и ПРС, включая количество запасного кабеля для увеличения полосы пропускания между монтажными шкафами. Например, если вертикальный кабель между ПРС1 и ГРС используется на 80%, то можно применить две дополнительные пары для удвоения полосы пропускания.
- Подробную документацию на все кабельные трассы, как показано на врезке (рис. 4.13), идентификационные номера и порт на вертикальном или горизонтальном кросс-соединении, на котором заканчивается трасса. Например,предположим, что 203-я комната потеряла связь с сетью. Изучая врезку, можно выяснить, что эта комната использует трассу 203-1, которая заканчивается на 13-м порте горизонтального кросс-соединения. Теперь можно проверить трассу кабельным тестером, чтобы определить, вызвана ли проблема отказом на 1-ом уровне. Если это так, то для восстановления соединения можно просто использовать одну из двух других трасс, а затем заняться устранением неисправности трассы 203-1.

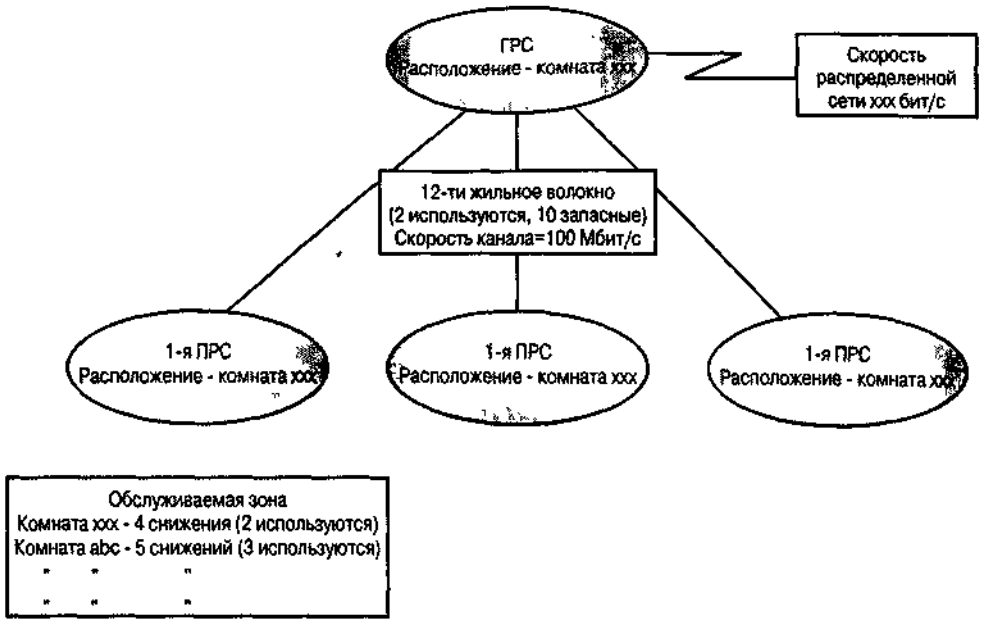


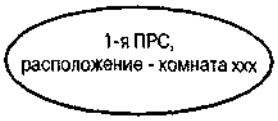
Рис 4.12 Логическая диаграмма — это крупномасштабная карта локальной сети. Она может оказаться полезной при устранении неисправностей и расширении сети в будущем

Вашингтонский проект: требования к схеме соединений локальной сети

В ходе планирования схемы соединений для сети Вашингтонского учебного округа необходимо принять во внимание требования к локальной сети, связанные с доступом пользователей, сегментацией, инфраструктурой, прокладкой кабеля, ГРС и ПРС. При проектировании сети, нужно выполнить описанные ниже требования.

- Первое требование. В каждой школе и окружном офисе необходимо развернуть два сегмента локальной сети. Первый из них предназначен для использования в программе обучения, а второй — для административных целей.
- Второе требование. Инфраструктура локальной сети должна основываться на Ethernet-коммутации, которая позволит перейти на более высокие скорости (т.е к большей полосе пропускания) при обмене данными с отдельными компьютерами и между ГРС и ПРС без изменения физической схемы соединений, а также приспособиться к будущим приложениям Скорости передачи должны соответствовать стандартам Ethernet ЮВазеТ, 100BaseT и 100BaseFX.
- Третье требование. Горизонтальные кабели должны быть пятой категории UTP и иметь возможность пропускать 100 Мбит/с. В вертикальных (магистральных) кабелях необходимо использовать кабели пятой категории UTP или многомодовые оптоволоконные кабели. Кабельная инфраструктура должна соответствовать стандартам EIA/TIA 568.
- Четвертое требование. В каждой школе необходимо разместить ГРС в качестве центральной точки, в которой будут заканчиваться все кабели локальной сети. Она также будет точкой присутствия (point of presence, POP) для соединения с

распределенной (глобальной) сетью. При использовании звездообразной или расширенной звездообразной топологии ПРС должна обслуживать свой участок и подсоединяться к ГРС.



Соединение	Идентификатор кабеля	Кросс-соединение номер пары/ Номер порта	Тип кабеля	Состояние
От1-йПРС к комнате 203	203-1	Горизонтальное кросс-соединение1/порт13	Кабель 5 категории UTP	Используется
От 1-й ПРС к комнате 203	203-2	Горизонтальное кросс-соединение1/лорт14	Кабель 5 категории UTP	Не используется
От 1-й ПРС к комнате 203	203-3	Горизонтальное кросс-соединение2/порт3	Кабель 5 категории UTP	Не используется
От 1-й ПРС кГРС	ПРС1-2	Вертикальное кросс-соединение 1 /порт1	Волокно, используемое а различных режимах	Используется
От 1-й ПРС кГРС	ПРС1-1	Вертикальное кросс - соединение 1 /порт2	Волокно используемое в различных режимах	Используется

Рис 4 13 Такая таблица является ценным пособием при устранении неисправностей на первом (физическом) уровне

Проектирование 2-го уровня топологии локальной сети

Как описывалось в главах 2 , "Коммутация в локальных сетях", и 3, "Виртуальные локальные сети", назначение устройств 2-го уровня состоит в обеспечении управления потоком данных, в обнаружении и коррекции ошибок и уменьшении перегрузок сети Двумя наиболее типичными устройствами 2-го уровня (не считая сетевых адаптеров, которые имеются у каждого хоста сети) являются мосты и коммутаторы Устройства этого уровня определяют размеры коллизионных и широковещательных доменов В настоящем разделе рассматривается реализация коммутации локальных сетей на 2-ом уровне

Вашингтонский проект: цели проектирования 2-го уровня

Ниже описаны цели проектирования топологии 2-го уровня локальной сети для Вашингтонского учебного округа

- Для уменьшения размера коллизионного домена следует устанавливать коммутирующие устройства, использующие микросегментацию

- Следует также создать виртуальные локальные сети и отдельные широковещательные домены, которые будут объединять рабочие группы пользователей.

Коллизии и большой размер коллизионного домена представляют собой два фактора, негативно влияющих на эффективность работы сети. Используя коммутацию, можно микросегментировать сеть, устранив таким образом коллизии, и уменьшить размеры коллизионных доменов Как показано на рис 4 14, еще одна важная черта коммутатора локальной сети состоит в его способности распределять полосу пропускания по портам и предоставлять, таким образом, большую полосу вертикальным и восходящим кабелям, а также серверам. Такой тип коммутации называется асимметричным. Он обеспечивает коммутацию портов с разными полосами пропускания, например, сочетание портов со скоростями 10 и 100 Мбит/с.

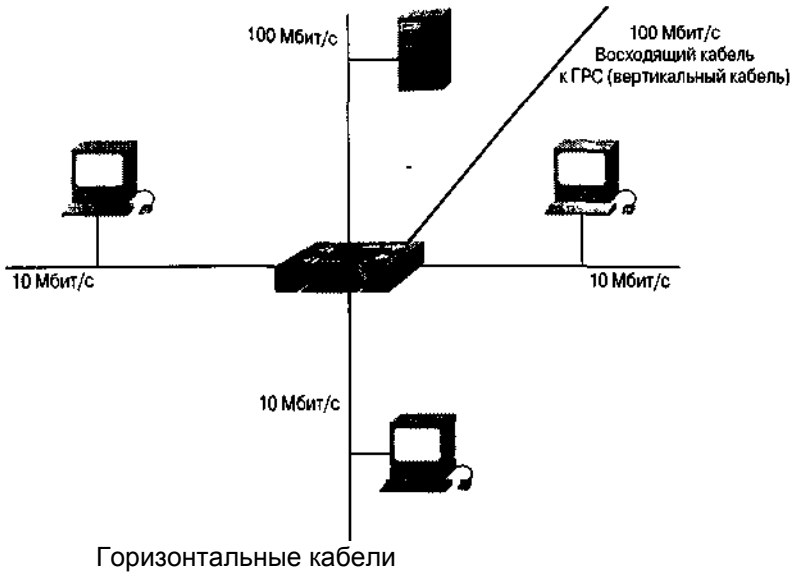


Рис 4 14 Пример асимметричной коммутации

Как было сказано ранее, микросегментация означает использование мостов и коммутаторов для повышения эффективности рабочей группы или магистрали. Обычно повышение эффективности таким способом включает в себя Ethemet-коммугацию. Как показано на рис 4 15, коммутаторы могут использоваться вместе с концентраторами для обеспечения соответствующего уровня эффективности для разных пользователей и серверов

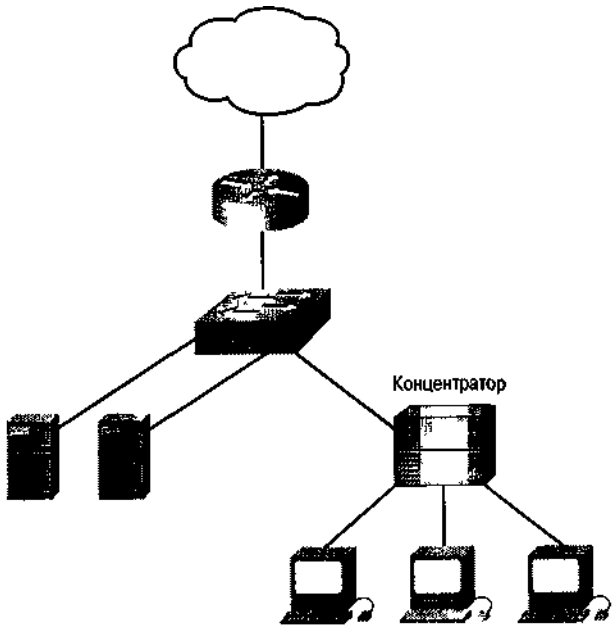


Рис 4 15 Используя микросегментацию для устранения коллизионных доменов, можно избежать перегрузок в локальной сети

Если коммутирующее оборудование локальной сети установлено в ГРС и ПРС и между ними пролегает вертикальный кабель, то по этому кабелю передаются все данные между ГРС и ПРС. Следовательно, пропускная способность этой трассы должна быть больше, чем у трасс между ПРС и рабочими станциями.

Трассы горизонтального кабеля используют пятую категорию UTP, поэтому ни одно кабельное снижение не должно превышать 100 метров. Это позволяет использовать каналы 10 или 100 Мбит/с. В обычных условиях 10 Мбит/с соответствуют горизонтальному кабельному снижению. Поскольку коммутаторы асимметричных локальных сетей позволяют совместное использование портов с полосой пропускания 10 и 100 Мбит/с на одном коммутаторе, следующей задачей является определение числа таких портов, необходимых ГРС и каждой ПРС. Эта задача может быть решена путем повторного изучения требований пользователей, касающихся числа снижений горизонтального кабеля в одной комнате и общего числа снижений в дренажной области, а также числа вертикальных кабельных трасс.

Например, предположим, что в соответствии с требованиями пользователей в каждой комнате должно быть установлено по четыре горизонтальных кабельных трассы. ПРС, обслуживающая дренажную зону, охватывает восемнадцать комнат. Путем несложных арифметических расчетов получаем число портов, равное семидесяти двум.

Вашингтонский проект: требования к топологии локальной сети

При проектировании топологии локальной сети Вашингтонского учебного округа, необходимо помнить ряд требований, предъявляемых к помещениям, из которых будет осуществляться доступ в сеть, и к точкам присутствия (POP) в этих помещениях.

- **Первое требование**. Каждое учебное помещение, которому требуется соединение с сетью, должно обладать возможностью поддерживать 24 рабочих станции и обеспечиваться четырьмя кабельными трассами пятой категории DTP для передачи данных. Одна из них должна подсоединяться к рабочей станции преподавателя. Эти

трассы должны подключаться к ближайшей ГРС или ПРС. Все кабели пятой категории DTP должны быть протестированы на предмет пропускной способности 100 Мбит/с.

- **Второе требование**. В каждом помещении должна быть предусмотрена точка присутствия. Это должен быть закрывающийся на замок кабинет, в котором находятся все кабельные окончания и электронные компоненты (например, концентраторы). Службы данных должны распределяться из этого кабинета в классную комнату по проводам, скрытым декоративными панелями. 1-я сеть должна быть предоставлена для использования в учебной программе, а 2-я сеть — для административных целей.

Коллизионные домены коммутатора второго уровня

Для определения размеров коллизионного домена необходимо знать, сколько хостов физически подключены к одному порту коммутатора. Этот фактор также влияет на полосу пропускания, доступную каждому отдельно взятому хосту.

В идеальном случае только один хост подключен к порту коммутатора. Это означает, что размер коллизионного домена равен двум (хост-источник и хост-адресат). Поскольку такой домен имеет небольшой размер, то в нем практически не должно быть коллизий при обмене данными между двумя хостами.

Другой способ реализации коммутации локальной сети — это установка на порты коммутатора совместно используемых концентраторов. Таким образом, несколько хостов подключаются к одному порту коммутатора (рис. 4.16). Все хосты, подключенные к концентратору, образуют коллизионный домен и делят между собой полосу пропускания (рис. 4.17).

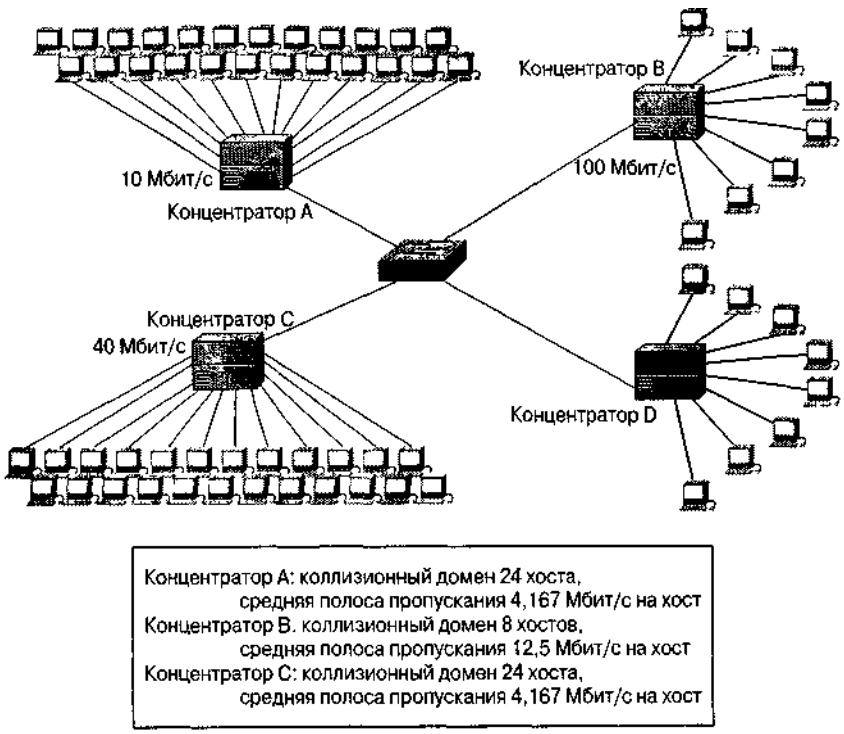


Рис. 4.16. При использовании концентраторов размер коллизионного домена увеличивается, а полоса пропускания делится между хостами

Следует заметить, что некоторые ранние модели коммутаторов, такие как Catalyst 1700, в действительности не могут делить коллизионный домен и полосу пропускания, поскольку не поддерживают множественное назначение MAC-адресов каждому порту. В этом случае число ARP-запросов и широковещательных рассылок становится большим.

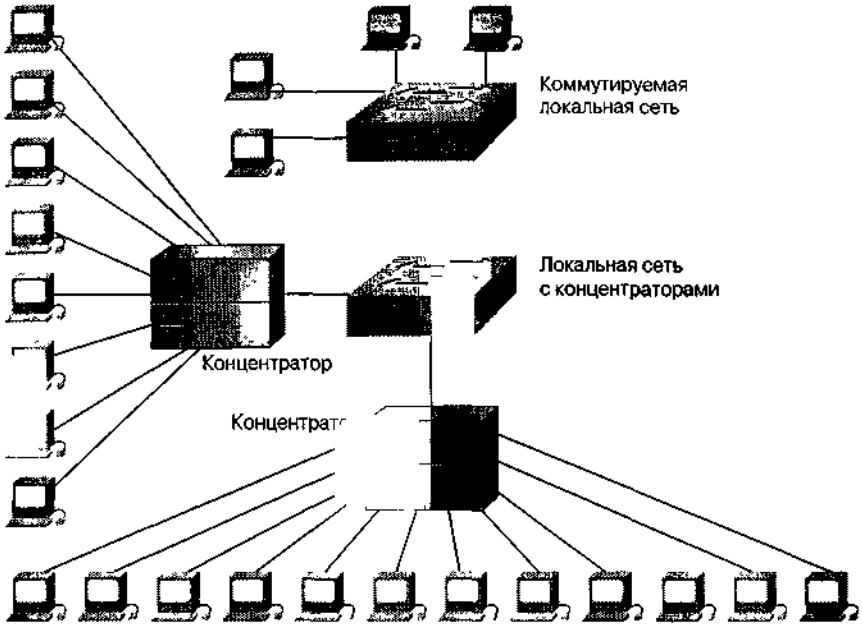


Рис. 4.17. В идеальной локальной сети размер коллизионного домена равен 2. В сети, использующей концентраторы, коллизионный домен становится значительно больше

Использование коммутатора второго уровня вместе с концентраторами

В большинстве случаев концентраторы среды с общим доступом используются в коммутируемой среде локальных сетей для увеличения количества точек подключения на концах горизонтальных кабельных трасс, как показано на рис. 4.18. Такой подход является приемлемым, однако нужно гарантировать, что размеры коллизионных доменов не будут увеличиваться и требования, касающиеся полосы пропускания к хосту, будут выполнены согласно спецификациям, собранным на соответствующем этапе проектирования сети.

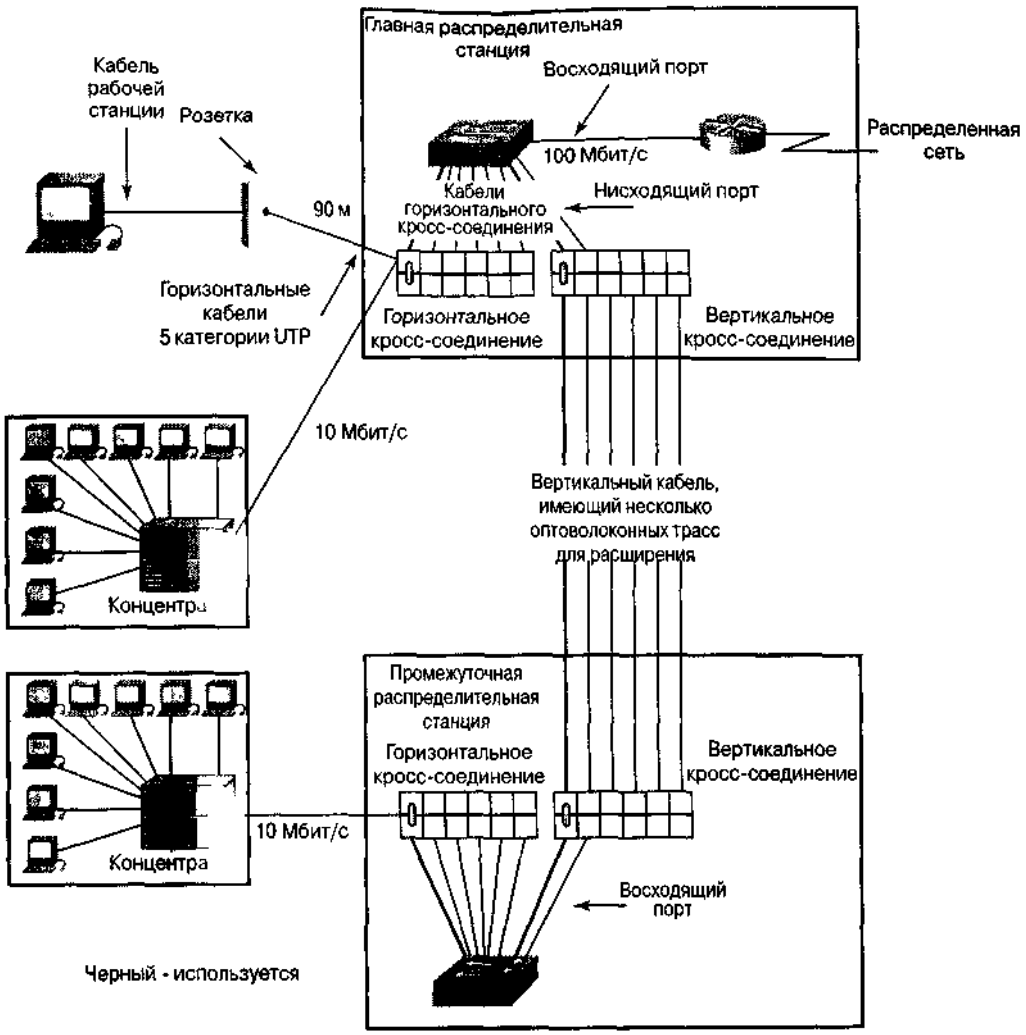


***Рис.** 4.18. Концентраторы можно использовать с целью создания большего количества точек подключения для хоста*

Переход на большую полосу пропускания на 2-ом уровне

При росте сети растет и потребность в большей полосе пропускания. В вертикальных соединениях неиспользуемое оптоволокно можно применить для связи с портом коммутатора, имеющим полосу пропускания 100 Мбит/с. Полоса пропускания сети, показанной на рис. 4.19, удвоена по сравнению с полосой пропускания вертикального кабеля сети, представленной на рис. 4.18. Это происходит за счет внедрения еще одной линии.

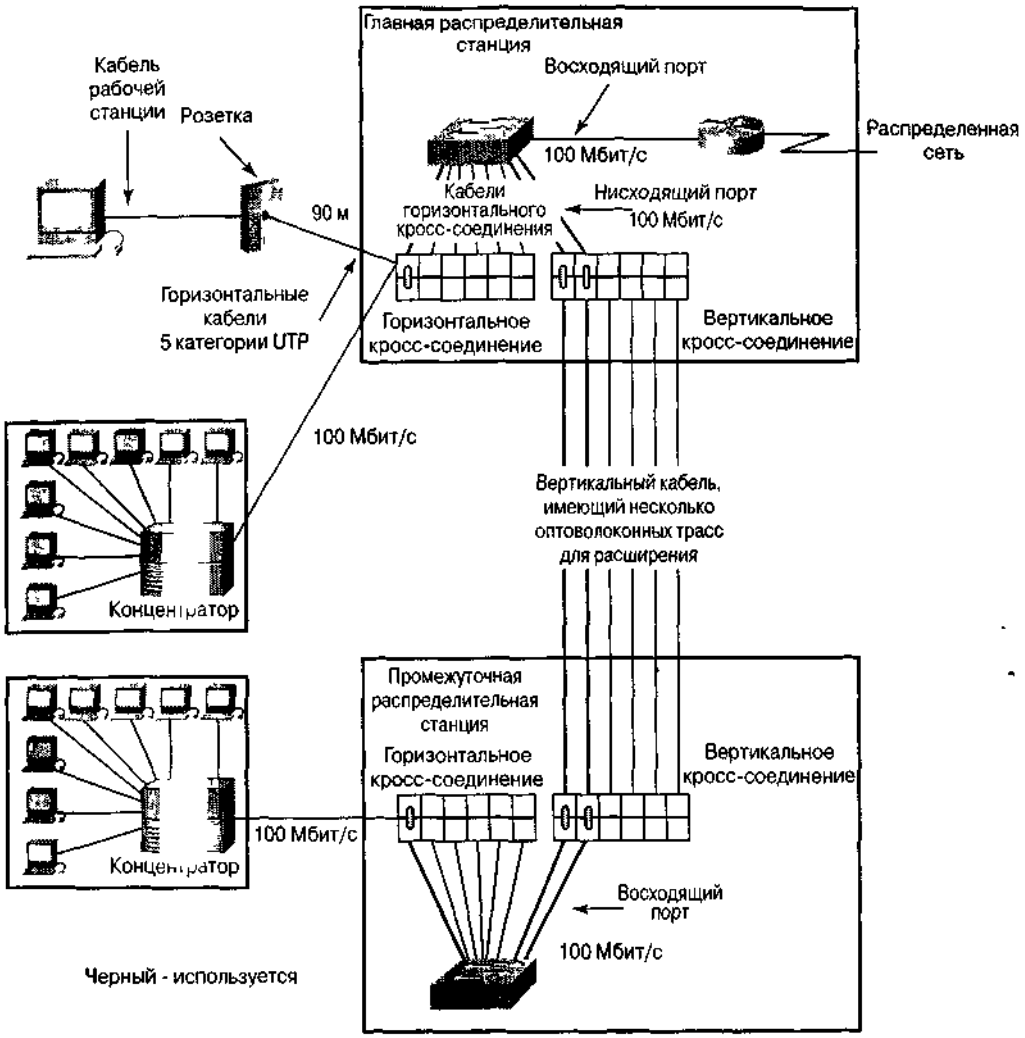


Рис. 4.19. Переход на большую полосу пропускания столь же прост, как подключение к высокоскоростному порту или добавление нескольких таких портов

В случае горизонтального соединения можно увеличить полосу пропускания в десять раз путем перекроссировки с горизонтального кросс-соединения на порт 100 Мбит/с коммутатора и замены концентратора на 10 Мбит/с концентратором на 100 Мбит/с. При установлении параметров коммутатора 2-го уровня локальной сети важно удостовериться в наличии достаточного количества портов на 100 Мбит/с, чтобы осуществить переход на большую полосу пропускания. Важно также занести в пакет документов по сети быстродействие каждого активного кабельного снижения.

Проектирование 3-го уровня топологии локальной сети

Устройства 3-го (сетевого) уровня, такие как маршрутизаторы, могут использоваться для создания отдельных сегментов локальной сети и обеспечения обмена информацией между сегментами, основываясь на адресации 3-го уровня, т.е. на IP-адресах. Внедрение устройств 3-го уровня, например маршрутизаторов, позволяет осуществить сегментацию локальной сети на обособленные физические и логические сети. Маршрутизаторы также позволяют подключаться к распределенным сетям (Wide-Area Network, WAN), таким как Internet.

Вашингтонский проект: цели проектирования 3-го уровня

Цели проектирования 3-го уровня топологии сети Вашингтонского учебного округа состоят в следующем.

- Построить путь между сегментами локальной сети, на котором будет происходить фильтрация потока данных.
- Изолировать широковещание протокола ARP.
- Разделить коллизии в сегментах.
- Обеспечить фильтрацию служб 4-го уровня между сегментами.

Установка в сети маршрутизатора 3-го уровня

Как показано на рис. 4.20, маршрутизация 3-го уровня определяет транспортировку потока данных между отдельными физическими сегментами сети такими, как IP-сеть и подсеть, основываясь на адресации 3-го уровня. Маршрутизатор представляет собой одно из наиболее мощных устройств в сети.

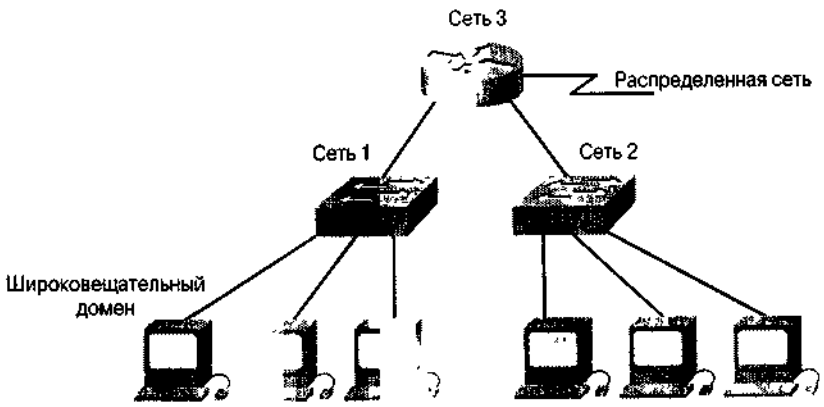


Рис. 4.20. Маршрутизация 3-го уровня решает такие вопросы, как необходимость физического разделения подсетей

Как известно, маршрутизатор перенаправляет пакеты данных, основываясь на адресах пунктов назначения. Вместе с тем, маршрутизатор не перенаправляет широковещательные рассылки локальных сетей, такие как ARP-запросы. Следовательно, интерфейс маршрутизатора рассматривается как точка входа-выхода широковещательного домена, которая предотвращает переход широковещательных рассылок из одних сегментов локальной сети в другие.

Реализация виртуальных локальных сетей

Одной из важнейших характеристик сети является общее количество широковещательных рассылок, таких как ARP-запросы. Используя виртуальные локальные сети, можно ограничить

поток широковещательных сообщений внутри сети и, таким образом, уменьшить широковещательный домен (рис. 4.21). Виртуальные сети могут также использоваться для обеспечения безопасности, путем создания групп в виртуальных сетях согласно функциям этих групп (рис. 4.22).

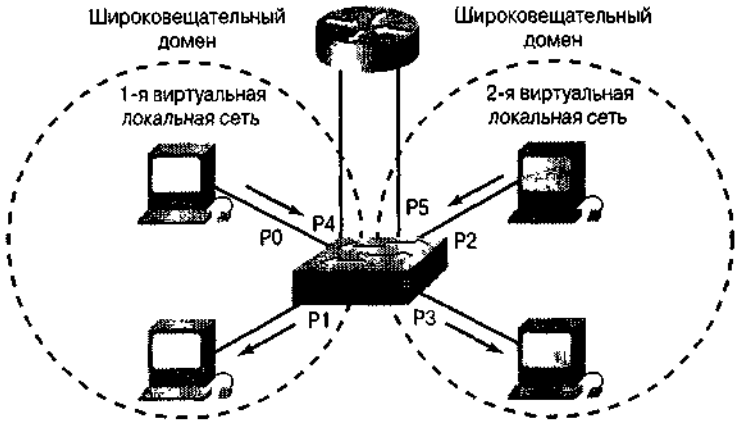


Рис 4 21 Маршрутизаторы обеспечивают обмен информацией между виртуальными локальными сетями

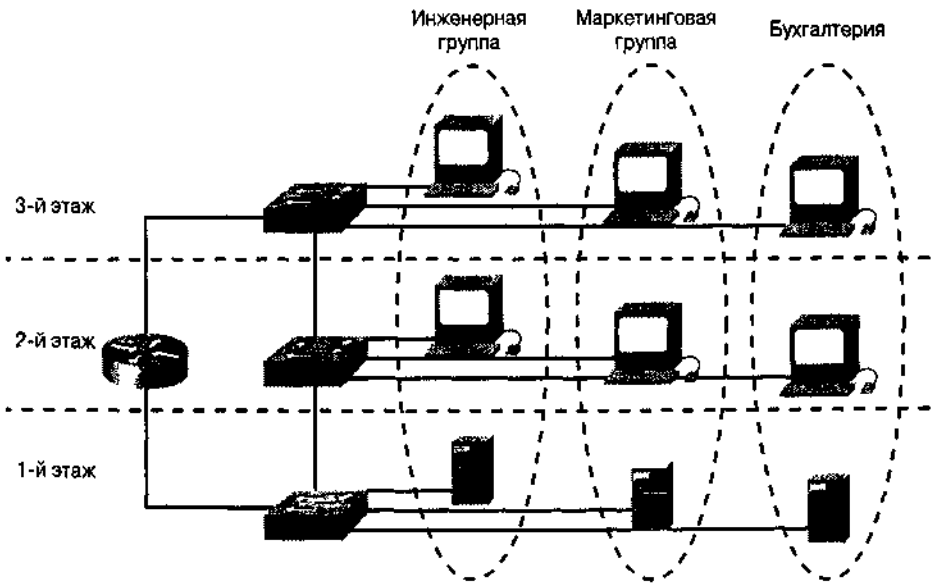


Рис 4 22. Виртуальные локальные сети сдерживают широковещание и повышают безопасность.

На рис. 4.21 физические порты используются для назначения виртуальной сети. Порты P0, P1, и P4 назначены виртуальной сети 1, а порты P2, P3, и P5 — виртуальной сети 2. Обмен информацией между виртуальными сетями 1 и 2 может происходить только через маршрутизатор. Эта схема ограничивает размеры широковещательных доменов и использует маршрутизатор для того, чтобы определить, может ли виртуальная сеть 1 обмениваться данными с виртуальной сетью 2. Это создает возможность увеличения безопасности, основанную на назначениях виртуальной сети.

Использование маршрутизаторов для создания расширяемых сетей

Маршрутизаторы обеспечивают расширяемость, так как они могут служить в качестве брандмауэров для широковещательных рассылок, как показано на рис. 4.20.

Кроме того, поскольку адреса 3-го уровня обычно являются структурированными, маршрутизаторы могут обеспечивать большую расширяемость путем разделения сетей и подсетей, и, следовательно, структурируя эти адреса (рис. 4.23). Способы, которыми можно достичь большей расширяемости сетей, описаны в табл. 4.2. Когда сети разделены на подсети, последним шагом является разработка и документирование схемы IP-адресации, используемой в сети.

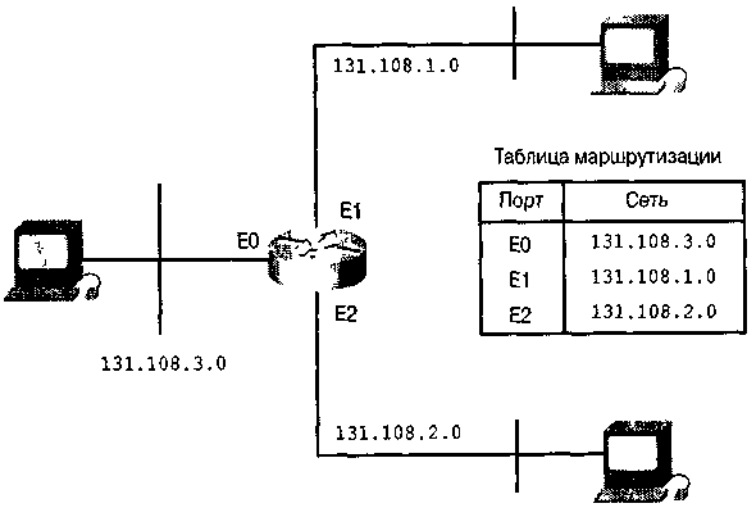


Рис 4 23 Маршрутизатор структурирует сеть, разделяя сети и подсети

Таблица 4.2. Логическая адресация и соответствующая ей физическая реализация

Таблица 4.2. Логическая адресация и соответствующая ей физическая реализация

Логический адрес	**Физическое сетевое устройство**
x.x.x.1-x.x.x.10	Маршрутизатор, локальная сеть, порты распределенной сети
X.X.X.11-X.X.X.20	Коммутаторы локальных сетей
X.X.X.21-X.X.X.3O	Серверы предприятия
X.X.X.31-X.X.X.80	Серверы рабочих групп
X.X.X.81-X.X.X.254	ХОСТЫ

Технология маршрутизации обеспечивает фильтрацию широковещательных и многоадресных рассылок канального уровня Добавляя порты маршрутизатора с дополнительными **адресами сети (network addresses)** или **подсети,** можно сегментировать сеть в соответствии с текущими требованиями. Адресация и маршрутизация, используемые сетевыми протоколами, обеспечивают встроенное расширение. При решении вопроса о том, что использовать — маршрутизатор или коммутатор, необходимо ответить на вопрос: "Какую проблему необходимо решить?" Если проблема связана скорее с протоколом, чем с конкуренцией в сети, то следует использовать маршрутизатор. Маршрутизаторы решают проблемы, связанные с чрезмерным широковещанием, плохо масштабируемыми протоколами, аспектами безопасности и адресацией сетевого

уровня. В то же время, маршрутизаторы стоят дороже и сложнее в настройке, чем коммутаторы.

Вашингтонский проект: адресация

Окружной офис должен разработать полную схему TCP/IP-адресации и соглашение об именах для всех хостов, серверов и межсетевых устройств. Следует запретить использование несанкционированных адресов. В административных сетях все компьютеры должны иметь статические адреса. Учебные компьютеры должны получать адреса, используя протокол динамического конфигурирования хостов (Dynamic Host Configuration Protocol, DHCP). DHCP предоставляет механизм динамического распределения IP-адресов таким образом, чтобы можно было многократно использовать адреса, которые, по каким-либо причинам, больше не нужны хостам (например, отключенным или отсоединенным компьютерам)

Использование маршрутизаторов для логического структурирования

Как показано на рис. 4.23, маршрутизаторы можно использовать для реализации IP-подсетей путем структурирования адресов. Мосты и маршрутизаторы должны отбрасывать все неизвестные адреса с каждого порта. Маршрутизаторы помогают хостам, использующим протоколы адресации сетевого уровня, отыскать другие хосты, без использования лавинной передачи. Если адрес пункта назначения является локальным, то посылающий хост может инкапсулировать данные в заголовок канального уровня и отправить фрейм непосредственно адресату. Маршрутизатор не видит этот фрейм и, естественно, не нуждается в лавинной передаче. Есть вероятность, что передающему хосту придется использовать АКР, что повлечет за собой широковещание. Однако, широковещание — локальное явление и не распространяется маршрутизатором. В случае, когда адресат не является локальным, посылающая станция передает пакеты маршрутизатору. Маршрутизатор отправляет фреймы по назначению или к следующему переходу, основывая свой выбор на собственной таблице маршрутизации. Исходя из приведенной выше функциональности, можно сделать вывод, что в крупных, расширяемых сетях необходимо использовать маршрутизаторы.

Использование маршрутизаторов 3-го уровня для сегментации

На рис. 4.24 приведен пример реализации системы, в которой есть несколько физических сетей. Весь поток данных из сети 1, предназначенный для сети 2, должен пройти через маршрутизатор. В приведенной реализации сети есть два широковещательных домена. Две сети имеют уникальные IP-адресации (адресные схемы сеть/подсеть).

В структурированной кабельной схеме 1-го уровня легко создавать многочисленные физические сети путем простого соединения вертикальных и горизонтальных кабелей с соответствующим коммутатором 2-го уровня. В следующих главах рассказывается, как подобный подход обеспечивает надежную реализацию защиты. И, наконец, следует напомнить, что маршрутизатор в локальной сети является центральной точкой прохождения потока данных.

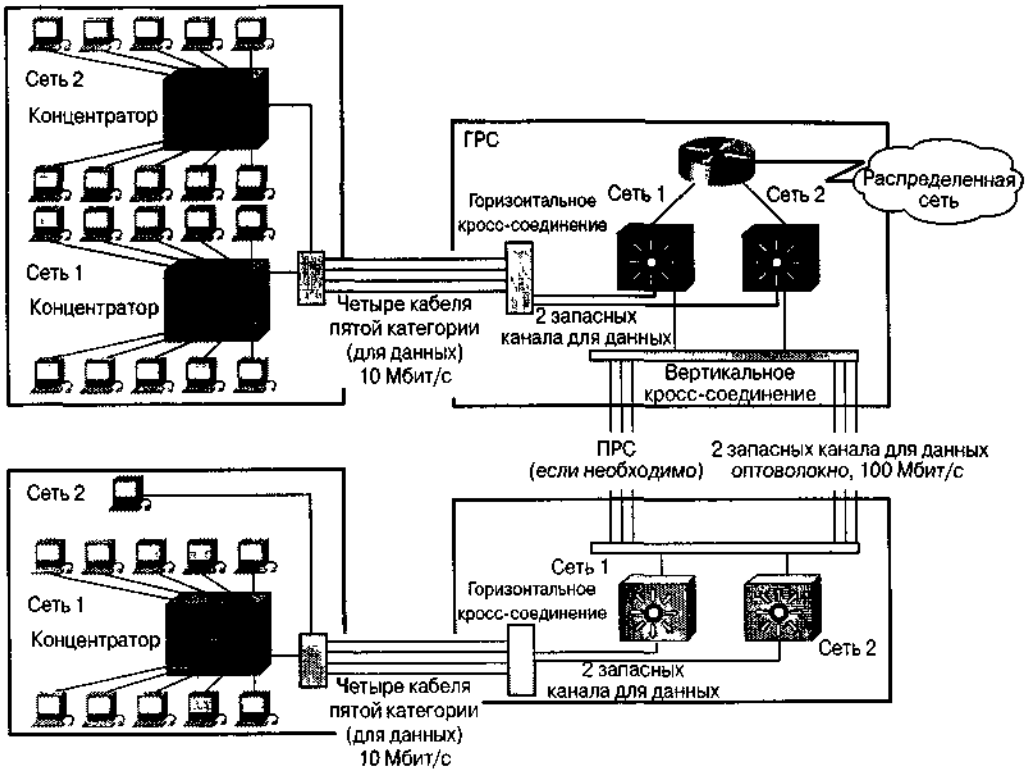


Рис. 4 24 В этой реализации маршрутизатор служит центральной точкой для направления потока данных в локальной сети, это также обеспечивает надежную защиту

Документирование логической и физической реализации сети

После разработки схемы IP-адресации для заказчика следует составить соответствующие документы для каждого ее участка и для сети внутри этого участка, как показано в табл. 4.2. Следует установить стандартное соглашение для адресации важнейших хостов в сети. Эта схема не должна содержать противоречий внутри всей сети (рис. 4.25). Создав карту адресации, вы получите снимок сети (рис. 4.26), а создание физической карты, изображенной на рис. 4.27 поможет при устранении сетевых неисправностей.

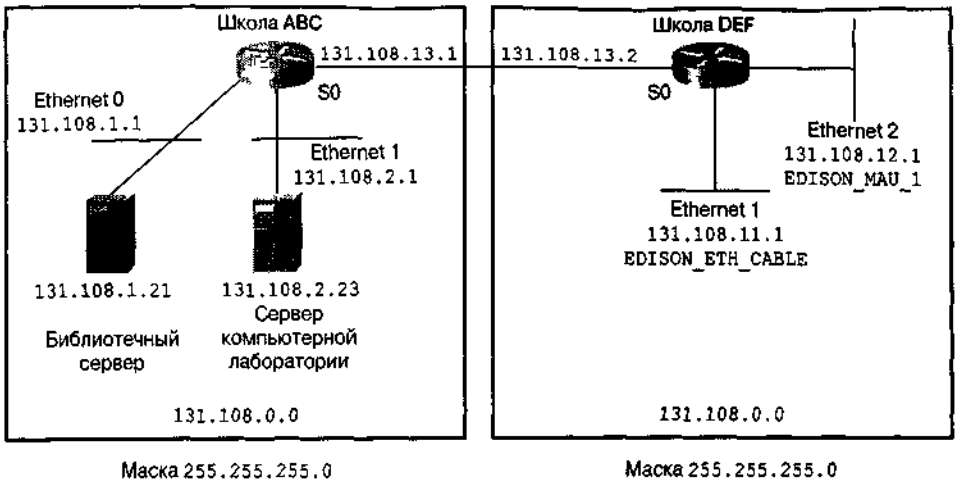


Рис. 4.25. В хорошо документированной сети легко устранять возникающие неисправности

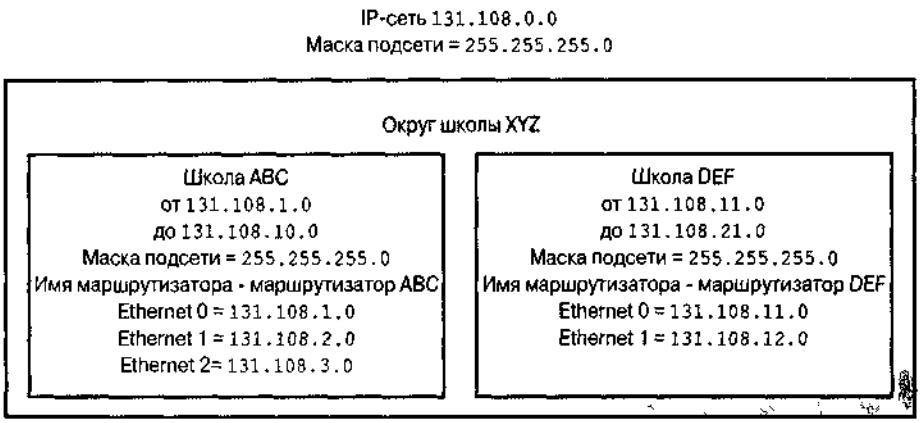


Рис. 4 26. Сети с хорошей документацией, такой как эта, значительно уменьшают груз сетевых проблем

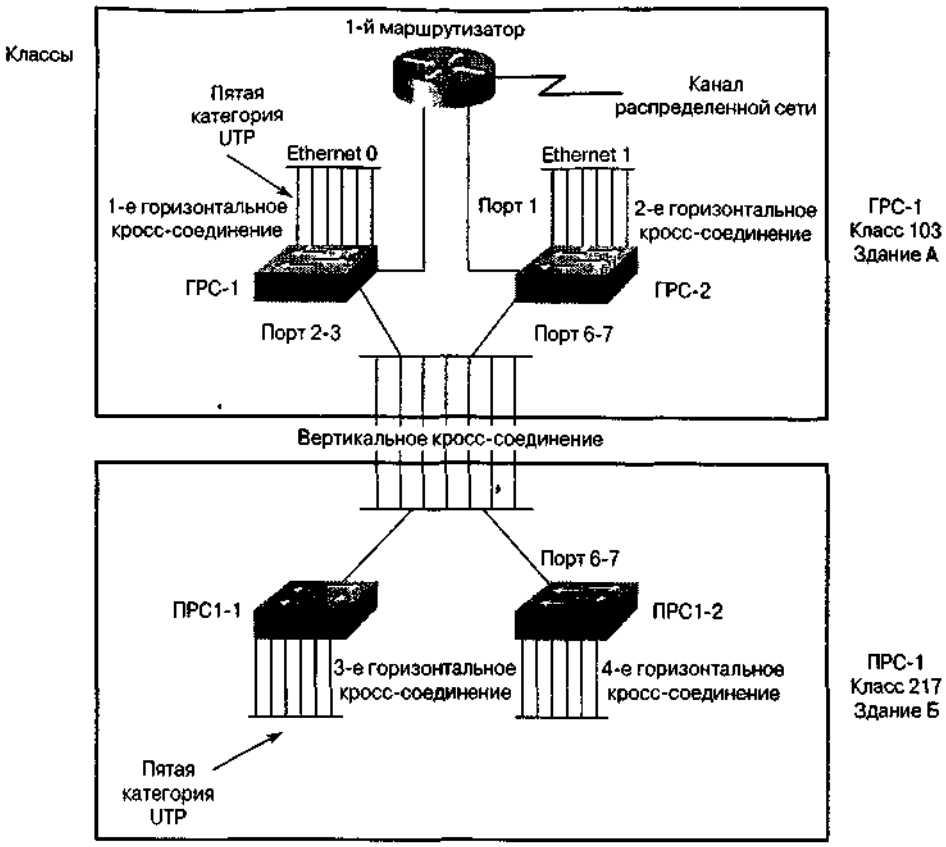


Рис. 4.27 Физическая карта показывает, где находятся ГРС и ПРС, а также точки подключения хостов к сети

Резюме

Одним из наиболее важных факторов в обеспечении быстрой и устойчивой работы сети является ее проектирование. Неудачное проектирование может привести к возникновению множества непредвиденных проблем, а рост сети будет затруднен или станет невозможным.

- Цели проектирования локальных сетей включают в себя функциональность, расширяемость, адаптируемость и управляемость.
- Вопросы проектирования сети включают в себя функции и размещение серверов, обнаружение ошибок и сопоставление широковещательных и широкополосных доменов.
- Процесс проектирования включает в себя следующие этапы:
- сбор пользовательских требований и ожиданий;
- определение нагрузки в настоящее время и в будущем, с учетом возможного роста сети и характера размещения серверов;
- определение всех устройств 1-го, 2-го и 3-го уровней наряду с топологиями локальной и распределенной сети;
- документирование физической и логической реализации сети.

Задачи проекта Вашингтонского учебного округа: проектирование локальной сети

В этой главе были изложены концепции, которые помогут начать процесс проектирования сети Вашингтонского учебного округа. При этом необходимо будет решить следующие задачи.

1. Собрать всю информацию необходимую для разработки локальной сети Вашингтонского учебного округа.
2. Спроектировать локальную сеть, основываясь на схеме адресации сети Вашингтонского учебного округа.
3. Разработать документацию на весь проект локальной сети, основываясь на требованиях округа и пользователей.

Для правильного проектирования сети Вашингтонского учебного округа и решения всех указанных задач необходимо следующее.

- Перечень пользовательских требований.
- Общая документация проекта, которая включает логическую модель локальной сети школы, а также полная документация на физическую конструкцию сети, включающая:
- детальное описание всех ГРС и ПРС в учебных помещениях, включая масштабную диаграмму;
- количество вертикальных и горизонтальных кросс-соединений и портов, а также коммутаторов локальной сети для удовлетворения существующих и планируемых в будущем потребностей.
- Спецификации на тип и количество кабельных носителей для всех горизонтальных и вертикальных кабельных трасс.
- Спецификации по безопасности, виртуальным локальным сетям и отдельно по сетям персонала и учащихся.
- Общую схему IP-адресации округа.

Контрольные вопросы

Дайте ответы на приведенные ниже вопросы для проверки понимания тем и понятий, изложенных в этой главе. Ответы приведены в приложении А.

1. Назовите основные цели любого сетевого проекта.
2. Каково назначение устройств 2-го уровня в сетевом проекте?
3. Каково назначение устройств 3-го уровня в сетевом проекте?
4. Каковы две основные категории серверов, которые следует рассматривать в процессе проектирования сети, и каково их назначение?
5. Для каких главных аспектов сети должны быть составлены соответствующие документы и почему?
6. Что из перечисленного ниже вероятнее всего вызовет перегрузку в сети?
   A. Доступ в Internet.
   B. Доступ к главной базе данных.
   C. Передача графики и видео.
   D. Все перечисленное.
7. Что из перечисленного ниже не вызывает чрезмерного широковещания?
   A. Слишком много клиентских пакетов, запрашивающих службы.
   B. Слишком много серверных пакетов, предоставляющих службы.
   C. Слишком много обновлений таблиц маршрутизации.
   D. Слишком много сетевых сегментов.
8. Основная цель проектирования канального уровня — это выбор устройств___, таких как

мосты или коммутаторы локальных сетей, используемых для соединения носителей_____ с целью образования сегментов локальных сетей?

A. 3-го уровня; 2-го уровня;
B. 1-го уровня; 2-го уровня;
C. 2-го уровня; 1-го уровня;
D. 2-го уровня; 3-го уровня.

9. Какая из следующих характеристик не верна для lOBaseT?

A. Скорость передачи — 10 Мбит/с.
B. Максимальная длина — 400 метров.
C. Метод передачи сигналов — полоса пропускания.
D. Носитель — кабель пятой категории UTP.

10. Что является преимуществом использования устройств 3-го уровня в локальной сети?

A. Оно позволяет разделять локальную сеть на уникальные физические и логические сети.
B. Оно фильтрует широковещание и многоадресные рассылки канального уровня и позволяют подключаться к распределенным сетям.
C. Оно обеспечивает логическое структурирование сети.
D. Все перечисленное.

Основные термины

100BaseFX. 100-Мбит/с стандарт Fast Ethernet, использующий два многожильных, многорежимных оптоволоконных кабеля на каждое соединение. Чтобы гарантировать соответствующую синхронизацию сигнала, lOOBaseFX-соединение не должно превышать 400 метров в длину. Основан на стандарте ШЕЕ 802.3.

100BaseTX. 100-Мбит/с стандарт Fast Ethernet, использующий две пары UTP или STP. Первая пара используется для получения данных, вторая — для передачи. Для обеспечения соответствующей синхронизации длина сегмента не может быть больше 100 метров. Основан на стандарте IEEE 802.3.

lOBaseT. Стандарт сети Ethernet для полосы частот 10 Мбит/с с использованием двух проводов типа "витая пара" (3, 4 или 5 категории). Одна пара предназначена для передачи данных, а другая — для получения. lOBaseT — часть стандарта IEEE 802.3 и имеет ограничение длины сегмента равное примерно 100 метрам.

EIA/TIA-568. Стандарт, описывающий характеристики и приложения для различных категорий UTP кабеля.

Ethernet. Спецификация локальных сетей, предложенная корпорацией Xerox и разработанная совместно Xerox, Intel и Digital Equipment Corporation. Сети Ethernet используют CSMA/CD и работают с различными типами кабелей со скоростью 10 Мбит/с. Стандарт Ethernet аналогичен серии стандартов IEEE 802.3.

Fast Ethernet. Спецификации Ethernet для скоростей до 100 Мбит/с. Fast Ethernet предлагает десятикратную, по сравнению с lOBaseT, скорость, сохраняя при этом такие характеристики, как формат фрейма, механизмы MAC и MTU. Подобное сходство позволяет использовать существующие lOBaseT-приложения и сетевые управляющие механизмы в сетях Fast Ethernet. Основан на расширении спецификации IEEE 802.3.

Intranet. Внутренняя сеть организации, к которой имеют доступ пользователи.

Асимметричная коммутация (asymmetric switching). Тип коммутации, обеспечивающий коммутируемые соединения портов с разной шириной полосы пропускания. Например, порты на 10 и 100 Мбит/с.

Вертикальная прокладка кабеля (vertical cabling). См. *магистральная прокладка кабеля.*

Вертикальное кросс-соединение (vertical cross-connect, VCC). Соединение, которое используется для подключения разных ПРС к центральной ГРС.

Волоконно-оптический кабель (fiber-optic cable). Физическая среда, способная передавать модулированные световые сигналы. Оптоволоконный кабель стоит дороже по сравнению с другими видами передающих сред, однако он не восприимчив к электромагнитной интерференции и способен передавать данные с более высокой скоростью. Иногда его называют *оптоволокном (optical fiber).*

Главная распределительная станция, ГРС (main distribution facility, MDF). Первичный коммуникационный зал здания. Центральная точка звездообразной сетевой топологии, где расположены коммуникационные панели, концентраторы и маршрутизаторы.

Горизонтальное кросс-соединение (horizontal cross-connect, HCC). Монтажный шкаф, где горизонтальные кабели подсоединяются к коммуникационной панели, которая, в свою очередь, соединена магистральным кабелем с ГРС.

Дренажная область (catchment area). Зона, входящая в область, которую обслуживает устройство сетевого взаимодействия (например, концентратор).

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

Инкапсуляция (encapsulate). Перенести данные в заголовок конкретного протокола. Например, в сетях Ethernet перед передачей данные переносятся в Ethernet-заголовок. То же происходит при соединении разных сетей: внутренний фрейм одной сети помещается в заголовок, который используется протоколом канального уровня другой.

Кабель 5-ой категории (category 5 cabling). Одна из пяти категорий UTP кабелей, описанная в стандарте EIA/TIA 568B. Кабель пятой категории может передавать данные на скоростях до 100 Мбит/с.

Конкуренция (contention). Метод доступа, при котором сетевые устройства конкурируют друг с другом за доступ к передающей среде.

Лавинная передача (flooding). Техника передачи данных, используемая коммутаторами и мостами. Поток данных, полученный устройством, отправляется дальше через все интерфейсы этого устройства, исключая принявший интерфейс.

Локальная сеть (local-area network, LAN). Высокоскоростная, надежная сеть передачи данных, охватывающая относительно малую географическую площадь (до нескольких тысяч метров). Локальные сети соединяют рабочие станции, терминалы, периферийные и другие устройства, находящиеся в одном здании или другом географически ограниченном пространстве. Стандарты локальных сетей определяют прокладку кабеля и прохождение сигналов на физическом и канальном уровнях эталонной модели OSI. Ethernet, FDDI и Token Ring - примеры широко используемых технологий локальных сетей.

Магистральная прокладка кабеля (backbone cabling). Прокладка соединительных кабелей между монтажными шкафами, между монтажными шкафами и точкой присутствия (POP), а также между зданиями, являющимися частью одной локальной сети.

Неэкранированная витая пара (unshielded twisted-pair, UTP). Кабель из четырех пар, использующийся для различных сетей. UTP не требует фиксированного пространства между соединениями, которое необходимо для коаксиальных кабелей. Всего существует пять часто используемых типов кабелей UTP. Они называются категориями с первой по пятую.

Одиночная передача (unicast). Сообщение, направленное единственному адресату.

Передающая среда (media). Различные носители, через которые проходят сигналы. Наиболее распространенные сетевые среды: витая пара, коаксиальный кабель, оптоволоконный кабель и атмосфера (через которую осуществляется высокочастотная, лазерная и инфракрасная передача). Иногда также называется *физической средой (physical media).*

Промежуточная распределительная станция, ПРС (intermediate distribution facility, IDF). Вторичное коммуникационное помещение здания, в котором используется звездообразная сетевая топология. ПРС зависима от ГРС.

Протокол (protocol). Формальное описание набора соглашений и правил, которые определяют обмен информацией между устройствами в сети.

Распределенная сеть (wide-area network, WAN). Сеть передачи данных, охватывающая

значительное географическое пространство. Часто использует передающие устройства, предоставленные общими поставщиками каналов связи. В качестве примеров технологий распределенных сетей можно назвать Frame Relay, SMDS и X.25.

Режим асинхронной передачи (Asynchronous Transfer Mode, ATM). Международный стандарт ретрансляции ячеек, в котором множество типов данных (таких как голосовые, видео и другие) передаются в ячейках фиксированной длины (53 байта). Фиксированная длина ячеек позволяет выполнять их скоростную обработку на аппаратном уровне, уменьшая, таким образом, задержки передачи. ATM разрабатывался в расчете на использование преимуществ высокоскоростных передающих сред, таких как E3, SONET и T3.

Сегментация (segmentation). Процесс разделения коллизионного домена на два или более доменов с целью уменьшения конфликтов и перегрузки сети.

Сервер предприятия (enterprise server). Сервер, обслуживающий всех пользователей в сети, предоставляя им различные службы, такие как *электронная почта (e-mail)* или *служба доменных имен (DNS).*

Сервер рабочей группы (workgroup server). Сервер, обслуживающий определенную группу (или группы) пользователей, и предоставляющий им такие службы, как текстовый процессор или совместный доступ к файлам, то есть службы, который могут понадобиться только некоторым группам пользователей.

Сетевой адрес (network address). Адрес сетевого уровня, ссылающийся на логическое, а не физическое сетевое устройство. Также называется *протокольным адресом (protocol address).*

Таблица маршрутизации (routing table). Таблица, хранящаяся в маршрутизаторе или другом сетевом устройстве, которая содержит маршруты к определенным пунктам назначения в сети и, в некоторых случаях, метрики, связанные с этими маршрутами.

Топология типа "звезда", звездообразная топология (star topology). Топология локальных сетей, в которой оконечные точки соединены с общим центральным коммутатором посредством связей типа "точка-точка". *Кольцевая топология (ring topology),* организованная как "звезда", вместо связей "точка-точка" использует однонаправленный замкнутый шлейф.

Широковещательный домен (broadcast domain). Группа устройств, каждое из которых принимает широковещательные фреймы, отправленные с любого узла этой группы. Широковещательные домены обычно ограничиваются маршрутизаторами, поскольку маршрутизаторы не пересылают широковещательные фреймы.

Ключевые темы этот главы

- Описаны функции маршрутизации сетевого уровня и связь этих функций с определением пути в маршрутизаторе
- Описаны маршрутизируемые протоколы и протоколы маршрутизации
- Описаны внутренние и внешние протоколы
- Описаны характеристики и конфигурация протокола маршрутизации
- Описаны характеристики, работа и задачи конфигурирования для протокола JGRP

Глава 5

Протоколы маршрутизации IGRP

Введение

В главе 4, "Проектирование локальных сетей", были описаны цели и методология проектирования локальных сетей. Кроме того, был рассмотрен процесс проектирования сети на 1-м, 2-м и 3-м уровнях эталонной модели взаимодействия открытых систем (Open System Interconnection Reference Model, OSI). При построении сети необходимо также рассмотреть вопросы надежности, легкости в эксплуатации, модификации и реализации, а также вопросы установления соединении между устройствами системы

- Для обеспечения надежности сети необходимо, чтобы она имела средства обнаружения и исправления ошибок
- В сети должна быть обеспечена возможность включения в нее ряда устройств и программных продуктов таким образом, чтобы они могли работать совместно
- Для того, чтобы в сети было легко и удобно работать, необходимо, чтобы пользователю не требовалось знать структуру сети и способ ее реализации
- Для того, чтобы в сеть было легко вносить изменения, она должна быть спроектирована таким образом, чтобы в ней были предусмотрены возможности внесения изменений и расширения, а также применения новых технологий
- Для того, чтобы сеть было легко реализовать, она должна удовлетворять общим промышленным сетевым стандартам, а также допускать возможность установки различных конфигураций в соответствии с нуждами пользователя

В настоящей главе будет описано, как использование маршрутизаторов позволяет решать эти вопросы Кроме того, в этой главе будут обсуждены вопросы использования маршрутизаторов для соединения двух или более сетей и передачи пакетов данных между сетями на основе информации сетевого протокола Будет также описано, NTO поскольку маршрутизатор подсоединен к нескольким сетям, ему назначается несколько IP-адресов Как было описано в первом томе этой книги, одной из важных функций маршрутизатора является исследование поступающих пакетов данных и выбор оптимального пути их отправки на основе информации, содержащейся в таблице маршрутизации. В этой главе будет более подробно описана работа маршрутизатора и используемые им типы протоколов. В заключение описывается маршрутизация и IP-протоколы,

а также обсуждается реализация созданной корпорацией Cisco версии **протокола маршрутизации внутреннего шлюза (Interior Gateway Routing Protocol).**

Вашингтонский проект: протоколы маршрутизации и реализация протокола IGRP

Рассматриваемые в этой главе вопросы помогут понять работу протоколов маршрутизации, которые управляют маршрутизируемыми протоколами (такими, как IGRP) для организации передачи данных в сети. Настоящая глава поможет применить протокол IGRP для сетевого проекта, создаваемого для Вашингтонского учебного округа. Кроме того, будет описана установка протокола IGRP и соответствующих ему конфигураций, которые необходимы для реализации сетевого проекта.

Основные положения, относящиеся к работе сетевого уровня эталонной модели OSI

Как было описано ранее, сетевой уровень эталонной модели обеспечивает интерфейс с другими сетями и оптимальный вариант услуг по доставке пакетов своему пользователю - транспортному уровню. Он обеспечивает пересылку пакетов от сети-отправителя к се получателю. Для осуществления такой пересылки на сетевом уровне должен быть определен оптимальный путь. Эта функция обычно выполняется маршрутизатором.

Определение пути на сетевом уровне

Функция **определения пути (path determination)** позволяет маршрутизатору оценить возможные варианты пути к пункту назначения и выбрать наилучший способ отправки пакета. Термин **маршрутизация (routing)** относится к процессу выбора наилучшего пути для отправки пакета и способа прохождения многочисленных промежуточных физических сетей. Такова основа любого обмена информацией в Internet. Большинство протоколов маршрутизации выбирают кратчайший путь, используя для этого различные методы. В последующих разделах описаны несколько способов, используемых протоколами маршрутизации для нахождения кратчайшего или наилучшего пути.

Маршрутизацию пакетов можно сравнить с вождением автомобиля: водитель определяет наилучший путь, используя дорожные знаки, а маршрутизатор определяет наилучший путь, используя протокол маршрутизации и анализируя таблицы маршрутизации.

Таблицы маршрутизации

В IP-сетях маршрутизатор перенаправляет пакеты данных от сети-отправителя к сети-получателю, используя таблицы маршрутизации. После определения наилучшего пути он приступает к коммутации пакета: приняв пакет на одном интерфейсе, маршрутизатор пересылает его на другой интерфейс, который является следующим **переходом (hop)** на наилучшем пути к месту назначения пакета. Этим объясняется важность протокола маршрутизации — каждый маршрутизатор, который обрабатывает пакет, должен знать, что с ним *нужно сделать*.

Таблицы маршрутизации хранят информацию о возможных пунктах назначения и о способах их достижения. Для осуществления маршрутизации достаточно хранить в таблицах только сетевую часть IP-адреса. Это делает таблицы более компактными и эффективными.

Записи в таблицах маршрутизации содержат IP-адрес следующего перехода на пути к месту назначения. Каждая запись описывает только один переход и указывает на следующий непо-

средственно подсоединенный маршрутизатор, т.е. такой, которого можно достичь в рамках одной сети.

Протоколы маршрутизации заполняют таблицы разнообразной информацией. Например, при получении приходящего пакета маршрутизатор использует таблицу с адресами пунктов назначения и следующего перехода. После поиска адреса получателя делается попытка связать этот адрес со следующим переходом. Таблица маршрутизации с адресами пункта назначения и следующего перехода сообщает маршрутизатору, что достичь пункта назначения можно путем отправки пакета на указанный в таблице маршрутизатор, представляющий собой следующий переход на пути к конечному пункту.

Для построения таблицы путем использования протоколов маршрутизации и посредством передачи разнообразных сообщений маршрутизаторы должны иметь возможность обмениваться друг с другом служебной информацией. Одним из таких служебных сообщений является сообщение об изменении маршрутизации (routing update message). Такое сообщение представляет собой таблицу маршрутизации или ее часть. Анализируя сообщения об изменениях, маршрутизатор имеет возможность создать полную картину топологии сети. При наличии такой картины маршрутизатор может определить наилучший путь к месту назначения.

Различные метрики для представления расстояний в сети

Важно, чтобы информация в таблице маршрутизации постоянно обновлялась, поскольку ее основное назначение состоит в том, чтобы всегда содержать точную информацию для маршрутизатора. Каждый протокол маршрутизации интерпретирует понятие *наилучшего пути* по-своему. Для каждого пути по сети назначается число, называемое **метрикой (metric).** Обычно меньшему значению метрики соответствует лучший путь. Таблицы маршрутизации могут также содержать информацию о желательности данного пути. Для определения наилучшего пути метрики различных маршрутов сравниваются между собой. Виды метрик различаются в зависимости от типа используемого протокола. Далее в настоящей главе описан ряд типовых метрик.

Для определения наилучшего пути могут быть использованы различные метрики. Некоторые протоколы маршрутизации, например, протокол маршрутизирующей информации (Routing Information Protocol, RIP), используют только одну метрику, другие, например, IGRP, используют комбинацию нескольких метрик. Часто используемые метрики приведены в табл. 5.1.

Таблица 5.1. Часто используемое метрики

Тип метрики	Описание
Количество переходов	Количество маршрутизаторов которые необходимо пройти пакету, чтобы достичь пункта назначения Чем меньше количество переходов тем лучше путь. Длина пути показывает суммарное количество переходов до адресата
Полоса пропускания	Пропускная способность канала
Задержка	Промежуток времени, необходимый для перемещения пакета от источника к адресату.
Нагрузка	Уровень активности сетевого ресурса, такого как маршрутизатор или канал
Надежность	Вероятность ошибок сетевого канала
Такт задержки	Задержка в канале данных, измеряемая количеством импульсов системных часов компьютера IBM PC (период следования составляет примерно 55 миллисекунд)
Оценка	Произвольное значение, обычно основанное на ширине полосы пропускания, стоимости или другой мере которая назначается сетевым администратором

Коммуникационный путь сетевого уровня

После изучения адреса пункта назначения пакета маршрутизатор определяет, известно ли ему, как отправить пакет на следующий переход Если способ отправки неизвестен, то пакет обычно отбрасывается Если же маршрутизатору это известно, то он изменяет физический адрес пункта назначения на адрес следующего перехода и пересылает туда пакет

Следующий переход может быть или не быть конечным пунктом Если это не конечный пункт, то обычно это следующий маршрутизатор, который осуществляет такой же процесс коммутации, как и предыдущий маршрутизатор Этот процесс проиллюстрирован на рис 5 1

Адресация сети и хоста

Сетевой адрес состоит из двух частей — адреса сети и адреса хоста, используемых маршрутизатором для ориентации в сетевой среде Для того, чтобы выяснить, находится ли пункт назначения в этой же физической сети, сетевая часть IP-адреса пункта назначения извлекается и сравнивается с адресом сети отправителя

При прохождении пакета по сети IP-адреса отправителя и получателя не изменяются IP-адрес вычисляется программным обеспечением и протоколом маршрутизации IP и называется адресом следующего перехода (next-hop address)

Сетевая часть адреса используется для выбора пути Маршрутизатор отвечает за грохождение пакета по сети в соответствии с выбранным путем.

При выполнении коммутации маршрутизатор принимает пакет на одном интеррейсе и направляет его на другой Функция определения пути позволяет маршрутизатору выбрать наиболее подходящий интерфейс для отправки пакета

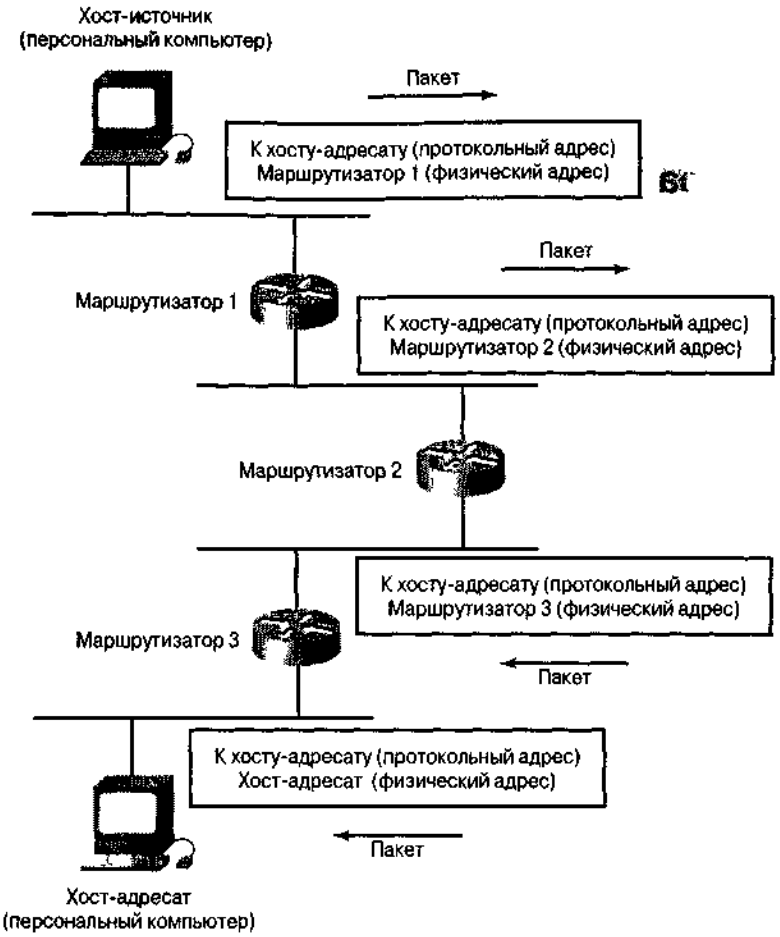


Рис 5 1 При движении пакета по сети его физический адрес меняется, но протокольный адрес остается неизменным

Маршрутизируемые протоколы и протоколы маршрутизации

Часто смешивают понятия *маршрутизируемого протокола (routed protocol)* и *протокола маршрутизации (routing protocol).* **Маршрутизируемыми (routed protocol)** являются протоколы, которые автоматически маршрутизируются в сети Примерами таких протоколов являются протокол управления передачей/Internet-протокол (Transmission Control Protocol/Internet protocol, TCP/IP) и протокол межсетевого обмена пакетами (Internetwork Packet Exchange, IPX) **Протоколы маршрутизации (routing protocol)** управляют работой маршрутизируемых протоколов Примерами протоколов маршрутизации являются IGRP, Enhanced IGRP, Open Shortest Path First (OSPF), Exterior Gateway Protocol (EGP), **Border Gateway Protocol (BGP),** OSI routing, Advanced Peer-to-Peer Networking (APPN), Intermediate System-to-Intermediate System и RIP. Кратко говоря, компьютеры (или *конечные системы, end systems)* используют маршрутизируемые протоколы, такие, как IP для "разговора друг *с* другом", в то время как маршрутизаторы (или *промежуточные системы, intermediate systems)* для "разговора о сетях и путях" используют протоколы маршрутизации.

Маршрутизация с использованием нескольких протоколов

Маршрутизаторы способны **работать с несколькими независимыми протоколами (multi-**

protocol routing), такими, например, как RIP и IGRP. Это позволяет маршрутизаторам передавать по одним и тем же каналам связи пакеты от нескольких маршрутизируемых протоколов, таких, например, как TCP/IP и IPX.

Вашингтонский проект: маршрутизация с использованием нескольких протоколов

В соответствии с пожеланиями пользователей сеть Вашингтонского учебного округа должна быть способна выполнять маршрутизацию с использованием нескольких протоколов. Округу желательно, чтобы в сети использовались два протокола маршрутизации — TCP/IP и IPX.

Протоколы IP-маршрутизации

Маршрутизация представляет собой процесс определения того, куда следует направить пакеты данных, направленные по адресам, лежащим вне данной локальной сети. Маршрутизаторы собирают и поддерживают информацию о маршрутах для того, чтобы обеспечить получение и отправку таких пакетов. Информация о маршрутах заносится в таблицу маршрутизации, каждой позиции которой соответствует один определенный маршрут. Протоколы маршрутизации позволяют маршрутизаторам создавать и поддерживать эти таблицы динамически и модифицировать их в соответствии с происходящими изменениями в сети.

Протоколы маршрутизации отличаются друг от друга следующими основными характеристиками.

- Во-первых, на работу протокола маршрутизации оказывают влияние конкретные цели его создателя.
- Во-вторых, существуют различные типы протоколов маршрутизации и каждый тип протокола оказывает свое специфическое влияние на ресурсы сети и маршрутизаторов.
- В-третьих, как говорилось выше, различные протоколы маршрутизации используют разные виды метрик для определения оптимального пути.

В целом протоколы маршрутизации можно разделить на два основных класса: внутренние и внешние. **Внутренние протоколы (interior protocols)** используются в сетях, находящихся под управлением одного администратора. До начала маршрутизации все внутренние IP-протоколы должны быть связаны со списком ассоциированных сетей. В процессе маршрутизации фиксируется информация об изменениях, поставляемая маршрутизаторами этих сетей, а собственная информация маршрутизации широковещательно передается в те же самые сети. Система поддержки внутренних протоколов корпорации Cisco включает в себя протоколы RIP и IGRP. **Внешние протоколы (exterior protocol)** используются для обмена информацией о маршрутизации между сетями, которые управляются разными администраторами. Примерами внешних протоколов могут служить EGP и BOP.

Перед началом работы внешним протоколам должна быть предоставлена следующая информация.

- Список соседних (также называемых, одноуровневыми, *peer)* маршрутизаторов, с которыми происходит обмен информацией о маршрутах.
- Список сетей, которые объявлены непосредственно достижимыми.

В следующих разделах характеристики протоколов маршрутизации обсуждаются более подробно.

Вашингтонский проект: реализация протокола IGRP

Далее в этой главе будут описаны понятия и техника конфигурирования в соответствии со следующими целями реализации протокола IGRP в сети Вашингтонского учебного округа.

- В сети должна обеспечиваться стабильная маршрутизация; при этом в маршрутах не должно быть петель.
- Сеть должна быстро реагировать на изменения в ее топологии.
- Сеть должна передавать по возможности меньшее количество служебной информации, а сам IGRP не должен использовать большей полосы пропускания, чем это действительно требуется для выполнения им своих функций.
- При проектировании сети должен учитываться уровень ошибок и уровень потоков данных по различным путям маршрутизации.

Оптимальный маршрут

Понятие *оптимального маршрута (optimal mute)* относится к способности протокола маршрутизации выбрать наилучший маршрут. Выбор наилучшего пути зависит от используемых метрик и их весов, используемых при вычислениях. Например, протокол маршрутизации может использовать метрику, включающую в себя количество переходов и время задержки, однако влияние времени задержки может быть преобладающим.

Простота и эффективность

При проектировании сетевых протоколов их стараются сделать максимально простыми и эффективными. Эффективность особенно важна, когда программное обеспечение, реализующее протокол, должно устанавливаться на компьютере с ограниченными вычислительными ресурсами.

Устойчивость

Протоколы маршрутизации должны быть устойчивыми. Иными словами, они должны правильно работать и в необычных или непредвиденных обстоятельствах, таких как аппаратные сбои, высокая нагрузка, а также в случае не совсем точной реализации. Поскольку маршрутизаторы устанавливаются в точках сопряжения сетей, при их сбоях возникают серьезные проблемы. Наилучшими протоколами маршрутизации часто являются те, которые прошли испытание временем и подтвердили свою стабильность в различных условиях.

Быстрая конвергенция

Протоколы маршрутизации должны обладать высокой степенью конвергенции. Под **конвер-**

генцией (convergence) понимается способность группы сетевых устройств, работающих с некоторым протоколом маршрутизации, учитывать изменения в сетевой топологии, а также скорость, с которой это происходит .

Когда в сети происходит какое-либо событие, например, выход из строя маршрутизатора или возобновление его работы, маршрутизаторы рассылают сообщения об изменениях в сети. Эти сообщения об изменениях направляются на другие сети, вызывая тем самым новое вычисление оптимальных маршрутов и переориентацию на них всех остальных маршрутизаторов Протоколы маршрутизации с низкой конвергенцией могут вызвать появление петель или простои сети.

На рис. 5.2 показан пример образования петли. В данном случае пакет поступает на 1-й маршрутизатор в момент времени Т1. В его таблицу маршрутизации уже внесены изменения, поэтому ему известен наилучший маршрут к пункту назначения, которым является следующий, 2-й маршрутизатор. Пакет направляется на этот 2-й маршрутизатор, который еще не обновил свою информацию о сети и поэтому полагает, что наилучшим следующим переходом будет 1-й маршрутизатор и, вследствие этого, вновь отправляет пакет на 1-й маршрутизатор. Эта передача пакета от одного маршрутизатора к другому будет продолжаться до тех пор, пока на 2-й маршрутизатор не поступят данные об изменениях в сети или пока не будет достигнуто максимально допустимое число коммутаций, задаваемое конфигурацией. Различные протоколы маршрутизации имеют разные допустимые максимумы числа коммутаций; обычно сетевой администратор может установить меньшее значение этого максимума. Например, протокол IGRP имеет максимум 255 коммутаций, по умолчанию устанавливается 100, а в реальных сетях этот максимум устанавливается на значение 50 или менее.

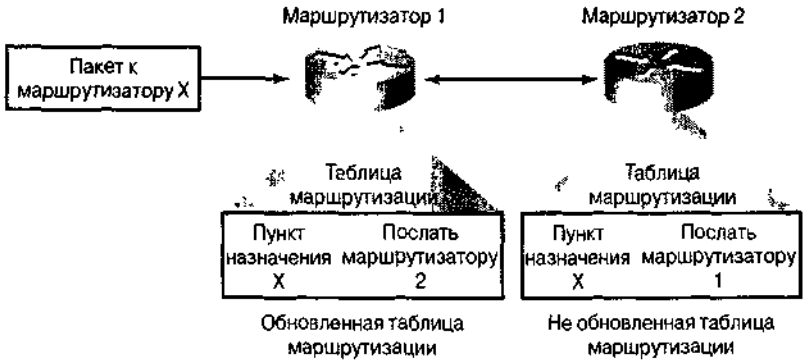


Рис 5 2 Петля в процессе маршрутизации существует до тех пор, пока не будет обновлена информация о сети или не будет достигнут допустимый максимум коммутаций

Гибкость

От протоколов маршрутизации требуется также достаточная гибкость Иными словами, они должны быстро и точно адаптироваться к различным ситуациям в сети. Например, предположим, что один из сегментов сети перестал функционировать. Многие протоколы маршрутизации быстро выбирают новый наилучший путь для всех маршрутов, которые в обычной ситуации использовали этот сегмент. Протоколы маршрутизации могут быть запрограммированы на адаптацию к изменениям ширины полосы пропускания, длины очереди, времени задержки и других переменных

Статическая маршрутизация

Протоколы **статической маршрутизации (static routing),** вообще говоря, не являются протоколами. Перед началом маршрутизации сетевой администратор самостоятельно заполняет

таблицы маршрутизации.

Эта таблица сохраняется до тех пор, пока сетевой администратор не изменит ее. Протоколы, использующие статические маршруты, просты в проектировании и хорошо работают в ситуациях, когда перемещение потоков данных в сети легко предсказуемо, а сама сеть имеет простую структуру.

Поскольку системы со статической маршрутизацией не могут реагировать на изменения в сетевой топологии, они обычно рассматриваются в качестве неприемлемых для современных обширных и постоянно меняющихся сетей. Такие сети требуют динамической маршрутизации.

Динамическая маршрутизация

Протоколы с **динамической маршрутизацией (dynamic routing)** обладают способностью адаптироваться к изменяющейся обстановке в сети Это делается на основе анализа поступающих от маршрутизаторов сообщений об изменениях в сети. Если в сообщении указывается на произошедшее в сети изменение, то программное обеспечение, осуществляющее маршрутизацию, заново вычисляет наилучшие маршруты и рассылает сообщения об изменениях на все маршрутизаторы сети. Эти сообщения распространяются по сети, побуждая маршрутизаторы заново пересчитать значения в таблице маршрутизации.

Там, где это целесообразно, динамические протоколы маршрутизации могут быть дополнены статическими. Например, может быть назначен **шлюз "последней надежды (gateway of last resort)** (т е. маршрутизатор, на которые пересылаются все пакеты, не поддающиеся маршрутизации). Этот маршрутизатор выступает в качестве основного места хранения для всех не поддающихся нормальной отправке пакетов, что позволяет обработать хотя бы каким-то образом все пакеты.

Различные подходы к маршрутизации

Как было описано ранее, большинство протоколов маршрутизации попадают в одну из следующих трех категорий.

- Дистанционно-векторные протоколы маршрутизации определяют направление (вектор) и расстояние для всех соединений в сети В качестве примеров дистанционно-векторных протоколов маршрутизации можно назвать IGRP и RIP
- Протоколы состояния канала связи (также называемые протоколами поиска первого кратчайшего пути) воссоздает точную топологию всей сети (или, по крайней, мере той ее части, в которой расположен маршрутизатор). Примерами протоколов состояния канала связи являются OSPF, IS-IS и протокол канальных служб корпорации NetWare (NetWare Link Services Protocol, NLSP).
- Протоколы гибридного типа соединяют в себе отдельные свойства дистанционно-векторных протоколов и протоколов состояния канала связи. Примером гибридного протокола является расширенный IGRP.

Конфигурирование IP-маршрутизации

Для каждого протокола маршрутизации должна быть установлена своя индивидуальная конфигурация. Этот процесс включает в себя два основных этапа.

1. Задание параметров процесса маршрутизации с использованием одной из команд маршрутизатора.
2. Конфигурирование конкретного протокола.

Как было описано ранее, перед началом работы внутренние протоколы, такие как IGRP и RIP, должны иметь список указанных сетей до начала маршрутизации. Кроме того, было сказано, что в процессе маршрутизации анализируются сообщения маршрутизаторов об изменениях в их сетях и этим же маршрутизаторам рассылаются широковещательные сообщения об изменениях. Протоколу IGRP также дополнительно требуется номер *автономной системы (autonomous system, AS).*

Вашингтонский проект: назначение номеров автономным системам

В процессе проектирования сети необходимо следить за согласованностью номеров автономных систем, которые должны быть едиными в пределах сети округа. Эти 16-битовые номера присваиваются Департаментом назначения номеров сети Internet.

При разработке любого протокола IP-маршрутизации необходимо задать параметры процесса маршрутизации, связать сети с этим процессом и приспособить протокол маршрутизации к конкретной сети. Выбор оптимального протокола маршрутизации представляет собой сложную задачу. При выборе этого протокола необходимо принять во внимание следующие факторы.

- Размер и сложность сети.
- Уровни потоков данных.
- Требования к защите информации.
- Требования надежности.
- Величина времени задержки для данной сети.
- Организационные вопросы.
- Допустимость изменений.

Описание работы протокола IGRP

Протокол IGRP является собственной разработкой компании Cisco и был создан для замены протокола RIP. IGRP представляет собой дистанционно-векторный протокол маршрутизации. Дистанционно-векторные протоколы маршрутизации требуют, чтобы каждый маршрутизатор через регулярные интервалы времени посылал полностью или часть своей таблицы маршрутизации своим соседям — маршрутизаторам. По мере того как информация о маршрутах распространяется по сети, маршрутизаторы рассчитывают расстояния до всех ее узлов.

Протокол IGRP использует комбинацию метрик. При принятии решения о маршруте используются с разными весами следующие величины: время ожидания, ширина полосы пропускания, надежность и нагрузка. Сетевой администратор может задать значения каждой из этих метрик. Для автоматического вычисления наилучшего пути протокол IGRP использует либо значения, установленные администратором, либо значения по умолчанию.

Протокол IGRP обеспечивает широкий диапазон изменения метрик. Например, надежность и нагрузка могут принимать любое значение в диапазоне 1—255, ширина полосы пропускания может иметь значения, соответствующие скоростям от 1200 бит/с до 10 Гбит/с, а время ожидания может принимать любое значение от 1 до 2^{24} секунд. Широкие диапазоны изменения метрик позволяют устанавливать в различных сетях адекватные значения метрик со значительно изменяющимися рабочими характеристиками. Вследствие этого сетевые администраторы могут

повлиять на выбор маршрута на основе интуитивных решений. Это делается путем приписывания различным метрикам индивидуальных весов, т.е. задавая маршрутизатору степень их влияния. В значениях, принимаемых по умолчанию, наибольший вес приписывается ширине полосы пропускания, благодаря чему IGRP превосходит RIP. Протокол RIP не приписывает метрикам весов, поскольку он использует лишь одну метрику.

Внутренние, системные и внешние маршруты протокола IGRP

Основной целью при создании корпорацией Cisco протокола IGRP было получение устойчивого протокола для маршрутизации в автономных системах. Автономная система представляет собой набор сетей, находящихся под общим административным управлением и вместе использующих одну и ту же стратегию маршрутизации (рис. 5.3).

Протокол IGRP использует комбинацию конфигурируемых пользователем метрик, которые включают в себя время ожидания, ширину полосы пропускания, надежность и нагрузку. В протоколе IGRP определены три типа маршрутов: внутренние, системные и внешние (см. рис. 5.3). Внутренними (interior) называются маршруты между подсетями сети, подключенной к одному интерфейсу маршрутизатора. Если сеть, подсоединенная к маршрутизатору, не разделена на подсети, то внутренние маршруты не объявляются. Кроме того, информация о подсетях не включается в изменения, фиксируемые протоколом, что представляет собой серьезную проблему для IP-подсетей, не являющихся непрерывными.

Системными (system route) называются маршруты к сетям внутри автономной системы. Маршрутизатор вырабатывает системные маршруты на основе анализа непосредственно подсоединенных сетевых интерфейсов и системной маршрутной информации, предоставляемой другими маршрутизаторами, использующими протокол IGRP. Системные маршруты не содержат информации о подсетях.

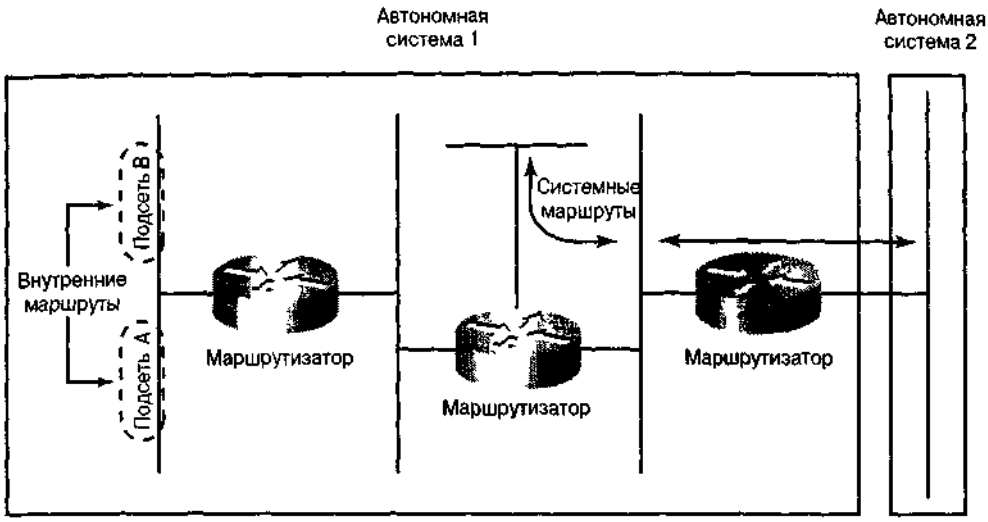


Рис. 5.3. Автономные системы разделены границами областей

Внешними (external) называются маршруты к сетям, лежащим вне автономной системы, которые рассматриваются при нахождении "шлюза последней надежды". Маршрутизатор выбирает направление к этому шлюзу из списка внешних маршрутов, предоставляемого протоколом IGRP. Шлюз последней надежды выбирается в тех случаях, когда не имеется лучшего пути для пакета, а пункт назначения не является подсоединенной сетью. Если автономная система имеет более чем одно соединение с внешней сетью, то различные маршрутизаторы могут выбрать разные внешние маршрутизаторы в качестве шлюза последней надежды.

Конфигурирование процесса IGRP-маршрутизации

Для установки конфигурации протокола IGRP необходимо задать характеристики его процесса маршрутизации. В настоящем разделе рассматриваются команды, необходимые для реализации протокола IGRP на маршрутизаторе. В нем также описаны действия выполняемые маршрутизатором для того, чтобы все соседние маршрутизаторы были оповещены о статусе всех сетей автономной системы, включая частоту, с которой рассылаются сообщения об изменениях в сети и информацию о том, каково влияние этих изменений на использование полосы пропускания.

Инженерный журнал: конфигурирование протокола IGRP

Для задания характеристик процесса маршрутизации в протоколе IGRP необходимо выполнить описанные ниже действия, начав работу в режиме установки глобальной конфигурации.

Процесс маршрутизации начинается с помощью команды **router igrp:**

router igrp *автономная-система*

Аргумент *автономная-система* указывает маршруты к другим маршрутизаторам протокола IGRP и используется для создания тега прошедшей информации о маршрутизации. Для прекращения процесса маршрутизации в автономной системе, указанной в качестве аргумента *автономная-система,* используется команда по **router igrp:**

no router igrp *автономная-система*

Связывание сети с процессом маршрутизации производится путем выполнения команды **network**:

network номер-сети

Аргумент *номер-сети* представляет собой номер сети, записанный в точечном десятичном формате. Отметим, что этот номер не должен содержать информации о подсетях. Могут быть выполнены несколько команд **network**.

При установке конфигурации процесса маршрутизации необходимо указать номер автономной системы. Этот номер может быть указан заранее или не указан. Номер автономной системы используется для создания тега изменений в сети, связанных с процессами маршрутизации, количество которых в протоколе IGRP может изменяться от одного до четырех. Команда no **network** с номером сети может быть использована для удаления сети из списка:

no network номер-сети

В приведенном ниже примере маршрутизатор конфигурируется для протокола IGRP и включается в автономную систему 109. В последних двух строках две команды **network** включают две сети в список сетей, получающих изменения в IGRP.

```
Router(config)# router igrp 109
network 131.108.0.0.
network 192.31.7.0
```

Протокол IGRP посылает сообщения об изменениях на интерфейсы указанных сетей. Если интерфейс сети не указан, то он не объявляется ни в каких сообщениях об изменениях протокола IGRP.

Повышение устойчивости протокола IGRP

Протокол IGRP обладает рядом средств, предназначенных для повышения его устойчивости, включая следующие:

- удержание (holddown);
- расщепление горизонта (split horizon);
- обратное исправление (poison reverse update).

Эти средства описаны в последующих пунктах.

Удержание

Когда маршрутизатор узнает, что сеть находится дальше, чем это было предварительно известно, или узнает, что сеть прекратила функционировать, то маршрут к этой сети переводится в состояние удержания (holddown). Во время этого удержания маршрут объявляется, однако все поступающие объявления об изменениях в этой сети со всех маршрутизаторов, кроме того, который первоначально объявил новую метрику сети, игнорируются. Этот механизм часто используется для предотвращения образования в сети петель, однако он увеличивает время конвергенции сети.

Удержания используются для того, чтобы предотвратить рассылку регулярных сообщений об изменениях маршрута, который, возможно, стал недействительным. Когда маршрутизатор выходит из строя, соседние маршрутизаторы узнают об этом по отсутствию запланированных регулярных сообщений об изменениях. В этом случае они вычисляют новые маршруты и рассылают сообщения об изменениях для того, чтобы проинформировать своих соседей об изменении маршрута. Такая деятельность вызывает появление волны изменений, которые фильтруются, проходя по сети. Сообщения об изменениях приходят на сетевые устройства не мгновенно, поэтому становится возможной такая ситуация, когда устройство А, которое еще не было проинформировано о сбое в сети, рассылает регулярные сообщения об изменениях (указывающие, что маршрут, который перестал существовать, по-прежнему находится в рабочем состоянии) устройству В, которое только что было проинформировано о сбое в сети. В этом случае устройство. В будет содержать (и потенциально объявлять другим) неверную информацию о маршрутизации.

Механизм удержания заставляет маршрутизаторы задерживать на некоторое время всю информацию об изменениях в сети, которая могла бы повлиять на действия маршрутизаторов. Время удержания обычно выбирается несколько большим того, которое необходимо для внесения в сеть изменений. Это позволяет предотвратить образование петель маршрутизации, вызванное медленной конвергенцией.

Расщепление горизонта

Расщепление горизонта (split horizon) возникает в том случае, когда маршрутизатор пытается послать информацию о маршруте в том же направлении, в котором он ее получил. В качестве примера рассмотрим ситуацию, изображенную на рис. 5.4. Первоначально маршрутизатор 1 объявляет, что он имеет маршрут к сети А. В результате у маршрутизатора В отсутствуют причины для повторного включения этого маршрута в информацию о маршрутизаторе А, поскольку последний ближе к сети А. Правила расщепления горизонта требуют, чтобы маршрутизатор 2 исключил этот маршрут из всех сообщений об изменениях, которые он посылает маршрутизатору 1.

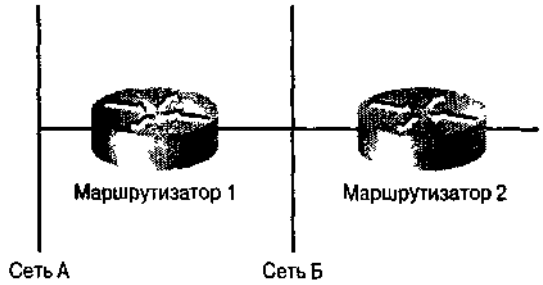


Рис. 54 Поскольку маршрутизатор 1 находится ближе к сети А, маршрутизатор 2 должен исключить сообщения об изменениях, направляемые маршрутизатору 1, которые касаются его маршрута к сети 2

Правила расщепления горизонта помогают избежать появления петель маршрутизации. Например, рассмотрим случай, когда интерфейс маршрутизатора 1, подключенный к сети А, выходит из строя. Если бы не было расщепления горизонта, то маршрутизатор 2 продолжал бы информировать маршрутизатор 1 о том, что у него есть доступ к сети А (через маршрутизатор 1). Если маршрутизатор 1 не обладает способностью обрабатывать такую ситуацию, то он, возможно, действительно выберет маршрут через маршрутизатор 2 в качестве альтернативы своему вышедшему из строя соединению, создав таким образом петлю. Хотя удержания должны предотвратить это, в IGRP также используется и разделение пространства, поскольку оно обеспечивает дополнительную стабильность протокола.

Обратное исправление

В то время как расщепление горизонта должно предотвращать возникновение петель между соседними маршрутизаторами, метод обратного исправления (poison reverse update) предназначен для ликвидации петель в более обширных группах. Значительное увеличение значений метрик маршрутизации обычно свидетельствует о возникновении петель. Как только обрывается связь с некоторой сетью, анонсирующий ее маршрутизатор сохраняет в своей таблице данные об этой сети на время посылки нескольких периодических сообщений об обновлении. При этом в широковещательных сообщениях указывается бесконечная стоимость маршрута к сети, с которой отсутствует связь.

Инженерный журнал: команды timers **basic и** holddown

Приведенное ниже описание **команд timers basic и holddown** позволяет управлять изменениями в маршрутизации.

- **Команда timers basic. Команда timers basic** позволяет контролировать частоту, с которой протокол IGRP рассылает сообщения об изменениях. По умолчанию это происходит каждые 90 секунд. В случае потери пакетов протоколу IGRP может потребоваться несколько минут для того, чтобы исключить ставшие неработоспособными маршруты. При удалении маршрута и принятии нового протоколу IGRP из-за удержания могут вновь потребоваться несколько минут.

  Первое, что следует сделать для уменьшения этой задержки — уменьшить временные константы. Для основной временной константы рекомендуется значение 15 вместо 90 В этом случае маршруты будут исключаться после истечения 45 секунд. Другие значения будут уменьшать это время пропорционально.

В действительности значение времени удаления маршрута не столь важно, как можно было бы предположить. Как правило, маршруты вообще не исчезают. Их уничтожают по причине отсутствия активной связи с каким-либо интерфейсом. Сообщения об активности обычно поступают каждые 10 секунд, соответственно, для обнаружения интерфейса таким способом требуется 30 секунд Следует устанавливать время сообщений об активности на линиях T1 равным 4. Это позволяет обнаружить сбой в течение 12 секунд.

- **Команда no metric holddown**. Другим важный параметр, используемый для принятия нового маршрута, устанавливается командой `no metric holddown`. Эта команда отключает механизм удержаний, в том смысле, что после удаления маршрута новый принимается немедленно. Однако для использования удержаний имеются серьезные теоретические причины. Например, возможны случаи, когда при отсутствии удержаний старый маршрут вообще не сможет покинуть систему.

Информация о метриках протокола IGRP

Протокол IGRP использует несколько типов метрик. Для каждого пути в автономной системе он регистрирует сегмент с наименьшей полосой пропускания, накопившуюся задержку, наименьший размер **максимальной единицы передачи данных maximum transmission unit, MTU),** надежность и уровень нагрузки.

Для задания относительных весов каждой метрики используются специальные переменные. По умолчанию при вычислении наилучшего пути наибольший вес придается ширине пропускания. Для сети, использующей только одну метрику (например, в сетях Ethernet), эта метрика сводится к количеству переходов. Для сетей, использующих комбинированную метрику (например, Ethernet вместе с последовательными пиниями, имеющими скорости от 9600 бод до скоростей уровня T1), маршрут с минимальной метрикой отражает наиболее предпочтительный путь к месту назначения с учетом всех описанных выше факторов.

Сообщения об изменениях протокола IGRP

Маршрутизаторы, использующие протокол IGRP, рассылают широковещательные сообщения об изменениях каждые 90 секунд. Маршрут объявляется недостижимым, если по нему в течение трех циклов, т.е. в течение 270 секунд, не проходит сообщение об изменении в сети, посланное первым маршрутизатором. После пяти циклов (450 секунд) маршрутизатор удаляет этот маршрут из своей таблицы. Для ускорения конвергенции протокол маршрутизации IGRP использует мгновенные сообщения и отключение сообщений.

Мгновенное изменение (triggered update) представляет собой рассылку сообщения об изменении в сети до истечения стандартного интервала уведомления других маршрутизаторов об изменениях метрики. Обратное исправление (poison reverse update) предназначено для предотвращения появления больших петель в маршрутах, чем это вызвано увеличением метрики маршрутизации. При этом рассылаются сообщения для удаления маршрута из таблиц маршрутизации и перевода его в состояние удержания, благодаря чему в течение некоторого периода времени исключается использование новой информации о маршрутизации

Подсчет максимального количества переходов

Максимальное количество переходов в протоколе IGRP равно 255. Однако обычно оно устанавливается меньшим, чем принимаемые по умолчанию 100 переходов. Поскольку в IGRP ис-

пользуется метод мгновенных изменений (triggered updates), подсчет до 100 не отнимает слишком много времени. Рекомендуется использовать меньшее значение этого параметра, кроме случаев очень большой сети. Однако оно не должно быть меньшим, чем общее количество маршрутизаторов, через которые может пройти маршрут. Если происходит обмен данными о маршрутизации с другой сетью, го при выборе максимального количества переходов необходим учет маршрутизаторов в обеих сетях. При подсчете числа переходов необходимо также учитывать, как будет выглядеть конфигурация в случае, если несколько линий связи по какой-либо причине перестанут функционировать.

Ниже приведен пример задания конфигурации маршрутизатора, в котором использованы все описанные в настоящем разделе механизмы (в конкретных случаях вместо сети 128.6.0.0 следует подставить номер используемой сети).

```
Router(config)# router igrp 46
timers basic 15 45 0 60
network 128.6.0.0
no metric holddown
metric maximum-hop 50
```

После задания такой конфигурации изменения в *маршрутизацию* обычно вносятся в течение 30 секунд, при условии, что значение **интервала рассылки сообщений об активности (keepalive interval),** представляющего собой промежуток времени между рассылкой сообщений, было установлено равным 4.

Резюме

- Функции маршрутизации сетевого уровня включают в себя адресацию и выбор наилучшего пути для потока данных.
- В таблицах маршрутизации хранится информация о возможных пунктах назначения и способах их достижения.
- Маршрутизируемые протоколы представляют собой протоколы определяемые в сети, а протоколы маршрутизации реализуют маршрутизируемые протоколы.
- Протоколы маршрутизации могут быть статическими или динамическими.
- Внутренние протоколы используются для осуществления маршрутизации в сетях, управляемых одним администратором. Внешние протоколы применяются для обмена информацией о маршрутизации в сетях, у которых нет общего администратора.
- Протокол IGRP представляет собой внутренний дистанционно-векторный шлюзовой протокол, использующий комбинацию различных метрик: время задержки, ширину полосы, надежность и уровень загрузки. Веса, определяющие относительное влияние этих метрик задаются пользователем.
- Стабильность работы протокола IGRP может быть повышена за счет использования удержаний, расщепления горизонта и обратного исправления.
- При конфигурировании протокола IGRP обязательным является только задание характеристик процесса маршрутизации; остальные установки не являются обязательными.

Задачи проекта Вашингтонского учебного округа: протоколы маршрутизации и конфигурирование IGRP

В настоящей главе были описаны концепции и процессы маршрутизации, которые помогают

реализовать протокол IGRP в качестве протокола маршрутизации в сети Вашингтонского учебного округа. Частью конфигурирования протокола IGRP и его реализации является решение следующих задач. Идентификация и сбор всей информации, необходимой для реализации протокола IGRP в отдельных школьных сетях и во всей сети округа. Эту информацию следует присоединить к той, которая отражает существующие требования и описывает проектирование локальной сети (рекомендуется ознакомиться с техническими требованиями Вашингтонского учебного проекта).

1. Определение сетей, которые будут объявляться маршрутизатором в учебном округе, и занесение информации о них в соответствующие документы. Эту информацию следует присоединить к той, которая отражает существующие требования и описывает проектирование локальной сети (рекомендуется ознакомиться с техническими требованиями Вашингтонского учебного проекта).
2. Определение IGRP-номера автономной системы учебного округа и занесение его в соответствующие документы.
3. Запись последовательности команд маршрутизатора, необходимых для реализации протокола IGRP на маршрутизаторах конкретных школ.
4. Описание процесса, посредством которого все маршрутизаторы будут оповещены о статусе всех сетей автономной системы.
5. Определение оптимальных установок для максимально допустимого числа переходов, для таймера удержания, таймера оповещения об изменениях и т.д. Следует также занести в документы значения ширины полосы пропускания для последовательных интерфейсов.

Контрольные вопросы

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

1. На каком уровне эталонной модели OSI происходит определение пути и какова функция этого уровня?
2. Как маршрутизатор определяет, на какой интерфейс следует направить пакет данных?
3. Что означает термин *мультипротокольная маршрутизация (multiprotocol routing)?*
4. От каких двух основных параметров маршрутизатора зависит работа протокола динамической маршрутизации?
5. Что означает термин *конвергенция (convergence) ?*
6. После определения пути, по которому следует направить пакет, какое следующее действие может выполнить маршрутизатор?
   A. Широковещание.
   B. Хранение пакета в таблице маршрутизации.
   C. Выбор протокола маршрутизации.
   D. Коммутация пакета.
7. От какого из приведенных ниже действий зависит успех динамической маршрутизации?
   A. Ручной ввод маршрутов.
   B. Поддержание таблицы маршрутизации.
   C. Периодическое внесение изменений в таблицу маршрутизации.
   D. B. и C.
8. _____ _____протоколы маршрутизации определяют направление и расстояние до любого канала сети совместного использования; _____ протоколы маршрутизации также называются протоколами выбора первого кратчайшего пути.
   A. Дистанционно-векторные; канального уровня.
   B. Дистанционно-векторные; гибридные.
   C. Канального уровня; дистанционно-векторные.
   D. Динамические; статические.

9. Что из перечисленного ниже *не* является переменной, используемой протоколом IGRP для определения значения комбинированной метрики?
   A. Ширина полосы пропускания.
   B. Задержка.
   C. Нагрузка.
   D. Протокол IGRP использует все эти величины.
10. Какую из приведенных ниже команд следует использовать для выбора IGRP в качестве протокола маршрутизации?

```
A. show igrp
B. router network grip
C. enable igrp
D. router igrp
```

Основные термины

Автономная система (autonomous system, AS). Набор сетей, работающих под одним административным управлением и использующих общую стратегию маршрутизации. Также называется *доменом маршрутизации.* Департамент назначения номеров Internet (Internet Assigned Numbers Authority) присваивает автономным системам 16-битовый номер.

Адрес следующего перехода (next-hop address). IP-адрес, вычисляемый протоколом маршрутизации IP и программным обеспечением.

Внешний протокол (exterior protocol). Протокол, используемый для обмена информацией о маршрутизации между сетями, находящимся под различным административным управлением.

Внутренний протокол (interior protocol). Протокол, используемый в сетях, находящихся под единым административным управлением.

Динамическая маршрутизация (dynamic routing). Маршрутизация, автоматически учитывающая изменения в сетевой топологии.

Задержка (delay). Промежуток времени между началом передачи пакета данных от отправителя к адресату и началом получения ответа отправителем. Также время, которое требуется пакету для того, чтобы дойти от отправителя к получателю по заданному пути.

Количество переходов (hop count). Метрика маршрутизации, используемая для измерения расстояния между отправителем и получателем. Для протокола RIP это единственная используемая метрика.

Конвергенция (convergence). Способность или скорость группы устройств, использующих один протокол и совместно работающих в сети, согласовать топологию после того, как в ней произошли изменения.

Максимальная единица передачи данных (maximum transmission unit, MTU). Максимальный размер пакета, измеряемый в байтах, который может обрабатываться конкретным интерфейсом.

Маршрутизируемый протокол (routed protocol). Протокол, который может управляться маршрутизатором.

Мгновенное изменение (triggered update). Отправка сообщения об изменении до истечения стандартного промежутка времени для отправки таких сообщений. Используется для уведомления других маршрутизаторов о смене метрики.

Метрика (metric). Стандартизованная числовая характеристика (например, длина пути), используемая протоколами маршрутизации для нахождения оптимального пути к пункту назначения.

Мультипротокольная маршрутизация (multiprotocol routing). Или маршрутизация, использующая несколько протоколов. Тип маршрутизации, при котором пакеты от различных маршрутизирующих протоколов, таких как TCP/IP или IPX передаются по одним и тем же каналам данных.

Нагрузка (load). Величина, отражающая сетевую активность некоторого ресурса, | такого, например, как маршрутизатор или канал.

Надежность (reliability). Измеряется коэффициентом ожидаемых от канала сообщений об

активности. Если этот коэффициент велик, то канал считается надежным. Используется в качестве одной из метрик маршрутизации.

Обратное исправление (poison reverse update). Свойство протокола IGRP, имеющее целью избежать возникновения маршрутных петель. Как только обрывается связь с некоторой сетью, анонсирующий ее маршрутизатор сохраняет в своей таблице данные об этой сети на время посылки нескольких периодических сообщений об обновлении. При этом в широковещательных сообщениях указывается бесконечная стоимость маршрута к сети, с которой отсутствует связь.

Определение пути (path determination). Принятие решения о том, по какому пути следует направить поток данных в сетевом пространстве. Определение пути происходит на сетевом уровне эталонной модели OSI.

Оценка (cost). Величина любого типа, вычисляемая на основе количества переходов, ширины полосы пропускания передающей среды и других параметров, задаваемая сетевым администратором и используемая для сравнения различных путей в сетевом пространстве.

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

Протокол маршрутизации (routing protocol). Протокол, осуществляющий маршрутизацию при реализации конкретного протокола. Примерами протоколов маршрутизации могут служить IGRP, OSPF и RIP.

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

Протокол пограничного шлюза (Border Gateway Protocol, BGP). Протокол маршрутизации для обмена информацией между доменами. В настоящее время постепенно заменяет протокол маршрутизации внешнего шлюза (Exterior Gateway Protocol). Протокол BGP обменивается информацией о достижимости пунктов назначения с другими системами BGP и определяется стандартом RFC 1163.

Расщепление горизонта (split horizon). Свойство протокола IGRP, имеющее целью не допустить выбора маршрутизаторами ошибочных путей. Расщепление горизонта предотвращает образование петель между соседними маршрутизаторами и уменьшает количество сообщений об изменениях.

Сообщение об активности (keepalive). Сообщение, посылаемое одним сетевым устройством другому устройству о том, что виртуальная сеть между ними остается активной.

Статическая маршрутизация (static routing). Тип маршрутизации, при котором данные маршрутов явно указываются администратором и заносятся в таблицу маршрутизации. При динамической маршрутизации статические маршруты имеют приоритет перед всеми другими.

Такт задержки (tick). Задержка в канале данных, осуществляемая с использованием периода срабатывания таймера (встроенного в персональные компьютеры). Равна примерно 55 миллисекундам. Точное значение 1/18 секунды.

Удержание (holddown). Свойство протокола IGRP отвергать все маршруты с одним и тем же пунктом назначения в течение некоторого периода времени.

Ширина полосы пропускания (bandwidth). Разность между наибольшей и наименьшей возможными частотами, допустимыми для сигнала в сети. Этот термин также используется для оценки пропускной способности сети или протокола.

Шлюз "последней надежды" или **маршрутизатор-склад (gateway of last resort).** Маршрутизатор, на который направляются все пакеты, не прошедшие маршрутизацию.

Ключевые темы этой главы

- Дано определение списка управления доступом, описаны цели использования таких списков и их работа в сети
- Описаны процессы, происходящие при тестировании пакетов с помощью списков управления доступом
- Описаны команды установки' 'конфигурации ACL, глоба́льные директивы и команды интерфейсов
- Дано определение шаблона маски, описаны ее функции и использование отдельных битов, а также шаблоны **any** и **host**
- Описаны стандартные списки управления доступом
- Описаны расширенные списки управления доступом
- Описаны именованные списки управления доступом
- Описано, как можно отображать и тестировать отдельные операции; использующие списки управления доступом

Глава 6

Списки управления доступом (ACL)

Введение

В своей работе сетевые администраторы постоянно сталкиваются с двумя взаимосвязанными проблемами с одной стороны, необходимо обеспечить доступ к сети санкционированных пользователей, с другой — ограничить доступ нежелательных. Хотя такие средства как пароли, аппаратура отзыва и физические устройства безопасности полезны, однако им часто не хватает гибкости при фильтрации потока данных, желательны также специальные управляющие средства, которые предпочитают большинство администраторов Например, бывают ситуации, когда сетевой администратор готов предоставить пользователям локальной сети выход в Internet, но при этом не хочет разрешать пользователям Internet, находящимся вне этой локальной сети, входить в эту сеть средствами протокола Telnet

Основные возможности фильтрации, такие как блокирование потока данных из Internet, предоставляют маршрутизаторы, используя для этого списки управления доступом (access control list, ACL). В настоящей главе будет описано использование стандартных и расширенных списков управления доступом в качестве средства контроля потока данных и одной из мер по обеспечению безопасности Список управления доступом представляет собой последовательность директив разрешения или запрещения доступа, которые применяются к адресам или протоколам верхнего уровня В настоящей главе основное внимание уделено стандартным, расширенным и именованным спискам

Кроме того, в главе приведены советы и основные принципы использования списков управления доступом, а также команды и типы конфигураций, необходимые для их создания В заключение приведены примеры стандартных и расширенных списков и описано их использование на интерфейсах маршрутизаторов.

Вашингтонский проект: списки управления доступом

В настоящей главе приведены основные понятия и команды файла конфигурации, которые будут полезны при использовании списков управления доступом в Вашингтонском проекте. Кроме того, по мере введения понятий и команд, связанных с использованием списков управления доступом, станет возможным их применение при проектировании и реализации этой сети.

Обзор списков управления доступом

Списки управления доступом представляют собой набор инструкций, применяемых к интерфейсу маршрутизатора. Они указывают маршрутизатору, какие пакеты следует принять, а какие отвергнуть. Решение об этом может основываться на определенных критериях, таких как адрес источника, адрес получателя или номер порта.

Списки управления доступом позволяют управлять потоком данных и обрабатывать конкретные пакеты путем группировки интерфейсов пунктов назначения в списке доступа. При такой группировке на интерфейсе устанавливается соответствующая конфигурация, после чего все проходящие через него данные тестируются и проверяйся на соответствие условиям, содержащимся в списке.

Списки управления доступом могут быть созданы для всех маршрутизируемых сетевых протоколов, таких, например, как Internet Protocol (IP) или Internetwork Packet exchange (IPX) с целью фильтрации пакетов по мере их поступления на маршрутизатор. Для списков управления может быть установлена конфигурация, позволяющая управлять доступом в сеть или подсеть. Например, в Вашингтонском учебном округе списки могут быть использованы для отделения потоков данных студентов от информации, распространяемой в административной сети.

Списки управления доступом фильтруют поток данных посредством решения вопроса о том, направить ли пакет далее или заблокировать его на интерфейсе. Каждый пакет исследуется на его соответствие условиям, имеющимся в списке. В качестве условий могут выступать адрес источника, адрес получателя, протокол более высокого ровня или другая информация.

Список управления доступом должен составляться для каждого отдельного протокола. Иными словами, для каждого протокола, используемого на интерфейсе маршрутизатора, должен быть составлен список, который будет регулировать прохождение потока данных для этого протокола. Отметим, что в некоторых протоколах списки управления доступом называются **фильтрами**. Например, если интерфейс маршрутизатора сконфигурирован для IP, AppleTalk и IPX, то необходимо будет определить, по меньшей мере, три списка управления доступом. Как показано на рис. 6.1, списки могут быть использованы в качестве гибкого средства фильтрации пакетов, посту-1ающих на интерфейс маршрутизатора или отправляемых с него.

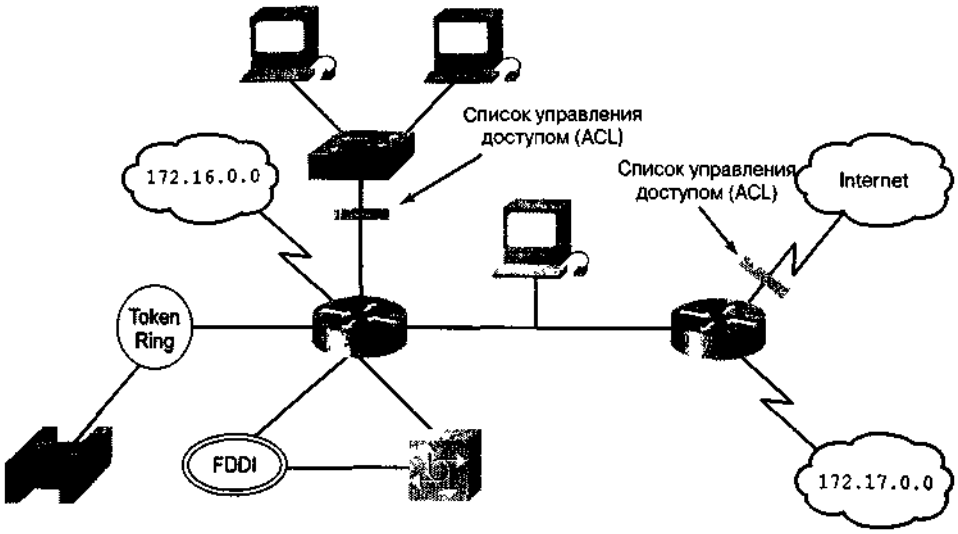


Рис. 6.1. Использование списков управления доступом позволяет выполнить тестирование пакетов на основе адресации или типа потока данных и на этой основе разрешить или запретить доступ потока данных на маршрутизатор или выход с него

Вашингтонский проект: рекомендации по обеспечению безопасности

Проектирование локальной сети для Вашингтонского учебного округа требует, чтобы каждая школа имела две сети — одну для студентов, а другую для администрации. Каждый конкретный сегмент должен быть подсоединен к отдельному Ethernet-порту маршрутизатора и обслуживаться им. Соображения безопасности требуют создать списки управления доступом, которые бы препятствовали доступу студентов к административному сегменту сети, оставляя вместе с тем возможность доступа административного персонала к студенческому сегменту.
Единственным исключением из этого правила является то, что маршрутизатор должен предоставлять всем пользователям доступ к серверу системы доменных имен (Domain Name System, DNS) и к сообщениям электронной почты на сервере DNS/email, расположенном в административном сегменте. Этот поток данных начинается в локальной сети, к которому имеют доступ студенты. Следовательно, если студент работает в Web и ему требуется, чтобы DNS-сервер преобразовал имена хостов, то список управления доступом должен разрешить ему это. Кроме того, этот список позволяет студентам получать и отправлять электронную почту.

Причины создания списков управления доступом

Для создания списков управления доступом имеется много причин, некоторые из них перечислены ниже.

- Для ограничения потока данных в сети и повышения ее эффективности. В частности, списки могут быть использованы для того, чтобы некоторые пакеты какого-либо протокола обрабатывались маршрутизатором ранее других. Такое явление называется **очередностью (queuing)** и используется для того, чтобы маршрутизатор не обрабатывал пакеты, которые в данный момент не являются необходимыми. Установка очередности ограничивает поток данных в сети и уменьшает вероятность перегрузки.
- Для управления потоком данных. Например, с помошью списков можно ограничить или

уменьшить количество сообщений об изменениях в сети. Эти ограничения используются для предотвращения распространения информации об отдельных сетях на всю сеть.

- Для обеспечения базового уровня защиты от несанкционированного доступа. Например, списки позволяют разрешить одному хосту доступ к некоторому сегменту сети, а другому закрыть доступ к этой же области. На рис. 6.2 показано, что хосту А разрешен доступ к сети пользователей, а хосту В такой доступзапрещен. Если на маршрутизаторе не установлен список управления доступом, то все пакеты, проходящие через маршрутизатор, поступают во все части сети.
- Для определения типа данных, которые будут направляться далее или блокироваться на интерфейсе маршрутизатора. Например, можно разрешить маршрутизацию электронной почты и в то же время заблокировать весь поток данныхпротокола Telnet.

Вашингтонский проект: использование списков управления доступом

При использовании списков управления доступом на маршрутизаторах Вашингтонского учебного округа весь поток данных со студенческого сегмента должен быть отделен от административной локальной сети. Из этого можно сделать исключения, например, разрешить свободное использование электронной почты и службы каталогов, поскольку они представляют минимальный риск.
Электронная почта и DNS должны быть доступны во всем округе, вместе с тем эти виды услуг не должны давать несанкционированного доступа к административной сети. Все списки управления доступом должны контролироваться из окружного офиса, а исключения в списках должны рассматриваться перед реализацией сети.

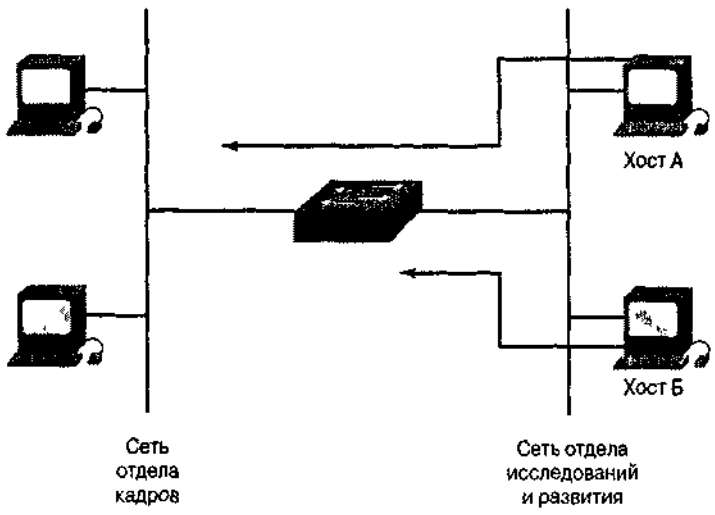


Рис. 6 2 Использование списков управления доступом позволяет предотвратить направление потока данных в какую-либо сеть

Важность порядка директив при создании списков управления доступом

При создании списков управления доступом важен порядок, в котором располагаются соответствующие директивы. Принимая решение о дальнейшей отправке пакета или его блокировке, операционная система Cisco Internetwork (Cisco Internetwork Operational System, IOS) проверяет его соответствие всем директивам в том порядке, в каком они записывались. Если такое соответствие обнаружено, то остальные директивы не рассматриваются.

Если была записана директива, разрешающая передачу всех данных, то все последующие директивы не проверяются. Если требуется внести дополнительные директивы, то нужно удалить весь список и заново создать его с новыми директивами. Поэтому целесообразно отредактировать конфигурацию маршрутизатора, используя текстовый редактор, а затем установить протокол простой передачи файлов (Trivial File Transfer Protocol, TFTP).

Примечание

Каждая дополнительная директива добавляется в конец списка. Таким образом, невозможно удалить в нумерованном списке отдельные директивы после того, как они были созданы, а можно удалить только весь список полностью.

Использование списков управления доступом

Список управления доступом может быть создан для каждого протокола, для которого должны фильтроваться данные, и для каждого интерфейса. В некоторых протоколах создается один список для фильтрации входных данных и другой для выходных данных Могут быть созданы два основных типа списков — стандартный и расширенный. Они будут описаны ниже в настоящей главе.

После того, как директива списка проверит пакет на соответствие заданному условию, ему может быть разрешено или запрещено использование интерфейса в группе доступа.

Списки управления доступом операционной системы Cisco проверяют пакет и заголовки верхних уровней, как показано на рис. 6.3. Например, можно использовать стандартный список для фильтрации пакетов только по адресу источника.

Как работают списки управления доступом

Список управления доступом представляет собой набор директив, которые определяют:

- как организован вход на интерфейсы;
- как происходит передача информации через маршрутизатор;
- как организованы выходные интерфейсы маршрутизатора.

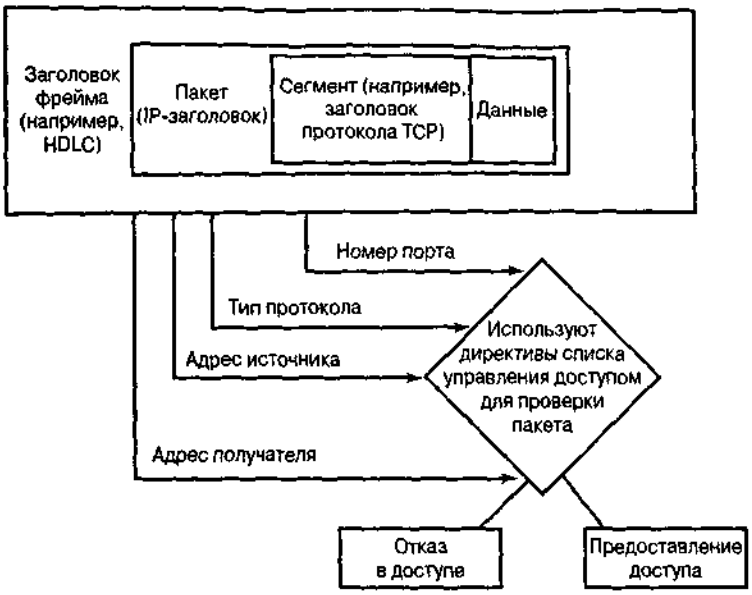


Рис. 6.3. Списки управления доступом проверяют заголовки пакета и заголовки более высоких уровней

Как показано на рис. 6.4, начальные операции по установке связи остаются одними и теми же, независимо от того, используются списки управления доступом или нет. Когда пакет поступает на интерфейс, маршрутизатор определяет, куда его направить — на маршрутизатор или на мост. Если пакет не может быть обработан маршрутизатором или мостом, то он отбрасывается. Если пакет поддается маршрутизации, то таблица маршрутизации указывает сеть-получатель, метрику или состояние маршрутизации и интерфейс, с которого следует отправить пакет.

Далее маршрутизатор проверяет, находится ли интерфейс получателя в группе списка управления доступом. Если его там нет, то пакет может быть направлен на интерфейс получателя непосредственно; например, при использовании интерфейса Too, который не использует списки управления доступом, пакет отправляется непосредственно с ToO.

Директивы списка исполняются последовательно. Если заголовок пакета соответствует директиве списка, то остальные директивы пропускаются. Если условие директивы выполнено, то пакету разрешается или отказывается в доступе.

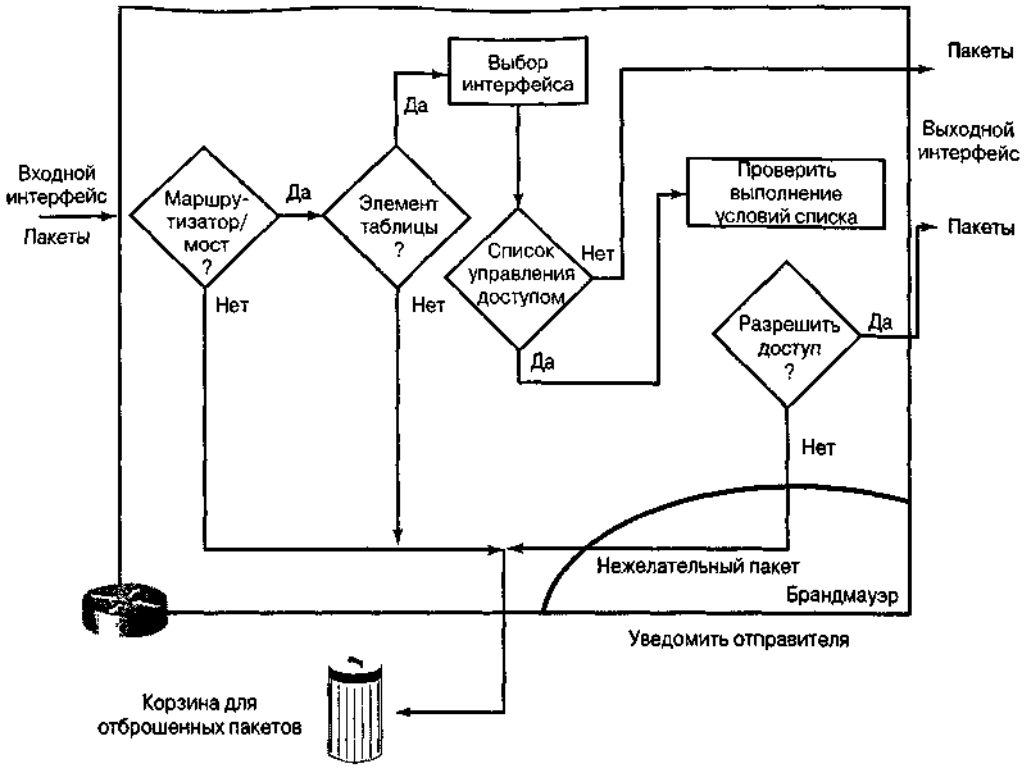


Рис. 6.4. Списки управления доступом фильтруют пакеты от внешних источников, но не фильтруют пакеты, которые поступают из самого маршрутизатора

Например, на рис. 6.5 пакет соответствует условию первой директивы и ему отказано в доступе. Он отбрасывается и помещается **в битовую корзину (bit bucket).** Его соответствие последующим условиям не проверяется.

Если пакет не соответствует условию первой директивы, то он проверяется на соответствие второй директиве из списка управления доступом. Если параметры пакета соответствуют следующему условию, которое представляет собой директиву разрешения доступа, то ему разрешается отправка на интерфейс получателя. Второй пакет не соответствует условиям первой директивы, но удовлетворяет условиям следующего и ему также дается разрешение на отправку.

Списки управления доступом позволяют установить, каким пользователям разрешен доступ к конкретной сети. Условия в файле списка позволяют:

- просмотреть определенные хосты для того, чтобы разрешить или заблокировать им доступ к некоторой части сети;
- установить пароль, что позволит получать доступ к сети только тем пользователям, которые ввели при подключении правильный пароль;
- предоставить доступ к сети пользователям, которым требуется воспользоваться собственными файлами или каталогами.

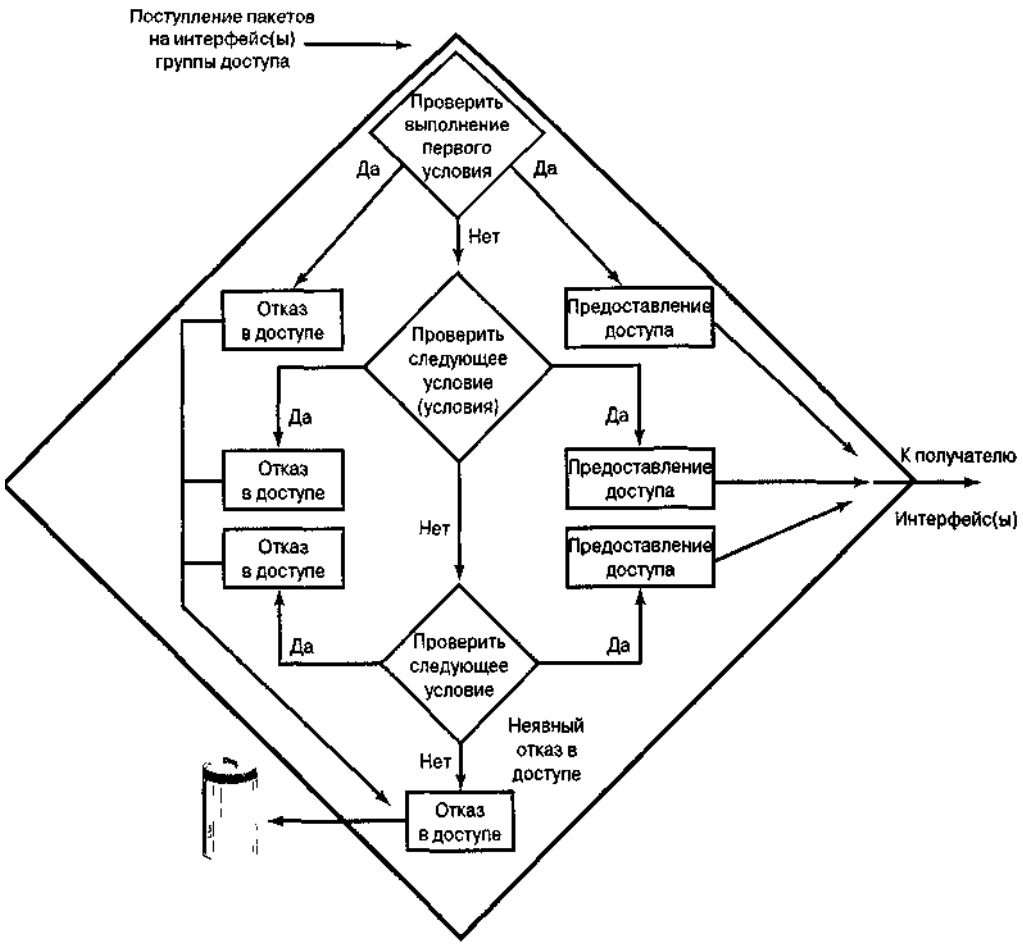


Рис. 6.5. Списки управления доступом исследуют поступающие пакеты и информируют отправителя в том случае, если какой-либо пакет является нежелательным

Вашингтонский проект: разрешение на доступ

Для всех компьютеров, включенных в административную сеть учебного округа необходимо разработать систему идентификационных номеров и паролей. Эта система должна быть доведена до сведения всех пользователей и строго соблюдаться. Необходимо также обеспечить всем компьютерам окружной сети доступ к Internet.

Примечание

Для логической завершенности список управления доступом должен содержать условия, которые выполняются для всех пакетов, использующих этот список. Последняя директива в списке относится ко всем пакетам, которые не удовлетворяют предыдущим условиям. Ее условия должны приводить к отказу в доступе. Вместо обработки этих приходящих или отправляемых пакетов они должны быть отброшены. Если такое условие нежелательно, то последней директивой в списке должна быть команда **`permit any`**. Отметим, что неявный отказ в доступе не отображен в файле конфигурации и поэтому некоторые сетевые администраторы предпочитают ввести эту команду явным образом. При этом она появляется при просмотре файла конфигурации, что облегчает задачи контроля за работой сети.

Конфигурирование списков управления доступом

На практике команды списков управления доступом представляют собой длинные символьные строки. Основными задачами, решение которых описано в этом разделе, являются следующие.

- Создание ACL в обычном процессе установки глобальной конфигурации маршрутизатора.
- Задание номера ACL от 1 до 99 указывает маршрутизатору на создание стандартного списка. При указании номера от 100 до 199 создается расширенный ACL.
- При создании ACL необходимо тщательно отбирать необходимые директивы и соблюдать их логическую последовательность. Должны быть указаны допустимые IP протоколы; всем данным других протоколов должно быть отказано в допуске.
- Необходимо выбрать проверяемые IP-протоколы; все остальные протоколы проверяться не будут. В дальнейшем для большей точности можно будет также указать порт получателя.
- Фильтрация с использованием IP-адреса осуществляется с помощью маски адреса, которая задает способ проверки соответствующих битов адреса.

Для лучшего понимания основных команд конфигурирования списков управления доступом целесообразно объединить эти команды группы, соответствующие двум этапам.

Этап 1. Определить список, используя команду

```
Router(config)# access-list номер-списка {permit | deny}
{условия отбора}
```

Глобальная директива **access-list** определяет список управления доступом. В частности, диапазон номеров от 1 до 99 зарезервирован для стандартного IP-протокола. Этот номер определяет тип списка. В версии 11.2 операционной системы Cisco или в более поздних для названия списка вместо номера можно также использовать имя, например, `education_group`. Команда **permit** или **deny** в директиве указывает, каким способом операционная система Cisco обрабатывает пакеты, которые удовлетворяют заданному условию. Команда **permit** обычно разрешает использовать один или более интерфейсов, которые будут указаны позднее. Заключительная часть команды указывает условия проверки, которую выполняет эта директива.

Этап 2. Для применения списка к одному из интерфейсов используется команда **access-group**, подобно тому как это сделано в следующем примере:

```
Router (config-if)# {протокол} access-group список
```

Все директивы, указанные в параметре *список*, связаны с одним или несколькими интерфейсами маршрутизатора. Всем пакетам, удовлетворяющим условиям списка, может быть предоставлен доступ к любому интерфейсу, входящему в группу доступа.

Группировка списков по интерфейсам

Хотя каждый протокол обладает своими специфическими требованиями и правилами, выполнение которых необходимо для фильтрации потока данных, в целом создание списков управления доступом требует выполнения двух основных действий, писанных в этом разделе. Первое действие состоит в создании списка, а второе — в применении списка к конкретному интерфейсу.

Списки управления доступом применяются к одному или нескольким интерфейсам и выполняют фильтрацию входных или выходных данных, в зависимости от установленной конфигурации. Списки для выходных данных обычно более эффективны и поэтому их использование предпочтительнее. Маршрутизатор со списком для входных данных должен проверять каждый пакет на его соответствие условиям списка перед отправкой его на выходной интерфейс.

Назначение номера каждому списку управления {доступом

При установке конфигурации на маршрутизаторе каждому списку управления доступом необходимо присвоить его индивидуальный номер.

При назначении номера необходимо принимать во внимание диапазон номеров, возможных для данного протокола.

Номера, допустимые для различных протоколов, приведены в табл. 6.1.

Таблица 6.1. Протоколы, в которых списки управления доступом указываются номерами

Протокол	**Диапазон изменения номеров списков-управления доступом**
IP	1-99
Extended IP	100-199
AppleTalk	600-699
IPX	800-899
Extended IPX	900-999
IPX Service Advertising Protocol	1000-1099

После создания нумерованных списков их требуется назначить конкретным интерфейсам. Если требуется изменить список, содержащий пронумерованные директивы, то для этого придется удалить все директивы списка командой

no access-list *номер-списка*

Инженерный журнал: пример установки конфигурации для нумерованного списка управления доступом

В приведенном ниже примере определяются списки 1 и 2.

```
  interface  ethernet   0
  ip  address   1.1.1.1   255.0.0.0
  ip access-group 1 in
  ip access-group 2 out
   !
 access-list 1 permit 5.6.0.0 0.0.255.255
 access-list 1 deny 7.9.0.0 0.0.255.255
 !
   access-list 2 permit 1.2.3.4
   access-list 2 deny   1.2.0.0 0.0.255.255
```

Предположим, что интерфейс получает 10 пакетов от IP-адреса 5.6.7.7 и 14 пакетов от IP-адреса 1.2.23.21. Тогда первые команды будут выглядеть следующим образом:

```
   list I permit 5.6.7.7   1 packet

   list 2 deny  1.2.23.21 1 packet
```

Использование битов шаблона маски

Шаблон маски представляет собой 32-битовую величину, которая разделена на четыре октета, каждый из которых состоит из 8 бит. Бит 0 маски означает, что этот бит должен проверяться, а бит равный 1 означает, что условие для него проверяться не будет (рис. 6.6).

Рис. 6 6. Тщательный подбор шаблона маски позволяет выбрать один или несколько IP-адресов для выполнения тестов на разрешение доступа или отказ в доступе

Примечание

Маскирование списков управления доступом с помощью шаблона отличается от маскирования, используемого для IP-подсетей. Нулевой бит в маске списка указывает, что соответствующий бит в адресе будет проверяться, а единица означает, что значение бита не будет приниматься во внимание. Таким образом, битовый шаблон маски списка управления доступом часто выглядит как инвертированная маска подсети (например, шаблон маски списка выглядит как `0.0.255.255`, а маска подсети — `255.255.0.0`).

Шаблон маски применяется к IP-адресам; значения битов шаблона указывают на способ обработки соответствующих битов IP-адреса.

Шаблон маски используется для указания одного или нескольких адресов, которые проверяются на соответствие условиям разрешения или блокирования доступа. Термин *маскирование по шаблону (wildcard masking)* применяется для обозначения процесса побитового сравнения и используется по аналогии с карточной игрой "покер", в которой джокер заменяет любую карту.

Хотя шаблон маски списков управления доступом и маска подсети представляют собой 32-битовую величину, выполняемые ими функции значительно различаются. Нули и единицы в маске подсети определяют сеть, подсеть и номер хоста. Биты шаблона маски в IP-адресе определяют, будет ли проверяться соответствующий бит.

Как было сказано ранее, нули и единицы в шаблоне маски указывают списку управления доступом на необходимость проверять или не проверять соответствующие биты в IP-адресе. На рис. 6.7 изображен процесс применения шаблона маски.

Предположим, что необходимо проверить IP-адрес для подсети, которому может быть разрешен или блокирован доступ. Предположим, далее, что этот адрес относится к классу B (т.е. первые два октета представляют собой номер сети), а следующие 8 битов обозначают номер подсети (третий октет предназначен для номера подсети). Если требуется разрешить доступ всем пакетам с номерами подсети от `172.30.16.0` до `172.30.31`. О, то следует использо-

вать шаблон маски, которая показана на рис. 6.7.

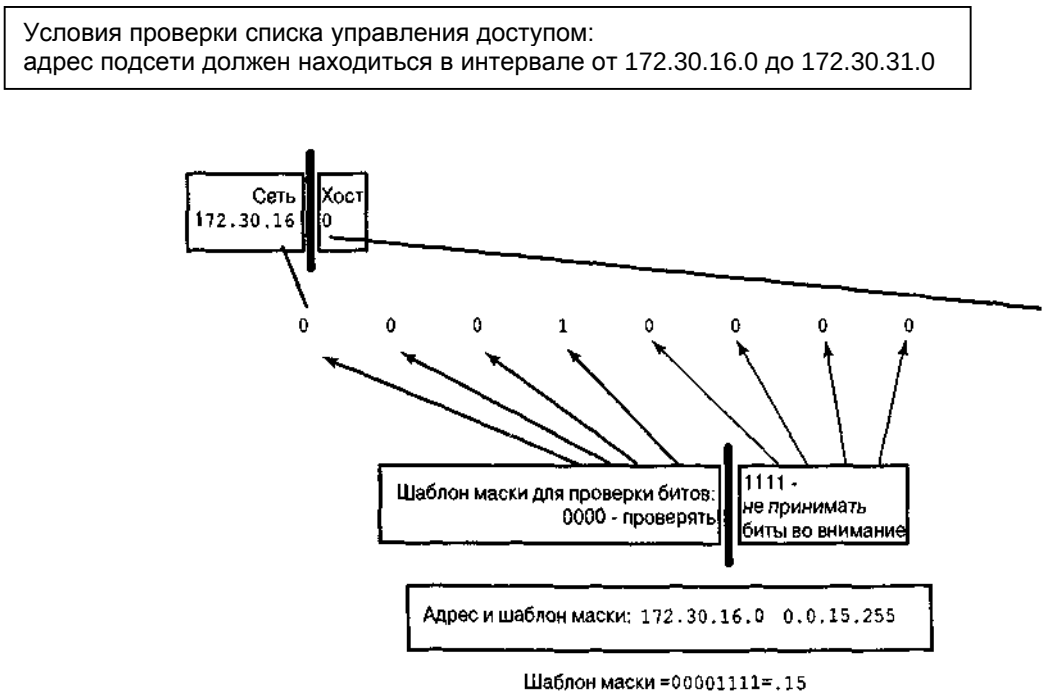


Рис. 6.7. Адрес 172.30.16.0 с шаблоном маски 0.0.15.255 соответствует сетям с номерами от 172.30.16.0 до 172.30.31.0

Сначала с использованием нулевых битов шаблона маски проверяются первые два октета (172.30).

Поскольку индивидуальные адреса хостов не представляют интереса (идентификационный номер хоста не содержит в конце адреса 0.0), шаблон маски не учитывает последний октет, а использует единичные биты в шаблоне маски.

В третьем октете шаблон маски равен 15 (00001111), а IP-адрес равен 16 (00001000). Первые четыре нуля шаблона маски указывают маршрутизатору на необходимость проверки первых четырех битов IP-адреса (0001). Так как последние четыре бита не принимаются во внимание, все числа в интервале от 16 (00010000) до 31 (00011111) будут удовлетворять условию проверки, поскольку все они начинаются с 0001.

Последние (наименее важные) четыре бита в этом октете шаблона маски во внимание не принимаются — здесь могут находиться как нули, так и единицы, а соответствующие биты маски равны единице.

В приведенном примере адрес 172.30.16.0 с маской 0.0.15.255 соответствует подсетям с номерами от 172.30.16.0 до 172.30.31.0. Другие подсети не удовлетворяют условиям маски.

Использование шаблона any

Работа с десятичным представлением битов шаблона может показаться утомительной. В большинстве случаев применения маскирования можно использовать ключевые слова или маски. Они уменьшают количество символов, которое приходится набирать на клавиатуре при записи условий для конкретных адресов. Например, если требуется разрешить доступ для всех номеров получателей, можно указать маску 0.0.0.0, как показано на рис. 6.8. Для указания на то, что список управления доступом не должен принимать во внимание никакие значения адреса (т.е. пропускать их без проверки), все биты маски адреса должны быть равны единице (т.е. 255.255.255.255). Для задания операционной системе Cisco этого условия можно также использовать ключевое слово any. Вместо набора на клавиатуре 0.0.0.0 255.255.255.255 также можно использовать в качестве ключевого слова any.

Например, вместо использования строки

```
Router(config)#  access-list   1  permit  0.0.0.0  255.255.255.255
```
можно набрать
```
Router(config)#  access-list   1  permit  any
```

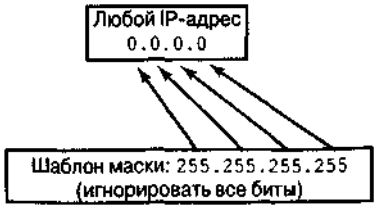


Рис. 6.8. При необходимости задания маски, соответствующей произвольному адресу, вместо длинной строки шаблона маски можно использовать шаблон `any`

Использование шаблона host

Вторым случаем, когда можно использовать ключевое слово, является ситуация, когда необходимо соответствие всех битов адреса хоста шаблону. Например, предположим, что надо заблокировать доступ конкретному хосту. Для указания адреса его надо полностью ввести (например, 172.30.16.29, как показано на рис. 6.9), а затем указать, что список должен проверить все биты адреса, т.е. шаблон маски должна состоять только из нулей (0.0.0.0). Это же условие можно записать с использованием ключевого слова **host**. В приведенном ниже примере вместо набора 172.30.16.29). О. О. О перед адресом можно записать ключевое слово host.

Например, вместо набора строки

```
Router(config)#  access-list   1  permit  172.30.16.29   0.0.0.0
```

можно записать

```
Router(config)#  access-list  1  permit  host   172.30.16.29
```

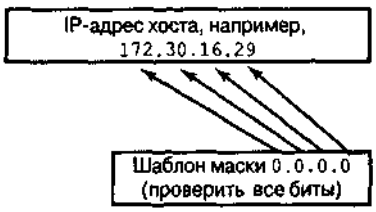


Рис. 6.9. Примером использования ключевого слова host *в условии списка управления доступом может служить строка* host 172.30.16.29

Стандартные списки управления доступом

Стандартные списки управления доступом используются при необходимости заблокировать или, наоборот, разрешить весь поток данных от какой-либо сети или хоста, а также отказать в доступе набору протоколов. Стандартные списки управления доступом проверяют адреса источников для пакетов, которые могут быть обработаны маршрутизатором. В результате предоставляется доступ или отказывается в нем всему протоколу. Это решение принимается на основе анализа адресов сети, подсети и хоста. Например, изображенные на рис. 6.10 пакеты, по-

ступающие на интерфейс E0, проверяются по адресу источника и по протоколу. Если им предоставляется доступ, то они направляются через интерфейс SO, который логически связан со списком управления доступом. Если им отказывается в доступе, то они отбрасываются.

Примеры стандартных списков управления доступом

Как было описано ранее, для определения списка с номером используется стандартная команда установки конфигурации access-list. Она используется в командном режиме задания глобальной конфигурации.

Рис. 6.10. Пакеты, поступающие с интерфейса E0, проверяются на соответствие адресу источника и протоколу

Полная форма команды имеет вид:

Router(config)# **access-list** *номер-списка* **{permit | deny} source**

[шаблон-источника] [log]

Для удаления стандартного списка управления доступом используется форма этой команды с ключевым словом no:

```
Router(config)# no access-list номер-списка
```

Ниже приводится описание параметров, используемых в команде.

Параметр	Описание
номер - списка	Номер списка управления доступом. Представляет собой десятичное целое число от 1 до 99 (для стандартных IP-списков)
deny	Отказ в доступе, если условие выполнено
permit	Разрешение доступа, если условие выполнено
source	Номер сети или хоста, с которого посылается пакет. Источник можно указать двумя способами Использовать 32-битовую величину в точечно-десятичном формате, состоящем из четырех частей Использовать ключевое слово any в качестве аббревиатуры для источника и шаблона источника с адресами в диапазоне от О.О.О.ОД0255.255.255.255
шаблон-*источника*	(Необязательный) Биты шаблона, применяемые к источнику Существует два способа указать шаблон источника. Использовать 32-битную величину в точечно-десятичном формате, состоящем из четырех частей. Если какие-либо биты нужно игнорировать, то в них следует записать единицы. Использовать ключевое слово any в качестве аббревиатуры для ис-

	точника и шаблона источника с адресами в диапазоне от 0.0.0.0 до 255.255.255.255
log	(Необязательный) Вызывает появление информационного сообщения о регистрации в системном журнале (logging message) пакета, который удовлетворяет ссылке, которая будет послана на консоль (Уровень сообщений записываемых на консоль, задается командой logging console) Это сообщение включает в себя номер списка управления доступом, указывает, было ли дано пакету разрешение на доступ, адрес источника и количество пакетов Данное сообщение генерируется для первого пакета, удовлетворяющего условию, а затем генерируется с пятиминутным интервалом, при этом также сообщается количество пакетов, которым было разрешено или отказано в доступе за предыдущий пятиминутный интервал

Для отображения на экране содержания всех списков используется команда **show access-lists**. Она может использоваться и для отображения одного списка.

В приведенном ниже примере стандартный список разрешает доступ хостам трех указанных сетей:

```
access-list I permit 192.5.34.0 0.0.0.255
access-list 1 permit 128.88.0.0 0.0.255.255
access-list 1 permit 36.0.0.0 0.255.255.255
! (Примечание: доступ от остальных сетей неявно заблокирован)
```

В этом примере биты шаблона применяются только к части сетевого адреса, относящейся к хосту. Любому другому хосту с адресом источника, не соответствующим этим директивам, будет отказано в доступе.

При необходимости указать большое число индивидуальных адресов шаблон можно опустить, если все его биты равны нулю. Приведенные ниже две команды установки конфигурации эквивалентны:

```
access-list 2 permit 36.48.0.3
access-list 2 permit 36.48.0.3 0.0.0.0
```

Команда **ip access-group** применяет уже существующий список управления доступом к интерфейсу. Отметим, что для каждого порта, протокола и направления допускается только один список. Команда имеет следующий формат.

Router (config) # **ip access-group** номер-списка {**in** | **out**}

Параметры команды имеют следующее значение.

Параметр	Описание
номер-списка	Указывает номер списка управления доступом, который будет логически связан с данным интерфейсом
in | out	Показывает, к какому из интерфейсов будет применяться список управления доступом — к входному или выходному Если ни одно из значений in, out не указано, то по умолчанию принимается out

Примечание

Для удаления списка необходимо сначала ввести команду no ip access-group с номером списка для каждого интерфейса, на котором он использовался, а затем команду no access-list(с номером списка)

Примеры стандартных конфигураций списков управления доступом, приведенные в последующих разделах, относятся к сети, показанной на рис. 6 11. В первом примере разрешается передача от сети-источника 172.16.0.0. Во втором примере отказано в передаче хосту с сетевым адресом 172.16.4.13 и разрешена передача данных всех остальных хостов. В третьем примере отказано в передаче подсети с сетевым адресом 172.16.4.0 и разрешена передача всех остальных данных.

Пример 1 стандартного списка управления доступом: разрешение передачи данных из сети-источника

В листинге 6.1 список управления доступом разрешает передачу данных только от сети-источника с номером 172.16.0.0. Передача всех остальных данных заблокирована. На рис. 6.11 показано, как список управления доступом разрешает передачу только от сети-источника 172.16-О.Ои блокирует передачу от всех остальных источников

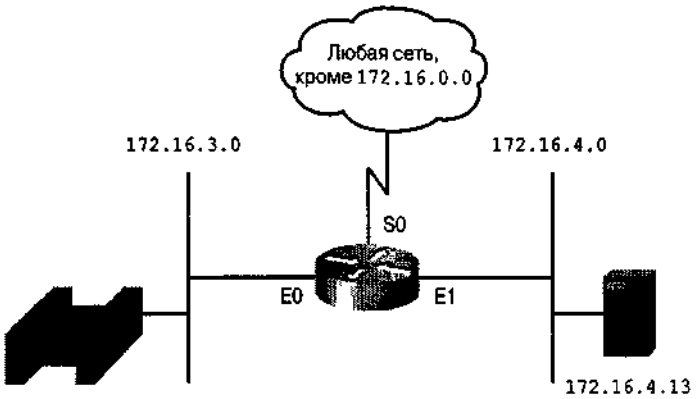


Рис. 6 11. Эта сеть представляет собой пример соединения двух подсетей маршрутизатором

Листинг 6.1. Разрешение передачи от сети-источника 172.16.0.0

```
access-list I permit 172.16.0.0   0.0.255.255
(неявно отказывается в доступе всем остальным;
в тексте это не отображается)
(access-list I deny 0.0.0.0  255.255.255.255)

interface ethernet 0
ip access-group 1 out
interface ethernet 1
ip access-group 1 out
```

Ниже описаны отдельные поля листинга 6.1

Поле	Описание
1	Номер списка управления доступом, в данном случае указывается, что это

	обычный список
permit	Поток данных, удовлетворяющий выбранным параметрам, будет направлен дальше
172.16.0.0	IP-адрес, который будет использован вместе с шаблоном маски для определения сети-источника
0.0.255.255	Шаблон маски, нули указывают позиции, которые должны соответствовать условиям, в то время как единицы указывают позиции, значение которых не влияет на предоставление доступа

Команда **`ip access-group`** в листинге 6.1 создает группу списка на выходном интерфейсе.

Пример 2 стандартного списка управления доступом: отказ в доступе конкретному хосту

В листинге 6 2 показано, как создать список, блокирующий передачу с адреса 172.16.4.13, а весь остальной поток направить на интерфейс Ethernet 0. Первая команда access-list отказывает в передаче указанному хосту, используя параметр deny. Маска адреса 0.0.0.0 в этой строке указывает на необходимость проверки всех битов.

Листинг 6.2. Отказ в доступе конкретному хосту

```
access-list I deny   172.16.4.13   0.0.0.0
access-list 1 permit 0.0.0.0      255.255.255.255
(неявно отказывается в доступе всем остальным; в тексте это не отображается) (ac-
cess-list I deny O.O.O.O 255.255.255.255)

 interface ethernet 0
 ip access-group 1
```

Ниже описаны поля листинга 6 2

Поле	Описание
1	Номер списка управления доступом, в данном случае указывается, то это обычный список
deny	Поток данных, удовлетворяющий выбранным параметрам, не будет аправлен дальше
host	Сокращение для шаблона маски 0.0.0.0
permit	Поток данных, удовлетворяющий выбранным параметрам, будет направлен дальше
0.0.0.0	IP-адрес хоста-источника, нули используются для указания знакоместа (placeholder)
255,255.255.255	Шаблон маски, нули указывают позиции, которые должны соответствовать условиям, в то время как единицы указывают позиции, значение которых не влияет на доступ Если все позиции заполнены единицами, то это означает, что все 32 бита в адресе источника не будут проверяться

Во второй команде access-list комбинация 0.0.0.0 255.255.255.255 задает шаблон маски, кото-

рая пропускает пакеты от любого источника. Она также может быть записана с использованием ключевого слова any Все нули в адресе указывают на необходимость подстановки на это место адреса и его проверки, а все единицы в шаблоне маски указывают, что все 32 бита в адресе источника не будут проверяться.

Любой пакет, не отвечающий условиям первой строки списка, будет удовлетворять условиям второй строки и направлен далее.

Пример 3 стандартного списка управления доступом: отказ в доступе конкретной подсети

В листинге 6.3 показана установка конфигурации списка управления доступом, которая блокирует передачу данных из подсети 172.16.4.0, а все остальные потоки данных направляет дальше. Следует обратить внимание на шаблон маски, записанный в виде: 0.0.0.255. Нули в первых трех октетах указывают на то, что эти биты не принимаются во внимание. Отметим также, что для IP-адреса источника использовано ключевое слово any.

Листинг 6,3. Блокировка данных с конкретной подсети

```
access-list 1 deny 172.16.4.0 0.0.0.255
access-list 1 permit any
(неявный отказ в доступе всем остальным)
(access-list I deny any)

interface ethernet 0 ip access-group 1
```

Ниже описаны поля листинга 6 3

Поле	Описание
1	Этот список управления доступом предназначен для блокирования информации, поступающей из конкретной подсети 172.16.4.0, все остальные потоки данных будут направлены далее
deny	Поток данных, удовлетворяющий выбранным параметрам, не будет направлен далее
172.16.4.0	IP-адрес подсети источника
0.0.0.255	Шаблон маски, нули указывают позиции, которые должны соответствовать словиям, в то время как единицы указывают позиции значение которых не влияет на доступ Маска с нулями в первых трех октетах указывает, что эти позиции должны удовлетворять заданным условиям, 255 в последнем октете показывает, что значение этой позиции не влияет на доступ
permit	Поток данных, удовлетворяющий выбранным параметрам, будет направлен далее
any	Вместо этого параметра подставляется 0.0.0.0 255.255.255.255. о, то все позиции маски равны единицам, означает, что все 32 бита в адресе источника не будут проверяться

Расширенные списки управления доступом

Расширенные списки управления доступом (extended access control list, extended ACL) используются чаще, чем стандартные, поскольку они обеспечивают большие возможности контроля. Рекомендуется, например, использовать их в тех случаях, когда надо разрешить передачу данных в Worldwide Web и заблокировать протоколы FTP (File Transfer Protocol) или Telnet для

использования их сетями, не принадлежащими компании. Расширенные списки проверяют как адрес источника, так и адрес получателя. Они могут также проверять конкретные протоколы, номера портов и другие параметры. Это придает им большую гибкость в задании проверяемых условий. Пакету может быть разрешена отправка или отказано в передаче в зависимости от того, откуда он был выслан и куда направлен. Например, на рис. 6.10 изображен расширенный список, который разрешает отправку электронной почты с EO на SO, но блокирует вход в систему с удаленных хостов и передачу файлов.

Предположим, что интерфейс EO на рис. 6.10 логически связан с расширенным списком управления доступом. Это означает, при создании списка были аккуратно и последовательно записаны соответствующие директивы. Перед тем, как пакет будет направлен на интерфейс, он проверяется списком управления доступом, связанным с этим интерфейсом.

На основании проверки, выполняемой расширенным списком, пакету может быть разрешена передача или отказано в доступе. Для выходных списков это означает, что пакет, которому разрешена передача, будет непосредственно направлен на EO. Если пакет не соответствует условиям списка, то он будет отброшен. Список управления доступом маршрутизатора обеспечивает контроль с помощью брандмауэра для запрещения использования интерфейса EO. При отбрасывании пакетов некоторые протоколы отправляют один пакет отправителю, сообщая, что получатель недостижим.

Для одного списка можно определить несколько директив. Каждая из них должна ссылаться на имя или на номер, для того, чтобы все они были связаны с одним и тем же списком. Количество директив может быть произвольным и ограничено лишь объемом имеющейся памяти. Конечно, чем больше в списке директив, тем труднее понять работу списка и контролировать ее. Поэтому рекомендуется аккуратно заносить всю информацию о списках в специальный журнал.

Может оказаться, что стандартные списки управления доступом (имеющие номера от 1 до 99) не обеспечивают требуемого уровня управления фильтрацией потока данных. Стандартные списки осуществляют фильтрацию на основе адреса источника и маски Они также могут полностью разрешить или заблокировать использование протокола управления передачей (Transmission Control Protocol, TCP). Возможно, что потребуется более точный способ управления потоком данных и доступом.

Более точное управление потоком и фильтрацией можно осуществить с помощью расширенных списков управления доступом. Их директивы проверяют как адрес источника, так и адрес получателя пакета. Кроме того, в конце директивы расширенного списка имеется поле, указывающее номер порта необязательного протокола TCP или протокола передачи пользовательских дейтаграмм (User Datagram Protocol, UDP), что обеспечивает дополнительную точность фильтрации. Эти номера соответствуют номерами портов протоколов TCP/IP. Некоторые часто используемые номера портов приведены в табл. 6.2.

Таблица 6.2. Общие номера портов

Номер порта (десятичный)	IP-протокол
20	Данные протокола FTP
21	Программа FTP
23	Telnet
25	Simple Mail Transport Protocol (SMTP)
53	DNS
69	TFTP

Можно задать логическую операцию, которую расширенный список будет выполнять с отдельными протоколами. Номера расширенных списков находятся в диапазоне от 100 до 199.

Примеры расширенных списков управления доступом

Полный формат команды access-list имеет следующий вид.

Router(config)# **access-list** *номер-списка* **{permit** | **deny}** *протокол* **source** *[маска-источника* **destination** *маска-получателя] [оператор операнд]* **[established]** [log]

Параметры команды имеют следующие значения.

Параметр	Описание
номер-списка	Указывает список, используются номера от 100 до 199
permit | deny	Указывает на то, разрешает ли данная позиция доступ к указанному адресу
протокол	Используемый протокол, например IP, TCP, UDP, ICMP, GRE или IGRP
source и destination	Указывает адреса источника и получателя
Маска - источника и *маска -получателя*	Шаблон маски, нули указывают позиции, которые должны соответствовать заданным условиям, в то время как единицы указывают позиции, значение которых не влияет на доступ
оператор операнд	it, gt, eq, neq (меньше чем, больше чем, равно, не равно) и номер порта
established	Разрешает прохождение TCP-потока если он использует установленное соединение (т е если бит АСК в заголовке сегмента установлен)

Команда ip access-group связывает созданный расширенный список с выходным или входным интерфейсом. Следует обратить внимание на то, что каждому порту, протоколу и направлению может соответствовать только один список. Команда имеет следующий формат.

Router(config)# **ip access-group** *номер-списка* **{in | out}**

Параметры команды имеют следующие значения.

Параметр	Описание
номер - *списка*	Указывает номер списка, который будет логически связан с этим интерфейсом
in I out	Выбирает, к каким пакетам данного интерфейса будет применяться условие приходящим или к отправляемым. Если не указан параметр in или out, то по умолчанию принимается значение out

Адресам источника и получателя или конкретным протоколам, использующим расширенные списки, должны быть присвоены номера из диапазона от 100 до 199. Номерам портов протоколов верхнего уровня TCP и UDP, в дополнение к другим условиям, также должны быть присвоены номера из этого диапазона. Некоторые часто используемые зарезервированные номера портов приведены в табл. 6.3.

Таблица 6.3. Зарезервированные номера часто используемых портов

Десятичное число	Ключевое слово	Описание	Протокол
0		Зарезервировано	

1-4		Не назначено	
20	FTP-DATA	FTP (данные)	TCP
21	FTP	FTP	TCP
23	TELNET	Терминальное соеди-	TCP
25	SMTP	SMTP	TCP
42	NAMESERVER	Сервер имен	UDP
53	DOMAIN	DNS	TCP/UDP
69	TFTP	TFTP	UDP
70		Gopher	TCP/IP
80		WWW	TCP
133-159		Не назначены	
160-223		Зарезервированы	
161		FNP	UDP
224-241		Не назначены	
242-255		Не назначены	

Примеры конфигурации расширенных списков управления доступом в приведенных ниже разделах относятся к сети, показанной на рис. 6.11. В первом примере блокируется протокол FTP для EO. Во втором примере блокируется только выход Telnet с интерфейса EO, а всем остальным потокам данных доступ разрешен.

Пример 1 расширенного списка доступа: блокировка протокола FTP на интерфейсе EO

В листинге 6.4 показан расширенный список управления доступом, который блокирует поток данных протокола FTP.

Листинг 6.4. Отказ протоколу FTP в доступе к интерфейсу eo

```
access-list  101 deny tcp  172.16.4.0        0.0.0.255   eq  20
                           172.16.3.0        0.0.0.255   eq  21
access-list  101 permit  ip  172.16.4.0     0.0.0.255
                             0.0.0.0      255.255.255.255
(неявно отказывает в доступе всем остальным;   в тексте это не отображается) (ac-
cess-list  101 deny  ip 0.0.0.0  255.255.255.255
                           0.0.0.0   255.255.255.255   )


interface  ethernet  0 ip access-group  101
```

Вот описание значений соответствующих полей листинга 6.4.

Поле	Описание
101	Номер списка управления доступом; указывает на расширенный список
deny	Поток данных, удовлетворяющий условию, будет блокирован
tcp	Протокол транспортного уровня
172.16.4.0 и 0.0.0.255	Адрес и маска источника, первые три октета должны отвечать условию, последний не имеет значения
172.16.3.0 и 0.0.0.255	Адрес и маска получателя, первые три октета должны отвечать условию, последний

	не имеет значения
eq 21	Указывает на известный номер порта для протокола FTP
eq 20	Указывает на известный номер порта для данных протокола FTP

Команда **interface EO access-group** 101 связывает 101-й список управления доступом с выходным интерфейсом EO. Отметим, что этот список не блокирует поток данных FTP; блокируются только порты 20 и 21. На серверах FTP легко может быть установлена конфигурация для работы на различных портах. Следует ясно осознавать, что описанные выше хорошо известные номера портов не гарантируют, что службы будут предоставляться именно на них.

Пример 2 расширенного списка доступа: разрешение доступа только на интерфейс EO и блокирование всех остальных потоков данных

В листинге 6.5 показан расширенный список управления доступом, который разрешает поток данных на интерфейс EO для протокола SMTP.

Листинг 6.5. Разрешение доступа только на интерфейс EO и блокирование всех остальных потоков данных

```
access-list 101 permit tcp 172.16.4.0     0.0.0.255 any eq 25
(неявно отказывает в доступе всем остальным; в тексте это не отображается)
(access-list   101   deny  ip  0.0.0.0     255.255.255.255
                               0.0.0.0     255.255.255.255)
interface ethernet 0 ip access-group 101
```

Ниже описаны значения отдельных полей листинга 6.5.

Поле	Описание
101	Номер списка управления доступом; указывает на расширенный список
permit	Поток данных, удовлетворяющий условию, будет направлен далее
tcp	Протокол транспортного уровня
172.16.4.0 и 0.0.0.255	Адрес и маска источника; первые три октета должны отвечать условию,последний не имеет значения
0.0.0.0 и 255.255.255.255	Адрес и маска получателя; все значения октетов не имеют значения
eq 25	Указывает на известный номер порта для SMTP
access-group 101	Направляет каналы списка управления доступом на интерфейс выходного порта EO

В этом примере разрешается пересылка SMTP-потока данных (eq 25) от сети 172.16.4.0 с интерфейса EO. Пересылка всех остальных данных от любого источника к любому получателю разрешена, как это указано ключевым словом any. Конфигурация интерфейса EO установлена командой access-group 101 out. Таким образом, список 101 связывается с интерфейсом EO выходного порта.

Использование именованных списков управления доступом

Именованные списки позволяют обращаться к стандартным и расширенным спискам управления доступом с помощью символьной строки (набор символов из букв и цифр) вместо номера (от 1 до 199). Именованные списки могут быть использованы для удаления из списков отдельных строк. Это позволяет модифицировать списки без их предварительного удаления и повторного конфигурирования. Рекомендуется использовать именованные списки в следующих случаях.

- Если желательно интуитивно определить список, используя символьное имя.
- Если уже имеется более 99 стандартных и более 100 расширенных списков, которые требуется сконфигурировать на маршрутизаторе для данного протокола.

Перед конкретной реализацией именованного списка следует принять во внимание следующее.

- Именованные списки несовместимы с версиями операционной системы Cisco, предшествовавшими версии 11.2.
- Нельзя использовать одно и то же имя для нескольких списков. Кроме этого, списки различных типов не могут иметь одинаковых имен. Например, нельзя присвоить имя George стандартному списку и одновременно расширенному списку.
- Для присвоения списку имени необходимо выполнить следующую команду.

```
Router(config)#  ip access-list   {standard   |   extended}   имя
```

В режиме конфигурирования можно указать одно или несколько условий разрешения или блокирования доступа. Этим определяется, будет ли пакет пропущен или отброшен.

```
Router (config   {std-   |   ext-}  nacl)# deny  {источник   [шаблон-источника]
        |  any}
```

или

```
Router (config {std- | ext-} nacljt permit (источник [шаблон-источника]
        | any}
```

Приведенная ниже конфигурация создает стандартный список управления доступом с именем `Internetfilter` и расширенный список с именем `marketinggroup`:

```
interface ethernetO/5
ip address 2.0.5.1   255.255.255.0
ip address-group Internetfliter out
ip address marketinggroup in
. . .
ip access-list standard Internetfliter
permit 1.2.3.4

deny any
ip access-list ip extended marketinggroup
permit tcp any 171.69.0.0   0.255.255.255  eq telnet

deny tcp any any
deny   udp any 171.69.0.0   0.255.255.255  It 1024

deny ip any log
```

Команда deny

Команда deny используется при конфигурировании списков управления доступом для задания условий в именованных списках. Полный синтаксис команды имеет вид:

deny *(источник [шаблон-источника]* \ **any** } [log]

Форма этой команды с ключевым словом по используется для удаления условия блокировки доступа. Синтаксис команды:

no deny *[источник [шаблон-источника]* \ **any**}

В приведенном ниже примере устанавливается условие блокировки для стандартного списка с именем Internetfilter:

```
ip access-list standard Internetfilter
   deny   192.5.34.   0 0.0.0.255
   permit 128.88.0.0  0.0.255.255
   permit 36.0.0.0    0.255.255.255
! (Примечание: всем остальным доступ блокирован неявным образом)
```

Команда permit

Команда **permit** используется при установке конфигурации именованного списка ля задания условий разрешения доступа. Полный синтаксис команды:

permit { источник *[шаблон-источника]* | **any** } [**log**]

Форма этой команды с ключевым словом по используется для удаления условия из ;писка. Синтаксис команды:

no permit { *источник [шаблон-источника]* \ **any** }

Эта команда используется в режиме задания конфигурации списка вслед за командой **access-list** для задания условий, при которых пакет проходит через список управления доступом.

Приводимый ниже пример задает стандартный список с именем Internetfilter:

```
ip access-list standard Internetfilter
   deny   192.5.34.0   0.0.0.255
   permit 128.88.0.0   0.0.255.255
   permit 36.0.0.0     0.255.255.255
!(Примечание: всем остальным доступ неявным образом блокирован)
```

В следующем примере директивы разрешения доступа и блокировки не имеют номера, а ключевое слово **no** удаляет одно из условий именованного списка:

```
Router(config (std- | ext-} nacl)# {permit | deny} {ip ACL условия отбора}
{permit | deny} {ip ACL условия-отбора}
no {permit | deny} {ip ACL условия-отбора}
```

В следующем примере на интерфейсе активизируется именованный список доступа протокола IP:

```
Router(config-if)# ip access-group {имя \ 1-199 {in | out}}
```

В следующем примере приведен полный листинг:

```
ip access-list extended come_on
permit tcp any 171.69.0.0  '0.255.255.255  eq telnet

deny tcp any any
deny udp any 171.69.0.0   0.255.255.255  It 1024

deny ip any any
interface ethrnetO/5
ip address 2.0.5.1   255.255.255.0
ip access-group over_out out
ip access-group come_on  in
ip access-list standard over_and
permit 1.2.3.4
```

```
deny any
```

Использование списков управления доступом с протоколами

Списки управления доступом могут управлять на маршрутизаторе Cisco большинством протоколов. Для этого номер протокола указывается в качестве первого аргумента глобальной директивы списка. Маршрутизатор определяет требуемый тип программного обеспечения на основе нумерованной ссылки. Для одного протокола могут использоваться несколько списков. Для каждого списка выбирается новый номер протокола из соответствующего диапазона. Однако для каждого интерфейса и протокола может использоваться только один список. Для некоторых протоколов на одном интерфейсе можно сгруппировать до двух списков — один для входного интерфейса и один для выходного. Для других протоколов возможно использование только одного списка, который обрабатывает как приходящие, так и исходящие пакеты. Если список является входным, то при получении маршрутизатором пакета программное обеспечение Cisco проверяет его на соответствие условиям директив. Если пакету предоставляется доступ, то он продолжает обрабатываться программным обеспечением. Если в доступе ему отказано, то пакет отбрасывается. Если список является выходным, то после получения и направления его маршрутизатором на выходной интерфейс, он проверяется на соответствие условиям директив. Если разрешение на доступ получено, то программное обеспечение передает пакет далее. Если доступ блокирован, то пакет отбрасывается и помещается в битовую корзину.

Инженерный журнал: присвоение протоколу имени или номера

Протоколу может быть присвоено имя, которым может быть одно из ключевых слов: eigrp, gre, icmp, igmp, igrp, ip, ipinip, nos, ospf, top, udp или число, которое представляет собой номер протокола и может быть целым числом в диапазоне 1-255. Для Internet-протоколов (включая ICMP, TCP и UDP) следует использовать ключевое слово ip. Протоколы и соответствующие им номера приведены в стандарте RFC 1700.

Размещение списков управления доступом

Как было описано ранее, списки управления доступом используются для контроля потоков данных путем фильтрации пакетов и уничтожения нежелательных потоков. От того, где размещен список, зависит эффективность его применения. Потоки данных, которым отказывается в доступе, и источник которых находится на большом удалении от маршрутизатора, не должны использовать сетевые ресурсы на пути к нему.

Предположим, что цель компании состоит в том, чтобы отказать в доступе Telnet-и FTP-потокам к порту E1 маршрутизатора D коммутируемой локальной сети Ethernet на порте E1 маршрутизатора A, как показано на рис. 6.12. В то же самое время все остальные потоки данных должны проходить беспрепятственно. Добиться поставленной Цели можно несколькими способами. Рекомендуется подход, связанный с использованием расширенного списка управления доступом, который выполняет проверку как адреса источника, так и адреса получателя. Расширенный список следует расположить на маршрутизаторе A. Тогда пакеты не проходят по Ethernet-сети маршрутизатора A герез последовательные интерфейсы маршрутизаторов B и C и не поступают на мар-лрутизатор D. Потокам данных с различными адресами источника и получателя по-зрежнему предоставляется доступ к портам маршрутизаторов.

Рекомендуется размещать список управления доступом как можно ближе к источнику дан-

ных, которым отказывается в доступе. Стандартные списки не проверяют ад-ес получателя, поэтому стандартный список необходимо размещать как можно ближе пункту назначения. Например, как показано на рис. 6.12, для предотвращения передачи данных с маршрутизатора A стандартный или расширенный список следует разместить на интерфейсе EO маршрутизатора D.

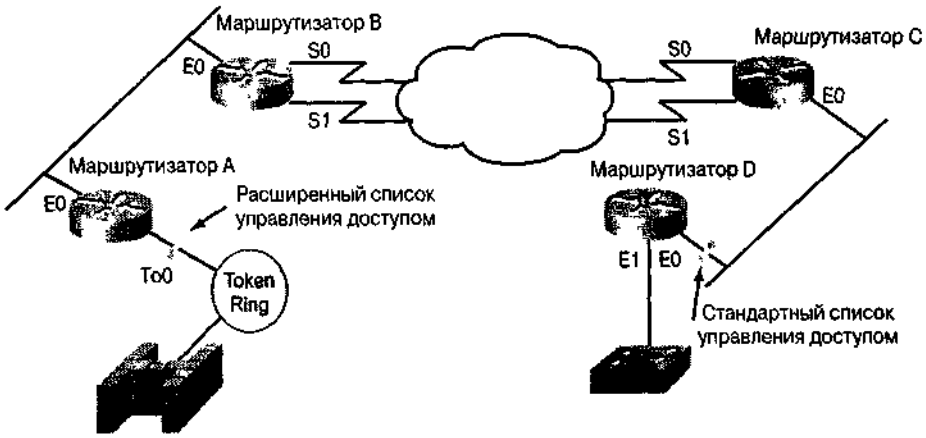


Рис. 6.12. Стандартные списки управления доступом следует размещать как можно ближе к пункту назначения, а расширенные — по возможности ближе к источнику

Использование списков управления доступом с брандмауэрами

Рекомендуется использовать списки управления доступом с маршрутизаторами, которые исполняют роль брандмауэров (firewall) и часто располагаются между внутренней и внешней сетью, такой как Internet. Брандмауэр создает изолированную точку, в результате чего внешние потоки не оказывают воздействия на структуру внутренней сети. Списки управления доступом могут также использоваться на маршрутизаторах, расположенных между двумя частями сети для управления входом и выходом данных из некоторого участка сети.

Примечание

Для большинства протоколов при определении входного списка управления доступом, используемого для фильтрации, в директивы необходимо также включить точные условия, делающие возможными передачу сообщений об изменениях в маршрутизации. Если этого не сделать, то возможна потеря связи с интерфейса в случае блокировки всех поступающих сообщений, в том числе и сообщений об изменениях в маршрутизации. Этого можно избежать, добавив директиву permit any в конец создаваемого списка управления доступом.

Для обеспечения большей безопасности сети следует устанавливать минимальную конфигурацию на **пограничных маршрутизаторах (border routers),** т.е. расположенных на границах сети. Это в большей степени изолирует частную сеть от внешней сети или от менее контролируемой части сети, обеспечивая большую степень защиты.

На пограничных маршрутизаторах списки управления доступом могут быть созданы для каждого сетевого протокола, конфигурация которого установлена на интерфейсах маршрутизатора. При этом можно сделать так, что входные потоки, выходные, или и те и другие будут фильт-

роваться на интерфейсе.

Вашингтонский проект: реализация брандмауэров

Соединение с Internet, предусмотренное в проекте Вашингтонского учебного округа, требует двойной изоляции брандмауэрами всех приложений, открытых для Internet и находящихся в общедоступной магистральной сети. Необходимо обеспечить, чтобы все соединения, сделанные из частной сети каждой школы, были заблокированы.

Настройка архитектуры брандмауэров

Брандмауэр представляет собой структуру, которая создается между частной сетью и внешним миром с целью защиты от несанкционированного вторжения. В большинстве случаев такое вторжение происходит из глобального Internet или из тысяч удаленных сетей, которые он связывает. Обычно сетевой брандмауэр состоит из нескольких устройств, как показано на рис. 6.13.

При такой архитектуре маршрутизатор, подсоединенный к Internet (т.е. внешний) направляет весь входящий поток на шлюз уровня приложения. Маршрутизатор, подсоединенный к внутренней сети (т.е. внутренний) принимает пакеты только со шлюза приложения.

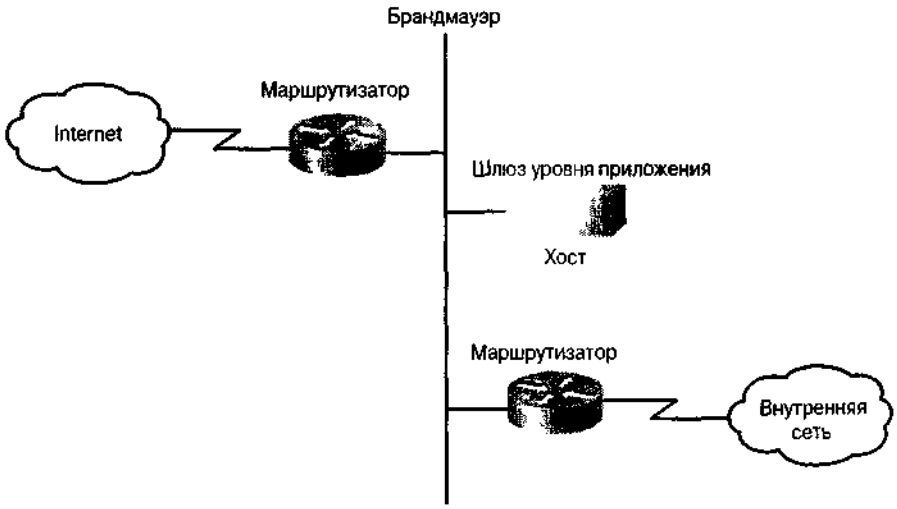


Рис. 6 13 Типичный брандмауэр ограждает сеть от несанкционированного вторжения из Internet

В действительности шлюз контролирует предоставление сетевых услуг как во внутреннюю сеть, так и из нее. Например, некоторым пользователям может быть предоставлено право работы в Internet, или только некоторым приложениям разрешено устанавливать соединение между внутренним и внешним хостами.

Если единственным допустимым приложением является электронная почта, то на [маршрутизаторе должно быть установлено соответствующее ограничение и через него должны проходить только такие пакеты. Это защищает шлюз приложения и предотвращает его переполнение, которое может привести к тому, что часть данных будет отброшена.

Инженерный журнал: использование маршрутизатора в качестве брандмауэра

В настоящем разделе описывается ситуация, показанная на рис. 6.13, где требуется с помощью списков управления доступом ограничить потоки данных на брандмауэр и с него.

Использование специально предназначенного для этого маршрутизатора в качестве брандмауэра является весьма желательным, потому что при этом маршрутизатор имеет четко выраженную цель и используется в качестве внешнего шлюза, не загружая этой работой другие маршрутизаторы. При необходимости изоляции внутренней сети брандмауэр создает изолированную точку и потоки данных во внешней сети не затронут внутреннюю сеть.

В приведенной ниже конфигурации брандмауэра подсеть 13 сети класса В представляет собой подсеть брандмауэра, а подсеть 14 обеспечивает связь с глобальной сетью Internet через провайдера услуг.

```
interface ethernet O
ip address B.B.13.1  255.255.255.0
interface  serial  0
ip address B.B.14.1     255.255.255.0
router igrp
network B.B.0.0
```

Эта простая конфигурация не обеспечивает никакой защиты и поток данных из внешнего мира поступает во все сегменты сети. Для обеспечения безопасности на брандмауэре необходимо использовать списки управления доступом и группы доступа.

Список управления доступом определяет потоки, которым будет предоставлен доступ или отказано в нем, а группа доступа применяет условия списка к некоторому интерфейсу. Списки могут быть использованы для блокировки соединений, которые представляются потенциально опасными и для разрешения доступа всем другим соединениям или предоставлять доступ некоторым соединениям и блокировать его для всех других. При установке конфигурации брандмауэров последний метод является более надежным.

Наилучшим местом для создания списка является хост. Для этого используется какой-либо текстовый редактор. Можно создать файл, содержащий команды access-list, а затем загрузить его в маршрутизатор. Перед загрузкой списка доступа все предыдущие определения должны быть удалены с помощью команды

no access-list 101

После этого команда access-list может быть использована для разрешения доступа всем пакетам, возвращающимся по уже установленным соединениям. Если использовать ключевое слово established, то условие будет выполнено, когда в заголовке TCP-сегмента будет установлен бит подтверждения (АСК) или бит сброса (RST).

```
access-list   101  permit  tcp  0.0.0.0     255.255.255.255

                                0.0.0.0     255.255.255.255  established
```

После загрузки списка управления доступом на маршрутизатор и записи его в энергонезависимую оперативную память (nonvolatile random-access memory, NVRAM), этот список можно связать с соответствующим интерфейсом. В данном примере поток данных, поступающий из внешнего мира через последовательный интерфейс О фильтруется перед размещением его в подсети 13 (ethernet 0). Поэтому команда access-group, назначающая список входным фильтрующим соединениям, должна выглядеть следующим образом.

```
interface ethernet O

ip access-group 101
```

Для управления выходным потоком из частной сети в Internet необходимо определить список управления доступом и применить его к пакетам, отсылаемым с последователь-

ного порта 0 маршрутизатора. Для этого возвращающимся пакетам, с хостов, использующих Telnet или FTP, должен быть разрешен доступ к подсети брандмауэра в. в. 13.0

Если имеется несколько внутренних сетей, подсоединенных к брандмауэру, и он использует выходные фильтры, то поток данных между внутренними сетями будет ограничен в связи с использованием фильтров списков управления доступом. Если входные фильтры используются только на интерфейсе, связывающем маршрутизатор с внешним миром, то ограничений на связь между внутренними сетями не будет.

Проверка правильности установки списков управления доступом

Команда **show ip interface** отображает информацию об интерфейсах и показывает, установлены ли списки управления доступом. Команда **show access-lists** отображает содержимое всех списков. При вводе имени списка управления доступом или его номера в качестве параметра этой команды отображается содержимое конкретного списка, как показано в листинге 6.6.

Листинг 6.6. Отобразить IP-интерфейс

```
Router> show

Ethernet0 is up, line protocol is up
    Internet address is 192.54.22.2, subnet mask is 255.255.255.0
    Broadcast address is 255.255.255.255
    Address determined by nonvolatile memory
    MTU is 1500 bytes
    Helper address is 192.52.71.4
    Secondary address 131.192.115.2, subnet mask 255.255.255.0
    Outgoing ACL 10 is set
    Inbound ACL is not set
    Proxy ARP is enabled
    Security level is default
    Split horizon is enabled
    ICMP redirects are always sent
    ICMP unreachables are never sent
    ICMP mask replies are never sent
    IP fast switching is enabled
    Gateway Discovery is disabled
    IP accounting is disabled
    TCP/IP header compression is disabled
    Probe proxy name replies are disabled
Router>
```

Резюме

- При работе Cisco-маршрутизатора списки управления доступом выполняют несколько функций, в том числе реализуют процедуры разрешения/запрещения доступа и процедуры обеспечения безопасности.
- Списки управления доступом используются для управления трафиком.
- В некоторых протоколах на одном интерфейсе могут быть установлены два списка управления доступом — один для входа, другой для выхода.
- При использовании списков управления доступом после проверки пакета на соответствие директиве списка этому пакету может быть разрешено или запрещено использование некоторого интерфейса в группе доступа.
- Биты IP-адреса (число 0 или число 1) указывают способ обработки соответствующего бита.
- Списки управления доступом могут быть сконфигурированы для работы со всеми маршрутизируемыми сетевыми протоколами для фильтрации или пропуска проходящих пакетов.
- Списки управления доступом обычно используются на маршрутизаторах, выполняющих роль брандмауэров, которые размещены между внутренней и внешней сетью, такой как Internet.

Задачи проекта Вашингтонского учебного округа: использование списков управления доступом

В настоящей главе были изучены понятия, связанные с использованием списков управления доступом, и описан процесс их конфигурирования. Это поможет при реализации списков управления доступом в сети Вашингтонского учебного округа. Для выполнения требований, предъявляемых к проектированию сети и обеспечению ее защиты необходимо решить следующие задачи.

1. Обосновать необходимость использования списков управления доступом и создать логическую диаграмму, описывающую общее влияние этих списков на всю сеть округа.
2. Выбрать тип списков управления доступом, которые будут установлены на маршрутизаторах округа, место их установки и причины выбора данного места.
3. Записать последовательность команд, которую необходимо выполнить для реализации списков управления доступом на маршрутизаторе каждой школы.
4. Описать влияние каждого списка управления доступом на поток данных между локальными сетями отдельных школ и на сеть всего округа.

Контрольные вопросы

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

1. Какова цель использования списков управления доступом?
2. Какое условие налагает стандартный список управления доступом на IP-пакеты данных?
3. Чем отличаются расширенные списки управления доступом от стандартных списков управления доступом?
4. Каким образом списки управления доступом сравнивают данные пакета с условиями списка?
5. Каким образом маршрутизатор различает стандартные списки управления доступом и расширенные?
6. Какую из приведенных ниже команд следует использовать для того, чтобы выяснить, установлены ли на данном интерфейсе списки управления доступом?
   A. `show running-config`
   B. `show ip protocols`
   C. `show ip interface`
   D. `show ip network`

7. Как называются дополнительные 32 бита в директиве **access-list**?

A. Биты шаблона.
B. Биты доступа.
C. Нулевые биты.
D. Единичные биты.

8. Какому из приведенных ниже высказываний эквивалентно выполнение команды Router(config**)# access-list 156.1.0.0 0.0.255.255**?

A. "Отказать в доступе только к моей сети."
B. "Разрешить доступ к конкретному хосту."
C. "Разрешить доступ только к моей сети."
D. "Отказать в доступе к конкретному хосту."

9. Утверждение: "При задании разрешения на доступ в списке управления, сопровождаемом неявным "отказать всем", всем потокам данных, кроме указанного в директиве permit, будет отказано в доступе".

A. Истинно.
B. Ложно.

10. Команда **show access-list** используется для того, чтобы:

A. просмотреть, установлены ли списки управления доступом;
B. просмотреть директивы списка управления доступом;
C. наблюдать за отладкой установки списков управления доступом;
D. просмотреть группировку списков управления доступом.

Основные термины

Битовая корзина (bit bucket). Место, в которое направляются отвергнутые маршрутизатором биты.

Брандмауэр (firewall). Маршрутизатор(ы) или сервер(ы) доступа, предназначенный для создания буфера между соединенными общедоступными и частными сетями. Для обеспечения безопасности частных сетей брандмауэр использует списки управления доступом и другие методы.

Доменная система имен (Domain Name System, DNS). Система, используемая в Internet для преобразования имен сетевых узлов в сетевые адреса

Очередность (queuing). Положение, при котором списки управления доступом задают обработку маршрутизатором некоторых пакетов ранее всех остальных данных.

Пограничный маршрутизатор (border router). Маршрутизатор, расположенный на границе сети и обеспечивающий функции защиты некоторой частной области сети от внешних сетей или от более доступных областей сети.

Расширенный список управления доступом (extended access control list, Extended ACL). Список управления доступом, проверяющий адреса источника и получателя.

Список управления доступом (access control list, ACL). Список, находящийся на маршрутизаторе Cisco и используемый для управления доступом к ряду услуг, предоставляемых маршрутизатором (например, для запрещения пакетам с определенными IP-адресами, покидать определенный порт маршрутизатора).

Стандартный список управления доступом (standard access control list, standard ACL). Список управления доступом, осуществляющий фильтрацию на основе адреса источника и шаблон маски. Стандартные списки управления доступом разрешают или запрещают доступ всему набору протоколов TCP/IP.

Шаблон маски (wildcard mask). 32-битовая последовательность, используемая наряду с IP-адресом для определения того, какие биты в IP-адресе следует проигнорировать при сравнении этого адреса с другим IP-адресом. Шаблон маски указывается при установке списка управления доступом.

Ключевые темы этой главы

- Объясняется, каким образом маршрутизаторы корпораций Cisco используются в сетях NetWare
- Описывается семейство протоколов Novell NetWare
- Описывается адресация протокола Novell IPX
- Описывается инкапсуляция Novell
- Объясняется, каким образом корпорация Novell использует протокол RIP для маршрутизации
- Описывается протокол уведомления о службах (Service Advertising Protocol)
- Описывается процесс конфигурирования Ethernet-маршрутизатора и последовательных интерфейсов с IPX-адресами
- Описывается процесс нахождения IPX-адресов на удаленных маршрутизаторах
- Описываются проверка работоспособности протокола IPX и связи между маршрутизаторами
- Описывается процесс устранения ошибок в работе протокола IPX

Глава 7

Протокол Novell IPX

Введение

Novell NetWare представляет собой **сетевую операционную систему (network operating system,** NOS), которая предоставляет персональным компьютерам и другим клиентам доступ к своим серверам Серверы NetWare предоставляют клиентам ряд сетевых служб, таких как совместный доступ к файлам и принтерам, службы каталогов и доступ к Internet Многие серверы NetWare функционируют в качестве Internet- и intranet-серверов, а также в качестве прикладных платформ для баз данных, предоставляемых для совместного использования Разработки Novell охватывают обширный сегмент рынка сетевых операционных систем (более 5 миллионов сетей и более 50 миллионов клиентов)

В качестве дополнения к протоколу управления передачей и Internet-протоколу (Transmission Control Protocol/Internet Protocol), **протокол межсетевого обмена пакетами (Internetwork Packet Exchange, IPX),** разработанный корпорацией Novell также является широко используемым в сетевой индустрии протоколом До выхода в 1998 году пятой версии ОС Novell NetWare все сети NetWare использовали протокол IPX Как и AppleTalk, Novell перевела ОС NetWare на использование протокола IP Поскольку IPX-сети уже установлены и работают, целесообразно поддерживать их и далее В этой главе описывается протокол Novell IPX, его принцип действия и конфигурирование

Вашингтонский проект: реализация протокола IPX

В этой главе описывается использование протокола Novell IPX в сети Вашингтонского учебного округа Необходимо установить серверы рабочих групп во всех компьютерных классах каждой школы Компьютерные классы находятся в соответствующих образовательных сегментах локальной сети Службы обоих видов, IP и IPX, следует объявить в сети округа для других образовательных сегментов локальной сети

Маршрутизаторы корпорации Cisco в сетях NetWare

Корпорации Cisco и Novell в течение многих лет сотрудничали с целью разработки и внедрения сетей, основанных на операционной системе NetWare. Хотя многие протоколы NetWare первоначально разрабатывались для использования в небольших однородных локальных сетях, корпорация Cisco внесла ряд усовершенствований с целью повышения производительности протоколов NetWare в крупных и разнородных сетях. Корпорация Cisco поддерживает многочисленные разновидности основного набора протоколов NetWare. Эти разновидности являются частью **программного обеспечения межсетевой операционной системы корпорации Cisco (Cisco Internetwork Operation System, IOS).**

Набор протоколов Novell NetWare

Корпорация Novell разработала и представила в распоряжение пользователей систему NetWare в начале 80-х годов двадцатого века. NetWare использует архитектуру типа клиент/сервер. Клиенты (иногда называемые также *рабочими станциями)* запрашивают у серверов службы, такие, например, как доступ к файлам и принтерам. В отличие от серверов сетей Windows NT, серверы NetWare являются выделенными и не могут использоваться в качестве рабочих станций клиентов. На рис. 7.1 представлен набор протоколов NetWare, протоколы доступа к передающей среде, поддерживаемые Cisco и NetWare, а также связь между протоколами NetWare и эталонной моделью взаимодействия открытых систем OSI.

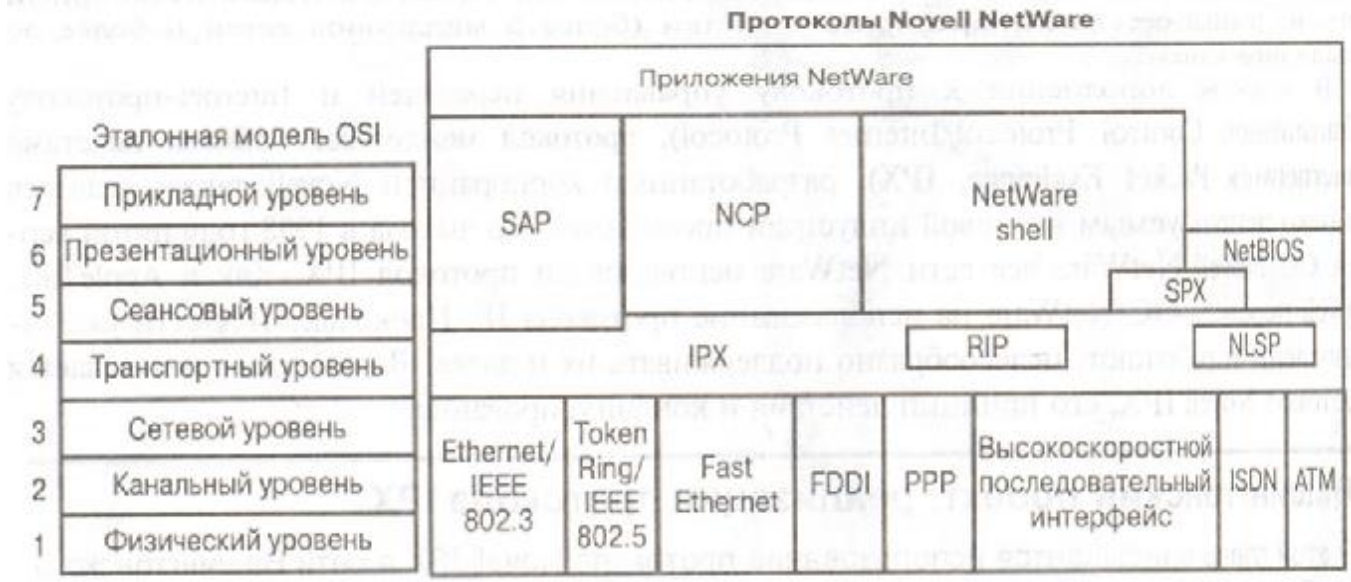


Рис. 7.1. Семейство протоколов NetWare поддерживает все типовые протоколы доступа к передающей среде

Примечание

Дейтаграмма представляет собой блок инкапсулированных данных, который проходит по сети и не требует подтверждения. Дейтаграммы используются протоколом IP и протоколом передачи пользовательских дейтаграмм (User Datagram Protocol, UDP). Слово *дейтаграммный* часто используется для описания протоколов и сетей, которые делят данные на дискретные блоки и не требуют подтверждения о доставке.

Novell IPX представляет собой набор протоколов, включающий в себя следующее.

- Протокол передачи дейтаграмм без установки логического соединения и без подтверждения о доставке каждого пакета.
- Протокол 3-го уровня, определяющий сеть и адреса узлов.
- Протокол маршрутной информации корпорации Novell (Routing Information Protocol, RIP), отличающийся от IP тем, что облегчает обмен информацией о маршрутизации.
- **Протокол уведомления о службах (Service Advertising Protocol, SAP)**, используемый для объявления об имеющихся в сети службах.
- Основной протокол NetWare (NetWare Core Protocol, NCP) для обеспечения соединения клиента с сервером и для использования приложений.
- **Протокол последовательного обмена пакетами (Sequenced Packet Exchange, SPX)** для служб 4-го уровня, ориентированных на логическое соединение.

Примечание

SPX представляет собой общий протокол транспортного (4-го) уровня сетей NetWare. SPX— надежный, ориентированный на логическое соединение протокол (аналогичный TCP), функционирующий на основе служб, предоставляемых протоколом IPX.

Обзор протокола IPX

IPX представляет собой протокол 3-го уровня, который используется для направления пакетов через взаимосвязанные сети. Под IPX понимаются дейтаграммы, передаваемые без установки логического соединения, подобно тому, как происходит передача IP-пакетов в сетях, использующих протоколы TCP/IP

IPX аналогичен TCP/IP и работает в тех же сетях. IPX также предоставляет возможность мультипротокольной маршрутизации. Ниже приведены некоторые характеристики IPX.

- IPX используется в клиент/серверном окружении.
- Он использует структуру адресации типа *сеть.узел.*
- Логический адрес этого протокола содержит MAC-адрес интерфейса.
- Протокол Novell RIP использует дистанционно-векторные метрики — такты задержки и количество переходов.
- Клиенты и серверы соединены в **точке доступа к службе (service access point);** используются широковещательные рассылки **протокола определения ближайшего сервера (Get Nearest Server, GNS)**.

IPX использует дистанционно-векторные протоколы (такие, например, как RIP) или протоколы состояния канала связи (такие как **протокол канальных служб NetWare (NetWare Link Services Protocol, NLSP).** IPX RIP рассылает обновления таблицы маршрутизации каждые 60 секунд. В качестве метрик маршрутизации RIP использует сетевые задержки и количество переходов. Область его действия ограничена 16 переходами.

Адресация в Novell IPX

В IPX-адресации Novell используются адреса, состоящие из двух частей — номера сети и номера узла (рис. 7.2). Номер узла обычно представляет собой MAC-адрес сетевого интерфейса этого узла. Novell IPX поддерживает множество логических сетей на одном сетевом интерфейсе; при этом каждая сеть требует единого типа инкапсуляции. Длина номера сети, который назначается сетевым администратором, не может превышать восьми шестнадцатеричных чисел.

Примечание

Для выбора наилучшего пути IPX в качестве метрики использует такт (tick), который является ожидаемой задержкой при пересылке пакета определенного размера. Один такт равен 1/18 секунды. В случае, когда два пути характеризуются одинаковым числом тактов, для выбора пути IPX RIP применяет количество переходов. Хотя различные реализации RIP имеют много общего, следует отметить, что версия корпорации Novell несовместима с реализациями RIP, используемыми в других наборах сетевых протоколов, таких как TCP/IP.

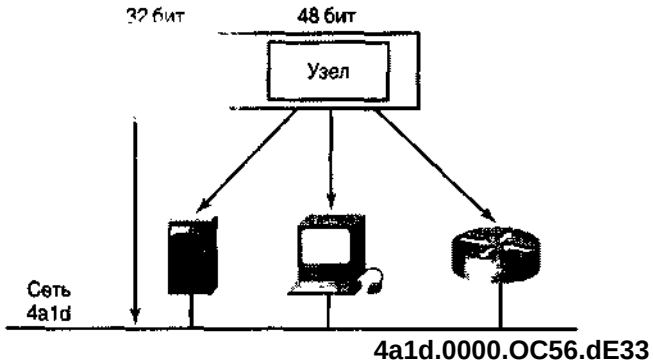


Рис. 7.2. Формат 80-битового адреса протокола Novell IPX; из них 32 бита отводится под номер сети и 48 битов — под номера узла

На рис. 7.3 показаны две IPX-сети: `4ald` и `3f`. IPX-номер узла представляет собой число, состоящее из двенадцати шестнадцатеричных цифр. Обычно этот номер представляет собой MAC-адрес сетевого интерфейса данного узла. Использование MAC-адреса в логической адресации IPX избавляет от необходимости использования протокола преобразования адресов (ARP). Последовательные интерфейсы используют в качестве IPX-адреса узла MAC-адрес Ethernet-адаптера. На рис. 7.3 показан IPX-узел `0000. Oc56.de33` в сети номер `4ald` и узел `0000. Oc56.de34` в сети номер `3f`.

Независимо от того, используется ли интерфейс локальной или распределенной сети маршрутизаторам необходимо назначать те же номера IPX-сетей, какие имеют IPX-устройства, использующие эти маршрутизаторы. Основной способ получить адрес в сетях Novell — обратиться за ним к сетевому администратору. Сетевой администратор должен указать точный IPX-адрес сети, в которой необходимо реализовать поддержку IPX на маршрутизаторе Cisco. На маршрутизаторе Cisco необходимо использовать существующий в этой сети IPX-адрес. Этот адрес обычно указывается администратором сети NetWare. В тех случаях, когда нет возможности получить IPX-адрес у сетевого администратора, его можно получить от соседнего маршрутизатора. Для этого следует обратиться к соседнему маршрутизатору посредством эмулятора терминала (Telnet) с помощью команд **`show protocols` *или* `show ipx interface`**.

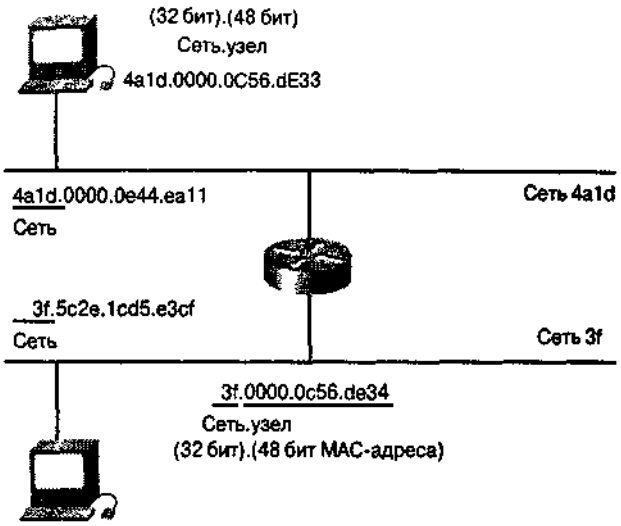


Рис. 7.3. Каждое устройство в сети IPX имеет свой уникальный адрес

Инженерный журнал: команда show ipx interface

Для определения статуса IPX-интерфейсов, конфигурация которых установлена на маршрутизаторе, следует использовать команду show ipx interface в привилегированном режиме (privileged EXEC command mode). Полный синтаксис команды:

show ipx interface *[интерфейс номер]*

Аргумент *interface* означает физический интерфейс и может быть одним из следующих типов: asynchronous (асинхронный), dialer (коммутируемый), ethernet (стандарта IEEE 802.3), FDDI (распределенный интерфейс передачи данных по волоконно-оптическим каналам (Fiber Distributed Data Interface, FDDI), loopback (программный эмулятор физического интерфейса), null (нуль-интерфейс), serial (последовательный), Token Ring или tunnel (туннельный). Аргумент *номер* обозначает номер интерфейса. Например, обозначение ethernet 0 указывает на первый интерфейс типа Ethernet.

Ниже приведен пример листинга, полученного в результате выполнения команды **show ipx interface**.

```
Router# show ipx interface Ethernet  1
Ethernet1   is  up,  line  protocol   is  up
  IPX address is COS.0000.Oc05.6030,  NOVELL-ETHER  [up]  line-up,
      RIPPQ:   0,   SAPPQ:   0
  Delay of  this  Novell  network,   in  ticks  is   1
  IPXWAN processing not  enabled on this  interface.
  IPX SAP update  interval  is  1 minute(s)
```

Ниже представлено подробное объяснение листинга.

Поле	Описание
Ethernet! is..., line protocol…	Тип интерфейса и его текущее состояние. Либо интерфейс подключен к сети и является активным (up), либо отключен и неактивен (down)
IPX address is...	Адрес сети и узла для локального интерфейса маршрутизатора; далее следуют тип инкапсуляции, установленный на интерфейсе и

	статус интерфейса
NOVELL-ETHER	Тип инкапсуляции, используемый на интерфейсе маршрутизатора (если она используется)
[up] line-up	Указывает, активизирована ли IPX-маршрутизация на данном интерфейсе. Line-up означает, что IPX-маршрутизация активизирована командой ipx routing, line-down, соответственно, означает что маршрутизация отключена. Слово в квадратных скобках предоставляет детальную информацию о состоянии IPX-маршрутизации в процессе ее включения-отключения
RIPPQ:	Число пакетов в RIP-очереди
SAPPQ:	Число пакетов в SAP-очереди
Secondary address is...	Адрес вторичной сети, сконфигурированной на данном интерфейсе (если она есть). За ним следует тип инкапсуляции и состояние интерфейса. Эта строка появляется только в том случае, когда посредством команды ipx network был установлен адрес вторичной сети.
Delay of this Novell network, in ticks...	Значение параметра задержки (устанавливается командой ipx delay)
IPXWAN processing..	Показывает, задана ли IPXWAN-обработка на этом интерфейсе. Устанавливается командой ipx ipxwan
IPX SAP update interval	Показывает частоту рассылки SAP-обновлений (устанавливается командой ipx sap-interval)

Вашингтонский проект: вопросы IPX-адресации

При планировании IPX-адресации нет необходимости нумеровать хосты, как это следовало бы сделать в случае использования протоколов TCP/IP. Это происходит потому, что адресами хостов для рабочих станций обычно являются MAC-адреса их сетевых адаптеров. Однако в распределенной сети Вашингтонского учебного округа необходимо разработать схему IPX-нумерации сетей. Нельзя забывать, что у маршрутизатора не может быть двух интерфейсов, принадлежащих одной логической (IP, IPX и др.) сети или подсети. По этой причине нет возможности использовать один сетевой номер во всей распределенной сети округа.

Во время разработки схемы IPX-нумерации следует помнить, что номера сетей могут иметь не более 32 бит (или 8 шестнадцатеричных чисел), но они могут начинаться с ряда нулей для "заполнения адреса" ("pad out"). Например, число 21 (шестнадцатеричное) может быть использовано в качестве приемлемого сетевого номера, поскольку к нему можно добавить нули для расширения до 32-битов (записывается, как 8 шестнадцатеричных чисел): 00000021.

Некоторые сетевые администраторы конвертируют IP-адрес сети в шестнадцатеричную форму и используют полученный результат в качестве IPX-номера сети. Например, подсеть 169.199.69.128/27 можно преобразовать в A9C74580. Однако нет правила, предписывающего поступать именно так. Можно использовать начальные нули для

создания очень простых номеров сетей (например, 10, 20, 30 и т.д.). Далее в настоящей главе будет показано, что из-за проблем на 2-м уровне может возникнуть необходимость функционирования интерфейса маршрутизатора в двух логических сетях, т.е. с двумя сетевыми номерами одновременно. После прочтения раздела, описывающего типы инкапсуляции фреймов в сетях Novell, следует внимательно изучить требования Вашингтонского учебного округа для учета вышесказанного при разработке схемы адресации.

Типы инкапсуляции сетей Novell

NetWare поддерживает несколько типов инкапсуляции (т.е. типов фреймов) для семейства протоколов Ethernet. Все они также поддерживаются маршрутизаторами корпорации Cisco.

Корпорации Xerox, Intel и Digital (известные также под коллективным названием DIX) разработали Ethernet-стандарт в 1980 году. Стандарт был назван *Ethernet версии I (Ethernet Version I).* Два года спустя DIX заменяет его стандартом *Ethernet версии II (Ethernet Version II),* который является стандартным типом инкапсуляции для TCP/IP. Затем в 1982 году Институт инженеров по электротехнике и электронике (Institute of Electrical and Electronic Engineers, IEEE) начинает работу над улучшением структуры фрейма Ethernet. За работу над этим проектом нес ответственность Комитет 802.3. Однако корпорация Novell не могла ждать официального выпуска спецификации фрейма и в 1983 году, основываясь на неоконченной разработке Комитета 802.3, выпустила собственную версию этой спецификации. Novell назвала этот тип фрейма 802.3 (или Ethernet 802.3). Поскольку IEEE окончательно не доработал спецификацию, этот стандарт также иногда называют "сырой Ethernet" (Ethernet raw). Двумя годами позже IEEE, наконец, выпускает окончательную версию спецификации 802.3, в которой фрейм включает в себя заголовок управления логическим каналом (logical link control, LLC). LLC содержит поля, которые указывают точку доступа к службам. Эти поля делают спецификацию IEEE (в настоящее время она называется 802.2) несовместимой с версией Novell 802.3, поскольку фрейм Ethernet 802.2 включает в себя точку доступа к службам. В программном обеспечении IOS корпорации Cisco этот стандарт называется ethemet sap (Novell называет его Ethernet_802.2). Проблемы совместимости версий привели к разработке четвертого типа фреймов — Ethemet SNAP. Основное, о чем необходимо постоянно помнить — их несовместимость друг с другом. Если сервер Novell использует фреймы 802.3, а на маршрутизаторе Cisco установлена инкапсуляция согласно стандарту 802.2, то два эти узла не смогут обмениваться данными.

Ниже приведены основные термины программного обеспечения IOS Cisco и сетей Novell, употребляемые при обсуждении инкапсуляции.

- Ethernet 802.3, называемый также "сырой" Ethernet, является стандартом по умолчанию для сетей NetWare со 2-й версии по 3.11, включительно.
- Ethemet 802.2 или sap (также называемый Novell Ethemet_802.2 или 802.3) представляет собой стандартный формат фреймов IEEE, включая заголовок LLC 802.2. С выходом в свет NetWare версий 3.12 и 4.x эта инкапсуляция стала новым стандартным форматом фреймов Novell и используется также для OSI- маршрутизации.
- Ethernet II или arpa (также называемый Novell Ethernet_II или Ethernet версии II) использует заголовок стандарта Ethernet версии II и применяется с TCP/IP.
- Ethernet SNAP или snap (также называемый Novell Ethernet_SNAP или snap) расширяет заголовок IEEE 802.2 путем добавления к нему заголовка протокола доступа к подсетям (Subnetwork Access Protocol, SNAP), который обеспечивает код "типа инкапсуляции", аналогичный коду, определенному в спецификации Ethernet версии II и используемому с TCP/IP и AppleTalk.

Примечание

На одном интерфейсе можно использовать несколько типов IPX-инкапсуляции, но только в том случае, если этому интерфейсу назначено несколько IPX-номеров сетей. Хотя различные типы IPX-инкапсуляции могут совместно использовать один интерфейс, клиенты и серверы сетей Novell с разными типами инкапсуляции не могут непосредственно обмениваться информацией друг с другом.

Наименования типов инкапсуляции, введенные корпорацией Cisco

Аппаратное и программное обеспечение IOS Cisco поддерживает весь спектр типов инкапсуляции Ethernet/802.3, применяемых в ОС NetWare. Оборудование корпорации Cisco распознает отличия между разнообразными типами пакетов, независимо от того, как они были инкапсулированы. На одном интерфейсе локальной сети может поддерживаться несколько типов инкапсуляции, что позволяет прежним и новым узлам NetWare сосуществовать в одном сегменте локальной сети до тех пор, пока в нем сконфигурированы различные логические сети. Поддержка нескольких типов IPX-инкапсуляции позволяет снизить эксплуатационные расходы, упростить настройку и облегчить переход с одного метода IPX-инкапсуляции на другой.

При конфигурировании IPX-сети может возникнуть необходимость указать тип инкапсуляции на серверах и у клиентов Novell, а также на маршрутизаторе Cisco. Таблица 7.1 помогает выбрать соответствующий тип путем сопоставления терминов Novell и Cisco IOS для одного и того же типа фреймов.

Примечание

Следует убедиться в том, что для соответствующей IPX-инкапсуляции используются наименования Cisco и что типы инкапсуляции серверов, клиентов и маршрутизаторов совпадают. Также следует обратить внимание на то, что, начиная с версии 3.11 NetWare, типы по умолчанию Ethernet IPX-инкапсуляции для маршрутизаторов Cisco не совпадают с типами по умолчанию для серверов Novell.

Таблица 7.1. Названия типов инкапсуляции, используемые корпорацией Cisco

Тип инкапсуляции	Наименование Novell IPX	Наименование Cisco IOS
Ethernet	Ethernet_802.3	novell-ether
	Ethernet_802.2	sap
	Ethernet-II	arpa
	Ethernet SNAP	snap
Token Ring	Token-Ring	sap
	Token-Ring SNAP	snap
FDDI	FDDI SNAP	snap
	FDDI_802.2	sap
	FDDI_RAW	novell-fddi

Конфигурируя маршрутизаторы для учебного округа, необходимо обратить внимание на серверы Novell подключенные к интерфейсу маршрутизатора. Если эти серверы работают под управлением NetWare 3.12 или 4.x, то необходимо настроить интерфейс маршрутизатора на использование ethernet sap в качестве типа фреймов. Если два сервера NetWare подключены к одному порту маршрутизатора и используют при этом разные типы фреймов, то следует настроить интерфейс маршрутизатора на использование нескольких типов пакетов. Таким образом, необходимо создать несколько логических сетей (т.е. интерфейс маршрутизатора будет иметь два IPX-адреса, которые совпадают по номеру хоста, но имеют разные номера сетей).

Примечание

Novell 3.11 представляет собой довольно старую технологию и многие сетевые администраторы перешли к использованию версии 3.12 или 4.x. Вследствие этого, если устанавливается новый сервер, использующий IPX, и Cisco-маршрутизатор, то необходимо в качестве типа фрейма указать sap. Это необходимо потому, что если сервер использует Ethernet 802.2, а рабочая станция использует только Ethernet 802_3, то они не смогут обмениваться информацией друг с другом. Cisco-маршрутизатор по умолчанию будет использовать Ethernet 802.3. Более современные серверы не используют по умолчанию это значение, поэтому, как правило, бывает необходимо явным образом установить конфигурацию инкапсуляции.

Форматы IPX-пакетов

IPX-пакет представляет собой основной информационный блок в сетях Novell NetWare. Ниже представлено описание полей IPX-пакета.

Поле	Описание
Checksum (контрольная сумма)	Показывает, что контрольная сумма не используется, когда это 16-битовое поле заполнено единицами (FFFF)
Packet length (длина пакета)	Указывает длину полной IPX-дейтаграммы в байтах IPX-пакеты могут быть любой длины в пределах максимального размера блока передачи в среде (media transmission unit, MTU) Фрагментация пакетов не допускается
Transport control (контроль транспорта)	Показывает количество маршрутизаторов, через которые прошел пакет. Когда это значение достигает 16, пакет отбрасывается ввиду предположения о возникновении маршрутной петли
Packet type (тип пакета)	Определяет, какой из протоколов верхнего уровня должен принять содержащуюся в пакете информацию. Наиболее часто

встречаются следующие значения.

5 — обозначает протокол SPX;

17 — обозначает протокол NCP.

Маршрутизация в сетях Novell с использованием протокола RIP

Соединение существующих локальных сетей Novell между собой и поддержка большого количества клиентов и серверов NetWare выдвигает особые требования в таких вопросах, как расширяемость и управление сетью. Программное обеспечение Cisco IOS предоставляет несколько принципиальных подходов для поддержания работоспособности больших сетей Novell.

Программное обеспечение Cisco IOS поддерживает стандартный протокол Novell RIP, который представляет собой основу для взаимодействия нескольких локальных сетей Novell. В то же время частая рассылка сообщений об обновлениях, медленная конвергенция во время изменений топологии сети и ограничение, налагаемое RIP на количество переходов (не более 16), делают этот протокол неудобным в крупных сетях или сетях, соединяемых посредством каналов распределенной сети.

Поскольку RIP является дистанционно-векторным протоколом маршрутизации, он использует две метрики для определения пути: такты задержки (ticks) и количество переходов (hop count). Novell RIP проверяет эти метрики, сравнивая вначале такты задержки для различных путей. Затем, если два или более путей имеют одинаковое количество тактов задержки, сравнивается количество переходов в путях. В случае, если два или более путей обладают одинаковым количеством переходов, маршрутизатор осуществляет распределение нагрузки. Распределение нагрузки (load share) означает использование двух или более путей для направления пакетов к одному и тому же пункту назначения. Пакеты при этом распределяются равномерно среди нескольких маршрутизаторов, что в свою очередь приводит к сбалансированной работе и увеличению производительности сети.

Инженерный журнал: команда ipx maximum-path

Для установки максимального количества равноценных путей, которые будут использоваться маршрутизатором при перенаправлении пакетов, следует использовать команду ipx maximum-path в режиме установки глобальной конфигурации. Полный синтаксис команды имеет вид: ipx maximum-path *пути*

Чтобы восстановить значение 1, принятое по умолчанию, следует использовать следующую форму этой команды: no ipx maximum-path

Аргумент *пути* показывает максимальное количество эквивалентных по затратам путей, которые будут использоваться маршрутизатором. Он может принимать значения в диапазоне от 1 до 512. Значение, принятое по умолчанию, равно 1.

Команда **ip$_x$ maximum-path** разработана для повышения пропускной способности. Эта команда позволяет маршрутизатору выбирать параллельные пути среди нескольких эквивалентных по затратам путей (напомним, что изначально маршрутизатор выбирает путь с минимальными затратами). IPX распределяет нагрузку на основе поочередной раздачи пакетов *в* режиме кольцевого списка ожидающих исполнения задач (round-robin fashion), независимо от используемого типа коммутации (быстрая, fast switching) или с обработкой (process switching)). Это означает, что первый пакет посылается по первому пути, второй по второму пути и т.д. Если пакет посылается по последнему выбранному пути, то следующий за ним пакет будет отправлен по первому пути и весь цикл повторится снова.

Ограничение на максимальное количество эквивалентных по затратам путей позво-

ляет оптимально использовать память в случае сложной конфигурации или ограниченного объема памяти маршрутизатора. Кроме того, в сетях с большим количеством различных путей и оконечных систем с ограниченной возможностью кэширования внеочередных пакетов, при использовании нескольких путей эффективность работы может понижаться. В приведенном ниже примере маршрутизатор использует до трех параллельных путей: Router(config)# ipx maximum-paths 3

Таблица маршрутизации Novell RIP отличается от таблицы маршрутизации протокола IP тем, что маршрутизатор ведет отдельную таблицу для каждого активного IPX-протокола. Следовательно, каждый активный IPX-маршрутизатор периодически рассылает копии своей Novell RIP-таблицы маршрутизации ближайшему соседу. Соседние IPX-маршрутизаторы добавляют дистанционные вектора перед передачей копий своих Novell RIP-таблиц своим собственным соседям.

Протокол расщепления горизонта, обладая "наилучшей информацией" предотвращает передачу соседним маршрутизатором широковещательных Novell RIP-таблиц об IPX-информации назад, в сети, из которых он получил эту информацию. Novell RIP также использует механизм устаревания информации для учета условий передачи, в то время как активный IPX-маршрутизатор прекращает работу без рассылки каких-либо сообщений своим соседям. Периодические обновления устанавливают на ноль таймер механизма устаревания. Обновления таблиц рассылаются с 60-секундными интервалами. В некоторых сетях такая частота обновлений может вызвать избыточный поток служебных данных.

Инженерный журнал: команда ipx routing

Для активизации IPX-маршрутизации используется команда ipx routing в режиме установки глобальной конфигурации. Полный синтаксис команды имеет вид:

Ipx routing *[узел]*

Для отключения IPX-маршрутизации используется форма этой команды с ключевым словом по:

no ipx routing [узел]

Аргумент узел в этой команде обозначает узловой номер маршрутизатора. Он является 48-битовой величиной, представленной разделенным точками триплетом из четырехзначных шестнадцатеричных чисел (xxxx. xxxx. xxxx).

Если аргумент узел опущен, то маршрутизатор использует в качестве узлового адреса текущий аппаратный MAC-адрес. Он представляет собой MAC-адрес Ethernet-, Token Ring- или FDDI- платы первого интерфейса. Если в маршрутизаторе нет подходящего интерфейса (например, в случае, когда имеются только последовательные интерфейсы), то аргумент узел является обязательным.

Команда ipx routing активизирует IRX RIP- или SAP-службы маршрутизатора. Если аргумент узел опущен, а MAC-адрес позднее изменяется, то узловой IPX-адрес также автоматически изменяется. Однако связь может быть потеряна в промежутке времени между изменением MAC-адреса и моментом, когда клиенты и серверы IPX узнают о новом адресе маршрутизатора. В приведенном ниже примере активизируется IPX-маршрутизация:

```
Router(config)# ipx routing
```

Инженерный журнал: расширенный протокол IGRP корпорации Cisco

Одним из важнейших средств объединения локальных сетей NetWare является расширенная версия протокола маршрутизации внутреннего шлюза корпорации Cisco. Расширенный IGRP (enhanced IGRP), кроме протоколов TCP/IP, обеспечивает поддержку сетей NetWare и AppleTalk. Расширенный IGRP представляет собой дистанционно-векторный протокол маршрутизации, который обеспечивает быструю конвергенцию в сетевой топологии канальных протоколов маршрутизации. Расширенный IGRP отправляет сообщения об изменениях только когда они действительно происходят, передает только измененную часть таблиц и ограничивает распространение информации об обновлениях только маршрутизаторами, которых это изменение затрагивает. В результате этого расширенный IGRP обеспечивает низкий уровень служебных сообщений, незначительное использование центрального процессора маршрутизатора и умеренные требования к оперативной памяти.

В отличие от протоколов канального уровня расширенный IGRP не требует, чтобы сеть была спроектирована с явной иерархией адресов, что дает сетевому администратору более гибкие средства для подсоединения новых и расширения существующих сетей. Кроме того, расширенный IGRP использует несколько метрик (задержка, ширина полосы пропускания, надежность и нагрузка), что дает более точную картину топологии всей сети и создает возможность более эффективного использования полосы пропускания сети. Расширенный IGRP может уменьшить магистральный поток данных в больших NetWare-сетях на 40-50%. Следствием прекрасной расширяемости и высокой эффективности расширенного IGRP стало то, что с его использованием были реализованы многие большие общедоступные и частные сети.

Для запуска процесса маршрутизации необходимо выполнить следующие действия:

Выполняемое действие	Команда
Переводит процесс маршрутизации расширенного IGRP-протокола в режим установки глобальной конфигурации	**ipx router eigrp** *номер-автономной-системы*
Переводит расширенный IGRP- протокол сети в режим установки конфигурации IPX-маршрутизатора	**network** *{номер-сети* | **all**}

В следующем примере устанавливается RIP в сетях 1 и 2 и расширенный IGRP в сети 1.

```
Router# ipx routing
!
interface ethernet 0
 ipx network 1
!
interface ethernet 1
 ipx network 2
!
ipx router eigrp 100
 network 1
```

В следующем примере устанавливается RIP в сети 2 и расширенный IGRP в сети 1:

```
Router# ipx routing
!
interface ethernet 0
 ipx network 1
!
interface ethernet 1
 ipx network 2
!
```

```
ipx router eigrp 100
 ipx network 1
!
ipx router rip
 no ipx network 1
```

Протокол уведомления о службах

NetWare-протокол уведомления о службах (NetWare SAP) позволяет сетевым ресурсам, включая файловые серверы и серверы печати, объявлять свои сетевые адреса и предоставляемые ими услуги. Каждая служба идентифицируется числом, называемым SAP-идентификатором. Обновления SAP рассылаются каждые 60 секунд.

Промежуточные сетевые устройства, такие как маршрутизаторы, анализируют SAP-обновления и создают таблицы известных служб и ассоциированных сетевых адресов. Когда клиент Novell запрашивает какую-либо сетевую службу, маршрутизатор дает ответ в виде сетевого адреса требуемой службы. После этого клиент может обратиться к службе непосредственно.

Серверы сетей NetWare могут объявлять свои службы и адреса. Все версии NetWare поддерживают широковещательные сообщения SAP для объявления и нахождения зарегистрированных сетевых служб. Добавление, поиск и удаление служб в сети происходит динамическим образом, поскольку они производятся на основе постоянно поступающих SAP-уведомлений.

Каждая SAP-служба является объектным типом, который идентифицируется некоторым номером. Ниже приведены несколько примеров.

Номер	SAP-служба
4	Файловый сервер NetWare
7	Сервер печати
24	Удаленный сервер моста (маршрутизатора)

Рабочие станции не хранят SAP-таблиц — это делают только маршрутизаторы и серверы. Все серверы и маршрутизаторы хранят полный список доступных в сети служб в своих SAP-таблицах. Аналогично RIP, протокол SAP использует механизм устаревания для идентификации и удаления элементов таблиц SAP, которые стали недействительными.

По умолчанию уведомления о службах рассылаются каждые 60 секунд. Однако, хотя в локальных сетях уведомления хорошо работают, в больших сетях или в сетях, подключенных к последовательным соединениям распределенных сетей, широковещательные службы потребовать слишком большой ширины полосы пропускания.

Маршрутизаторы не отправляют далее широковещательных сообщений SAP. Вместо этого каждый маршрутизатор строит свою собственную таблицу SAP и направляет ее другим маршрутизаторам. По умолчанию это происходит каждые 60 секунд, однако для контроля приема и отправки SAP-сообщений маршрутизатор может использовать списки управления доступом.

Программное обеспечение операционной системы Cisco также позволяет сетевому администратору отображать позиции SAP-таблицы по имени, а не по идентификатору SAP. Представляя сетевую конфигурацию в более удобном формате, эта возможность облегчает поддержание работоспособности сети и диагностику возникающих проблем.

Инженерный журнал: конфигурируемые RIP- и SAP-таймеры обновления и раз-

меры пакетов

При передаче информации о маршрутизации и предоставлении текущей информации о доступных сетевых службах клиенты и серверы NetWare полагаются на RIP- и SAP-сообщения об изменениях, которые по умолчанию поступают каждые 60 секунд. Каждую минуту таймеры RIP и SAP инициируют отправку широковещательных пакетов для того, чтобы проинформировать сеть о переменах во внутренних таблицах отдельных устройств. Однако эти пакеты обновлений могут отрицательно повлиять на эффективность работы сети, особенно в больших, постоянно меняющихся сетях с относительно медленными магистралями.

Программное обеспечение операционной системы Cisco поддерживает работу таймеров обновления протоколов RIP и SAP для отдельных интерфейсов. Установив правильную конфигурацию таймеров обновления, сетевой администратор может управлять величиной потока данных, вносимого в сеть протоколами RIP и SAP, что позволяет экономить полосу пропускания.

Программное обеспечение операционной системы Cisco позволяет также увеличить размер RIP- и SAP- пакетов (вплоть до MTU соответствующей сети). При увеличении размера этих пакетов общее количество пакетов обновлений может быть уменьшено, что увеличивает эффективность использования имеющейся полосы пропускания.

Протокол доступа к ближайшему серверу (Get Nearest Server Protocol)

Клиенты NetWare автоматически обнаруживают доступные сетевые службы, поскольку серверы и маршрутизаторы Novell объявляют эти службы, используя широковещательные сообщения SAP. Одним из видов объявлений SAP являются GNS, которые позволяют клиенту быстро найти ближайший сервер для подключения.

В NetWare взаимодействие клиент/сервер начинается в тот момент, когда клиент включает питание и запускает программу запуска. Эти программы используют сетевой адаптер клиента в локальной сети и инициируют установку соединения, которое будет использовать командная оболочка NetWare. Установка связи включает в себя отправку широковещательного сообщения, которое приходит от клиента с использованием протокола SAP. Ближайший файловый сервер NetWare отвечает другим SAP; при этом используется протокол GNS. Начиная с этого момента клиент может подключиться к нужному серверу, установить связь, обсудить размер пакета и приступить к использованию ресурсов сервера.

Если сервер NetWare расположен в этом сегменте, то он отвечает на запрос клиента. Маршрутизатор Cisco не отвечает на запрос GNS. Если в локальной сети нет сервера NetWare, то маршрутизатор Cisco отвечает адресом сервера из своей собственной таблицы SAP.

Программное обеспечение операционной системы Cisco позволяет найти клиента в сегменте локальной сети, в котором отсутствуют серверы. Когда клиент NetWare желает найти сервер NetWare, он рассылает запрос GNS. Маршрутизаторы Cisco просматривают поток данных NetWare, определяют доступные серверы и направляют запросы GNS именно на них. Посредством фильтрации GNS-пакетов можно явным образом исключить какие-либо серверы, что делает проектирование более безопасным и гибким.

В ответ на GNS-запросы программное обеспечение ОС Cisco может равномерно распределить клиентов среди доступных серверов. Например, предположим, что клиенты A и B оба отправили GNS-запросы, как показано на рис. 7.4. Маршрутизатор Cisco посылает GNS-ответы клиенту A, рекомендуя ему вступить в связь с сервером 1 и клиенту B, направляя его на сервер 2.

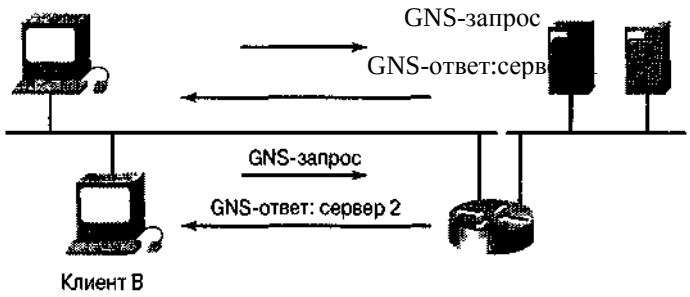


Рис. 7.4. GNS-запрос представляет собой широковещательное сообщение от клиента, которому требуется сервер

Поддерживая сегменты локальных сетей без серверов и равномерно распределяя клиентов среди доступных серверов, программное обеспечение Cisco обеспечивает распределение нагрузки, учитывающее состояние сети, увеличивает доступность приложений и сводит к минимуму необходимость конфигурировать и управлять большим количеством локальных серверов в том случае, когда эти серверы идентичны.

Цели установки конфигурации протокола Novell IPX

Установка конфигурации маршрутизатора для IPX-маршрутизации включает в себя глобальную и интерфейсную части.

Задачи установки глобальной конфигурации включают в себя следующее:

- запуск процесса маршрутизации;
- обеспечение при необходимости распределения нагрузки.
- Для установки конфигурации интерфейсов необходимо выполнить следующие действия.
- Назначить сетевой номер каждому интерфейсу. Одному интерфейсу может быть назначено несколько сетевых номеров, что позволяет поддерживать несколько типов инкапсуляции.
- Установить тип IPX-инкапсуляции, если он отличается от типа, принимаемого по умолчанию.

Решение этих вопросов установки конфигурации описано ниже.

Глобальное конфигурирование Novell IPX

Как было описано ранее, команда ipx routing активизирует процесс маршрутизации в сети Novell. Если не указан адрес узла, то маршрутизатор Cisco использует MAC-адрес интерфейса. Если маршрутизатор Cisco имеет только последовательные интерфейсы, то указание адреса является обязательным. Кроме этого, может быть задана команда ipx maximum-path, выполнение которой включает в себя процесс распределения нагрузки. Как было указано ранее, параметр этой команды представляет собой максимальное количество параллельных путей к пункту назначения. По умолчанию он равен 1, а максимальное значение равно 512.

Назначение сетевых номеров интерфейсам

При назначении сетевых IPX-номеров интерфейсам, поддерживающим несколько IPX-сетей, можно также сконфигурировать первичные и вторичные IPX-сети.

Первая логическая сеть, сконфигурированная на интерфейсе, рассматривается как *первичная (primary) сеть*. Все остальные сети рассматриваются как вторичные (secondary). Отметим еще раз, что каждая IPX-сеть на интерфейсе должна иметь свой собственный, отличный от других, тип инкапсуляции и этот тип должен соответствовать типу инкапсуляции клиентов и серверов, использующих тот же самый номер в сети. Задание номера вторичной сети является необходимым в том случае, когда в какой-либо индивидуальной сети используется дополнительный тип инкапсуляции.

Для назначения сетевых номеров интерфейсам, поддерживающим несколько IPX-сетей, как правило, используются подынтерфейсы. Подынтерфейс (subinterface) представляет собой механизм, позволяющий одному физическому интерфейсу поддерживать несколько логических интерфейсов или сетей. Таким образом, несколько логических интерфейсов или сетей могут быть связаны с одним интерфейсом оборудования. Каждый интерфейс должен иметь свой, отличный от других, тип инкапсуляции, который соответствует типу инкапсуляции клиентов и серверов, использующих этот же сетевой номер.

Вашингтонский проект: конфигурирование интерфейсов

Если интерфейс маршрутизатора должен использоваться в двух различных IPX-сетях, принимая два различных типа фреймов или обслуживая две различных IP-подсети, то необходимо установить конфигурацию этого интерфейса.

Инженерный журнал: подынтерфейсы

Использование подынтерфейсов целесообразно как *в* IP, так и в других протоколах. Возможен случай, когда один физический интерфейс маршрутизатора принадлежит двум различным подсетям. Кроме того, в сети IPX необходимо, чтобы все узлы работали с фреймами одного и того же типа. Поэтому при необходимости работать с узлами, использующими фреймы различного типа, в IP необходимо использовать подсети. Интерфейс EO может присутствовать в нескольких подсетях, а в IP он гложет использовать несколько типов фреймов. Следует, однако, помнить, что для того, чтобы одновременно использовать х типов фреймов, необходимо находиться в х подсетях.

В примере на рис. 7.5, показано глобальное конфигурирование Novell IPX и назначение сетевых номеров интерфейсам. Ниже описаны команды, используемые в этом примере:

Команда	Описание
ipx routing	Выбирает для маршрутизации протокол IPX и запускает протокол IPX RIP
ipx maximum-paths 2	Обеспечивает разделение нагрузки по параллельным путям к пункту назначения. Количество параллельных путей не может быть больше двух
interface ethernet o. 1	Указывает на первый подынтерфейс ин-

	терфейса EO
encapsulation novell-ether	Указывает, что в этом сегменте пути используется Novell-формат фрейма. В программном обеспечении Cisco ключевым словом является novell-ether; по терминологии Novell используется слово Ethernet_802.3
ipx network 9e	Сетевой номер, присвоенный подынтерфейсу EO
interface ethernet 0.2	Указывает на второй подынтерфейс интерфей са EO
ipx network 6c	Сетевой номер, присвоенный подынтерфейсу EO
encapsulation sap	Указывает, что в этом сегменте пути используется формат фрейма Ethernet 802.2. В программном обеспечении Cisco ключевым словом является sap

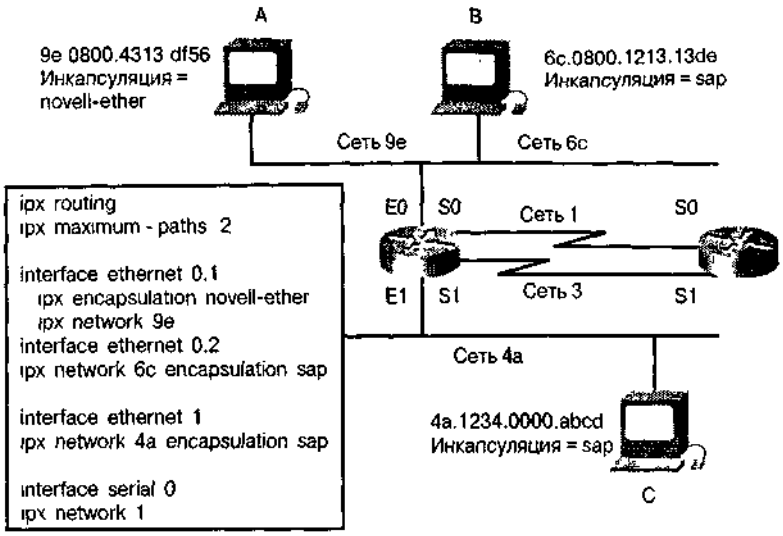


Рис. 7.5. Пример Novell IPX-конфигурации с назначением интерфейсам сетевых номеров

Тестирование IPX

После того как установка конфигурации маршрутизации закончена, можно проверить ее работу, используя команды, приведенные в табл. 7.2.

Таблица 7.2. Команды просмотра и устранения ошибок протокола IPX

Команда	Информация, выводимая на монитор

Команды мониторинга	
`show interface`	Отображает статус и параметры IPX
`show ipx route`	Отображает содержимое таблицы маршрутизации
`show ipx servers`	Отображает список серверов IPX
`show ipx traffic`	Отображает количество и типы пакетов
`Команды ликвидации ошибок`	
`debug ipx routing activity`	Отображает информацию о пакетах сообщений об изменениях в RIP-маршрутизации
`debug ipx sap`	Отображает информацию о пакетах сообщений об изменениях в SAP-маршрутизации
`ping`	Информация о конкретном узле, который способен отвечать на сетевые запросы

Мониторинг и управление IPX-сетью

Операционная система Cisco IOS включает в себя разнообразные средства конфигурирования, мониторинга и управления сетью. Эти средства облегчают установку NetWare-сетей и могут оказаться существенными при возникновении непредвиденных ситуаций.

Инженерный журнал: простой протокол управления сетью [1] (Simple Network Management Protocol)

Программное обеспечение Cisco IOS поддерживает информационную базу управления NetWare (NetWare Management Information Base), в которой имеется простой протокол управления сетью (Simple Network Management Protocol), позволяющий сетевому администратору выполнить следующие действия.

- Вручную удалить соседний маршрутизатор и все его маршруты из таблицы маршрутизации.
- Отобразить все связанные с IPX установки интерфейса, включая IPX-адрес интерфейса, состояние сетевого оборудования, включенную или выключенную обработку IPX-протокола, а также величину задержки для каждого пункта назначения.
- Отобразить имя ближайшего соседнего маршрутизатора и таблицы маршрутизации.
- Отобразить статистическую информацию о потоках данных протокола IPX, в частности:
  - общее число полученных IPX-пакетов;
  - количество пакетов с ошибками и типы ошибок;
  - общее число широковещательных пакетов, полученных, отправленных и перенаправленных от других источников;

- количество полученных и отправленных пакетов, являющихся ответами на запросы.

- Проверить выполнение важных операций протокола IPX, включая RIP, SAP, ответы на запросы и операции по маршрутизации.

Мониторинг состояния IPX-интерфейса

Команда show ipx interface отображает состояние IPX-интерфейса и IPX-параметры, установленные в конфигурации каждого интерфейса (листинг 7.1).

Листинг 7.1. Пример вывода информации по команде show ipx interface

```
Router# show ipx interface ethernet 0
EthernetO is up, line protocol is up
   IPX address is 3010.aaOO.0400.0284 NOVELL_ETHER [up] line-up RIPPQ:
0,SAPPQ: 0
   Delay of this Novel Network, in ticks, is 1
   IPXWAN processing not enabled on this interface
   IPX SAP update interval is 1 minute(s)
   IPX type 20 propagation packet forwarding is disabled
   Outgoing access list is not set -.- IPX Helper access list is not set
   SAP Input filter list is not set
   SAP Output filter list is not set
   SAP Router filter list is not set
   SAP GNS output filter list is not set I Input filter list is not set I Output
   filter list is not set I Router filter list is not set
   Netbios Input host access list is not set
   Netbios Input bytes access list is not set
   Netbios Output host access list is not set
   Netbios Output bytes access list is not set
   Update time is 60 seconds
   IPX accounting is disabled
   IPX fast switching is configured (enabled)
   IPX SSE switching is disabled
   RIP packets received 1, RIP packets sent 10006
   SAP packets received 1, SAP packets sent 6
```

Конфигурирование задержки на интерфейсе можно выполнить вручную, задав тактовую метрику. Для этого используется команда **ipx delay** *число*, в которой параметр *число* обозначает количество тактов для данного интерфейса. Эта команда отменяет установленные по умолчанию значения на маршрутизаторе Cisco:

- 1 такт — для интерфейсов локальных сетей;
- 6 тактов — для интерфейсов распределенных сетей.

Мониторинг таблиц маршрутизации протокола IPX

Команда show ipx route отображает содержимое таблицы маршрутизации протокола IPX.

В листинге 7.2 первая выделенная строка отображает информацию о маршрутизации в удаленной сети.

- Информация была получена из сообщения об обновлении.
- Номер сети 3030.
- Сеть расположена на расстоянии шести тактов или одного перехода. Информация используется для определения наилучшего пути. Если такты сливаются, то их разделения используются переходы.

- Следующим переходом является маршрутизатор 3021.0000. OcO3. 13d3.
- Информация была обновлена 23 секунды назад.
- Достичь маршрутизатора следующего перехода можно через последовательный интерфейс Serial 0 (для распределения нагрузки).
- Вторая выделенная строка содержит информацию о непосредственном соединении.
- Сетевой номер ЗОЮ.
- Тип инкапсуляции Novell-ETHER.

Листинг 7.2. Пример вывода по команде show ipx route

```
Router# show ipx route
Codes: C - Connected primary , c - connected secondary network,
   R - RIP, E - EIGRP, S - Static, W - IPXWAN connected
5 total IPX routes

Up to 2 parallel paths allowed, Novell routing protocol variant to use

R Net 3030 [6/1] via 3021.0000.Oc03.13d3, 23 sec, Seriall
   via 3020.0000.Oc03.13d3, 23 sec, SerialO
C Net 3020 (X25), SerialO
C Net 3021 (HDLC), Seriall
C Net 3010 (Novell-ETHER), EthernetO
C Net 3000 (Novell-ETHER), Ethernetl
```

В приведенной ниже таблице описаны поля, показанные в листинге 7.2.

Поле	Описание
Codes	Коды, показывающие как был найден маршрут: c — непосредственно подсоединенная первичная сеть; c — непосредственно подсоединенная вторичная сеть; R — маршрут получен из сообщения об изменении протокола RIP; E — маршрут получен из сообщения об изменении расширенного протокола RIP s — статически заданный маршрут, определенный командой ipx route; w — непосредственно подсоединенный маршрут, определенный посредством IPXWAN
5 Total IPX routes	Количество маршрутов в таблице маршрутизации IPX
Parallel paths allowed	Максимальное количество параллельных путей, на которое маршрутизатор был сконфигурирован командой ipx maximum-paths
Novell routing protocol variant in use	Указывает, использует ли маршрутизатор IPX-совместимый протокол маршрутизации (по умолчанию)
Net 1	Сеть, к которой ведет маршрутизатор

[6/1]	*Задержка/Метрика* Параметр Delay представляет количество тактов, сообщаемое сети-получателю. Параметр *метрика* обозначает число переходов, сообщаемое той же самой сети. Параметр *Задержка* используется в качестве первичной метрики, а параметр *метрика* (количество переходов) используется для разрыва связей
via *сеть.узел*	Адрес маршрутизатора, который является следующим переходом к удаленной сети
Age	Время (часы, минуты и секунды), истекшее со времени получения информации о данной сети
uses	Показывает, сколько раз происходил поиск данной сети в таблице маршрутизации Это поле увеличивается на единицу при коммутации пакета, даже если в конечном итоге пакет был отфильтрован и не был отправлен Поэтому величина в данном поле дает точную оценку количества раз использования данного маршрута
EthernetO	Интерфейс, через который пакеты будут отправлены в удаленную сеть
(NOVELL-ETHER) (HDLC) (SAP/SNAP)	Тип инкапсуляции (фрейма). Отображается только для непосредственно подсоединенных сетей

Мониторинг серверов в IPX Novell

Команда **show ipx servers** вызывает вывод списка серверов, обнаруженных посредством SAP-объявлений. При выводе по этой команде отображается следующая информация.

- Служба, обнаружившая сервер по SAP-сообщению об изменении.
- Имя сервера, его расположение в сети, адрес устройства и номер гнезда источника.
- Количество тактов и переходов для данного маршрута (берутся из таблицы маршрутизации).
- Количество переходов (берется из SAP-протокола).
- Интерфейс, через который можно получить доступ к серверу.

Для вывода списка серверов, обнаруженных посредством SAP-объявлений, следует (спользовать команду **show ipx servers** в пользовательском EXEC-режиме. Полный синтаксис команды имеет вид:

show ipx servers [sorted [name | net | type]]

Ниже описаны ключевые слова, использованные в команде.

Ключевое слово	Описание
sorted	(Необязательное) Сортирует выводимый список серверов согласно следующему за этим слову

name	(Необязательное) Отображает список серверов по их именам в алфавитном порядке
net	(Необязательное) Сортирует выводимый список серверов по номеру сети
type	(Необязательное) Сортирует выводимый список серверов по типу (номеру) SAP-услуги

В листинге 7.3 показан вывод по команде show ipx servers. Листинг 7.3. Вывод по команде show ipx servers

```
Route r > show ipx servers
Codes: P - Periodic, I - Incremental, H - holddown, S - Static
1 Total IPX Servers
Table ordering is based on routing and server info
Type Name    Net Address       Port  Route Hops Itf
P    4 MAXINE AD333000.0000.Ib04.0288:0451  32800/1    2 Et3
```

Ниже описаны поля, использованные в листинге 7.3.

Поле	Описание
Codes	Коды, показывающие как был найден сервер' p — информация о сервере была получена посредством обычных периодических сообщений о SAP-изменениях *i* — информация о сервере была получена с использованием возможности ступенчатого возрастания SAP (incremental SAP) в расширенном IGRP-протоколе н — предполагается, что сервер перестал функционировать и маршрутизатор не может больше предлагать его услуги s — Сервер определен статически посредством команды ipx sap
Total IPX Servers and server info	Количество серверов в списке
Table ordering is based on routing and server info	Перечисленные элементы взяты из маршрутной информации, ассоциированной с этим SAP. Информация о сервере используется для разрыва соединения
Type	Номер SAP-услуги
Name	Имя сервера
Net	Сетевой номер сервера

Address	Узловой адрес сервера
Port	Номер гнезда
Route	Значение метрики (числа переходов) для формирования маршрута в сети
Hops	Сообщаемое SAP число переходов от маршрутизатора к сети сервера
Itf	Интерфейс, через который был в первый раз обнаружен данный сервер

Мониторинг потоков данных в протоколе IPX

Команда show ipx traffic используется для получения информации о числе и типе IPX-пакетов, полученных и переданных маршрутизатором.

В листинге 7.4 большую часть полученных и отправленных пакетов составляют RIP-объявления. Это объясняется тем, что пример был взят из лабораторной сети, в которой практически нет пользовательских потоков данных. Из листинга видно, что протокол IPX генерирует много служебной информации.

(Листинг 7.4. Вывод по команде show ipx traffic

```
Routert# show ipx traffic
Rcvd:   32124925 total, 1691992 format errors, 0 checksum errors, 67
bad hop count,
         18563 packets pitched, 452467 local destination, 0 multicast
Bcast:  452397 received, 1237193 sent Sent:   2164776 generated, 31655567 forwarded
         0 encapsulation failed, 2053 no route
SAP:    3684 SAP requested, 10382 SAP replies
         259288 SAP advertisements received, 942564 sent
         0 SAP SAP flash updates sent, 0 SAP poison sent
         0 SAP format errors
RIP:    0 RIP format errors
Echo:   Rcvd 0 requests, 0 replies
         Sent 0 requests, 0 replies
         4252 unknown, 0 SAPs throttled, freed NDB len 0
Watchdog:
         0 packets received, 0 replies spoofed
Queue lengths:
         IPX input: 1, SAP 0, RIP 0, GNS 0
         Total length for SAP throttling purposes: 1/(no preset limit)
IGRP:   Total received 0, sent 0
         Updates received 0, sent 0
         Queries received 0, sent 0
         Replies received 0, sent 0
         SAPs received 0, sent 0
```

Ниже описаны поля, показанные в листинге 7.4.

Поле	Описание
Rcvd:	Описание пакетов, полученных маршрутизатором
32124925 total	Общее число пакетов, полученных маршрутизатором

Поле	Описание
1691992 format errors	Количество поврежденных и отброшенных пакетов (например, пакетов, использующих тип фрейма, не поддерживаемый маршрутизатором)
O checksum errors	Количество пакетов, содержащих ошибочную контрольную сумму
67 bad hops count	Количество пакетов, отброшенных потому, что их число переходов превышает 16 (т е. просроченных)
18563 packets pitched	Количество раз, когда маршрутизатор отбрасывал пакеты Это может происходить в следующих случаях • Когда распространение типа 20 или широковещание всех сетей не соответствует команде **ipx type-20-input-checks** • Когда обработка пакета по распространению типа 20 обнаруживает петлю, избыточное количество переходов или сама обработка выполнена неправильно • Когда RIP- или SAP-пакеты поступают в несоответствующую сеть • Когда маршрутизатор получает собственное широковещательное сообщение • Когда маршрутизатор получает локальные пакеты из неправильной сети-источника.
452467 local destination	Количество пакетов, отправленных по адресам локального широковещания или конкретно на данный маршрутизатор
O multicast	Количество полученных пакетов, которые были адресованы в несколько пунктов назначения
Bcast	Описание широковещательных пакетов, полученных и отправленных маршрутизатором
452397 received	Количество полученных широковещательных пакетов
1237193 sent	Количество отправленных широковещательных пакетов. Оно включает в себя как полученные, так и самостоятельно сгенерированные широковещательные пакеты.
Sent:	Количество отправленных пакетов Оно включает в себя как самостоятельно сгенерированные пакеты, так и полученные, а затем отправленные к другим местам назначения
2164776 generated	Количество пакетов, сгенерированных маршрутизатором и отправленных к месту назначения

Поле	Описание
31655567 forwarded	Количество пакетов, полученных от других источников и направленных далее
0 encapsulation failed	Количество пакетов, которые маршрутизатор не смог инкапсулировать
2053 no route	Количество раз, когда маршрутизатор не смог найти в своей таблице маршрута к месту назначения
SAP:	Описание SAP-пакетов, которые маршрутизатор отправил и получил
3684 SAP requests	Количество SAP-запросов, полученных маршрутизатором
10382 SAP replies	Количество ответов на SAP-запросы, отправленных маршрутизатором
259288 SAP advertisements received	Количество SAP-объявлений, полученных маршрутизатором от другого маршрутизатора
942564 sent	Количество SAP-объявлений, сгенерированных и затем отправленных маршрутизатором
0 SAP flash updates sent	Количество SAP-объявлений, сгенерированных и затем отправленных маршрутизатором в результате изменений в его собственной таблице маршрутизации
0 SAP poison sent	Количество случаев, когда маршрутизатор создал и передал сообщение об изменении, в котором информирует о недоступности какой-то услуги
○ SAP format errors	Количество некорректно отформатированных SAP-объявлений
RIP:	Количество RIP-пакетов, полученных и отправленных маршрутизатором
0 RIP format errors	Количество некорректно отформатированных RIP-пакетов
Echo:	Описание запросов и ответов команды ping, которые маршрутизатор отправил и получил
Rcvd 0 request, 0 replies	Количество запросов и ответов команды ping, полученных маршрутизатором
Sent 0 requests, 0 replies	Количество запросов и ответов команды ping, отправленных маршрутизатором
4252 unknown	Количество нераспознанных пакетов, отправленных на маршрутизатор
0 SAP throttled	Количество SAP-пакетов, отброшенных, поскольку они превосходили размер буфера

Поле	Описание
`Freed NDB len 0`	Количество блоков сетевого дескриптора (Network descriptor block, NDB), которые были удалены из сети, но требуют удаления из таблицы маршрутизации
`Watchdog:`	Описание пакетов контроля, обработанных маршрутизатором
`0 packets received`	Количество управляющих пакетов, полученных маршрутизатором от IPX-серверов локальной сети
`0 replies spoofed`	Количество случаев, когда маршрутизатор ответил на watchdog-пакет от имени удаленного клиента
`Queue lengths`	Описание выходных пакетов, которые находятся в буферах и ожидают обработки
`IPX input`	Количество входных пакетов, ожидающих обработки
`SAP`	Количество входных SAP-пакетов, ожидающих обработки
`RIP`	Количество входных RIP-пакетов, ожидающих обработки
`GNS`	Количество входных GNS-пакетов, ожидающих обработки
`Total length for SAP throttling purposes`	Максимально допустимое количество входных RIP- и SAP-пакетов в буфере. Все SAP-пакеты с номерами, превышающими это число, отбрасываются
`Unknown counter`	Количество пакетов, которые маршрутизатор не смог отправить далее, например, по причине отсутствия маршрута к месту назначения

Устранение ошибок при осуществлении маршрутизации в IPX

Программное обеспечение IOS Cisco включает в себя команды **debug** и ping, позволяющие сетевому администратору проанализировать практически все аспекты передачи информации в сети. Команда debug представляет собой важный инструмент наблюдения, управления и устранения ошибок в сетях Novell.

Команда debug ipx routing activity отображает информацию о пакетах обновления IPX-маршрутизации, которые передаются или принимаются в сети.

Маршрутизатор рассылает сообщения об обновлениях каждые 60 секунд. Каждый пакет обновления может содержать до 50 позиций. Если таблица маршрутизации содержит более чем 50 позиций, то обновление состоит более чем из одного пакета.

В листинге 7.5 маршрутизатор отправляет сообщения об изменениях в маршрутизации, но не получает их. Однако сообщения об изменениях, полученные от других маршрутизаторов, также приводятся в листинге.

Листинг 7.5 Пример вывода по команде debug ipx routing activity

```
Router# debug ipx routing activity
IPX routing debugging is on
Router#
IPXRIP: positing full update to 3010.ffff.ffff. ffff via EthernetO
```

```
   (broadcast)
   IPXRIP: positing full update to 3000.ffff.ffff.ffff via Ethernetl
   (broadcast)
   IPXRIP: positing full update to 3020.ffff.ffff.ffff via SerialO
   (broadcast)
   IPXRIP: positing full update to 3021.ffff.ffff.ffff via Seriall
   (broadcast)
   IPXRIP: sending update to 3020.ffff.ffff.ffff via SerialO (broadcast)
   IPXRIP: arc=3020.0000.0c03.14d8m dst=3020.ffff.ffff.ffff, packet sent
      network 3021, hops 1 , delay 6
      network 3010, hops 1 , delay 6
      network 3000, hops 1 , delay 6
   IPXRIP: sending update to 3021.ffff.ffff.ffff via Seriall (broadcast)
   IPXRIP: arc=3021.0000.0c03.14d8m dst=3021.ffff.ffff.ffff, packet sent
      network 3020, hops 1 , delay 6
      network 3010, hops 1 , delay 6
      network 3000, hops 1 , delay 6
   IPXRIP: sending update to 3010.ffff.ffff.ffff via EthernetO
   IPXRIP: arc=3010.aaOO.0400.0284, dst=3010.ffff.ffff.ffff, packet sent
      network 3030, hops 2 , delay 7
      network 3020, hops 1 , delay 1
      network 3021, hops 1 , delay 1
      network 3000, hops 1 , delay 1
IPXRIP: sending update to 3000.ffff.ffff.ffff via Ethernetl
```

Устранение ошибок в SAP IPX

Команда **`debug ipx sap`** отображает информацию об IPX SAP-пакетах, которые передаются или принимаются.

Сообщения об обновлениях протокола SAP также рассылаются каждые 60 секунд, но, в отличие от аналогичных сообщений протокола RIP, могут содержать более одного пакета. Как показано в листинге 7.6, каждый SAP-пакет при выводе представляется несколькими строками, включающими в себя сообщение с общим описанием пакета и сообщение с подробным описанием службы.

Листинг 7.6. Пример вывода по команде debug sap

```
   Router# debug ipx sap
   IPX SAP debugging is on
   Router#
   NovellSAP: at 0023F778
   I SAP Response type 0x2 len 160 arc:160.0000.OcOO.070d
   dest: 160.ffff.ffff.ffff(452)
   Type 0x4, "HELL02", 199.0002.0004.0006(451), 2 hops
   Type 0x4, "HELL01", 199.0002.0004.0008(451), 2 hops
   Novell SAP: sending update to 160
   NovellSAP: at 169080
   0 SAP Update type 0x2 len 96 ssoc; 0x452 dest: 160.ffff.ffff.ffff(452)
   Novell: type 0x4 "Magnolia", 42.0000.0000.0000(451), 2 hops
```

Ответом SAP на запрос могут быть:

- Oxl — общий запрос;
- 0x2 — общий ответ;
- 0x3 — GNS-запрос;
- 0x4 — GNS-ответ.

В примере вывода в каждой строке SAP-ответа указаны адрес и расстояние до отвечающего или запрашиваемого маршрутизатора.

IPX-версия команды ping

Для устранения возникающих в сети ошибок программное обеспечение IOS Cisco включает в себя IPX-версию команды ping. Эта команда позволяет сетевому администратору убедиться в том, что конкретный узел способен отвечать на сетевые запросы. Она также позволяет определить, существует ли физический путь через станцию, которая вызвала проблему в сети. Команда ping в Novell является стандартной и может быть использована клиентами Novell, серверами и сетевыми устройствами.

Привилегированная команда ping протокола IPX

Для проверки достижимости хоста и правильности установки сетевых соединений рекомендуется использовать команду ping в привилегированном командном режиме (EXEC). Полный синтаксис команды имеет вид:

ping [**ipx**] [сеть.узел]

Ниже описаны параметры, используемые в команде.

Параметр	Описание
ipx	(Необязательный) Указывает на использование протокола IPX
сеть. узел	(Необязательный) Адрес системы, используемый командой ping

Привилегированная команда ping предоставляет полный набор возможностей этой команды пользователям, которые имеют системные привилегии. Она работает только на маршрутизаторах Cisco, использующих версию IOS 8.2 или более позднюю. Устройства Novell IPX не реагируют на эту команду.

Команда ping не может быть выполнена с самого маршрутизатора. Для прекращения сеанса работы команды ping используется последовательность выхода. По умолчанию это сочетание клавиш <Ctrl+Shift+6+X>. Для выполнения этого действия следует одновременно нажать клавиши <Ctrl>, <Shift> и <6>, и, не отпуская их, нажать клавишу <X>.

В табл. 7.3 описаны символы, отображаемые на экране в ответ на команду ping.

Таблица 7.3. Символы, используемые для указания типа тестирования, выполняемого командой ping

Символ типа тестирования	Значение
!	Каждый восклицательный знак указывает на получение ответа от заданного адреса
.	Каждая точка свидетельствует о том, что сервер просрочил время, ожидая ответа от заданного адреса
U	Был получен модуль данных протокола (PDU) "пункт назначения недостижим"
C	Получен пакет, попавший в сетевой затор

I	Пользователь прервал тест
?	Неизвестный тип пакета
&	Превышено время, в течение которого пакет считается действительным

Текст в листинге 7.7 иллюстрирует ввод привилегированной команды ping и соответствующий вывод на экран.

Листинг 7.7. Вывод по привилегированной команде ping

```
Router# ping
Protocol [ip]: ipx
Target Novell Address: 211.0000.OcOl.f4cf
Repeat Count [5]:
Datagram Size [100]:
Timeout in seconds [2] :
Verbose [n]:
Type escape sequence to abort.
Sending 5 100-byte Novell echoes to 211.0000.OcOl.f4cf, timeout is 2
seconds.
!!!!!
Success rate is 100%, round trip min/avg/max = 1/2/4 ms.
```

Непривилегированная команда ping протокола IPX

Для проверки достижимости хоста и правильности сетевых соединений рекомендуется использовать команду ping в привилегированном командном режиме (EXEC). В отличие от привилегированной команды ping, команда ping уровня обычного пользователя предоставляет основные возможности пользователю, не имеющему системного приоритета. Эта команда эквивалентна упрощенной форме привилегированной команды ping. Она рассылает пять 100-байтовых пакетов. Полный синтаксис команды:

ping [**ipx**] *{узел \ адрес}*

Ниже дано описание параметров команды:

Параметр	Описание
ipx	(Необязательный) Указывает на использование протокола IPX
узел	Имя хоста в системе, используемое в команде ping
адрес	Адрес системы, используемый в команде ping

Команда ping пользовательского уровня работает только на маршрутизаторах Cisco, работающих с версией операционной системы 8.2 или более поздней. Устройства Novell IPX не отвечают на эту команду.

Команду ping нельзя выполнить непосредственно на маршрутизаторе. Если система не может найти адрес по имени хоста, то она возвращает сообщение об ошибке: %Unrecognized host or address.

В листинге 7.8 показан вывод по команде ping уровня пользователя.

Листинг 7.8. Вывод команды ping уровня пользователя

```
Router> ping ipx 211.0000.OcOl.f4of
```

```
Type escape sequence to abort.
Sending 5, 100-byte Novell Echoes to 211.0000.OcOl.f4cf,
            timeout is 2 seconds.
. . .
Success rate is 0 percent (0/5)
```

Резюме

- Novell IPX представляет собой набор протоколов, включающий в себя:
- протокол передачи дейтаграмм, не устанавливающий соединения, и не требующий подтверждения получения каждого пакета;
- протокол 3-го уровня, определяющий сетевой адрес и межузловой адрес.
- В Novell NetWare используется протокол R1P для обмена информацией о маршрутизации и протокол SAP для уведомления о сетевых службах. NetWare использует протокол NCP для установки соединений и использования приложений типа клиент/сервер, а также протокол SPX для ориентированных на соединение служб 4-го уровня.
- IPX является протоколом 3-го уровня NetWare и выполняет передачу дейтаграмм без установки соединения, аналогично протоколу IP в сетях IP/TCP.
- По умолчанию типами инкапсуляции на интерфейсах маршрутизаторов Cisco являются Ethernet (novel 1-ether), Token Ring (sap) и FDDI (snap).
- Novell RIP представляет собой дистанционно-векторный протокол маршрутизации, использующий для принятия решений о маршрутах две метрики: такты задержки и количество переходов.
- Протокол SAP в NetWare позволяет сетевым ресурсам объявлять свои сетевые адреса и предоставляемые ими службы.
- Протокол GNS позволяет клиенту найти ближайший сервер для входа в систему.
- Конфигурирование маршрутизатора в протоколе IPX включает в себя как глобальную, так и интерфейсную части.

Задачи проекта Вашингтонского учебного округа: конфигурирование протокола Novell IPX

В настоящей главе были описаны понятия и процесс конфигурирования, помогающие реализовать протокол IPX в сети Вашингтонского учебного округа. Составной частью конфигурирования и реализации IPX является решение следующих задач.

1. Оформление документации по изменениям в проекте сети в соответствии требованиями пользователей к протоколу IPX.
2. Оформление документации по изменениям в конфигурации маршрутизатора в соответствии с требованиями пользователей.
3. Составление списка команд маршрутизатора, необходимых для реализации IPX в сети.

Контрольные вопросы

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

1. Что используется в качестве сетевого адреса в IPX-сети?
2. Какую команду следует использовать для установки максимального числа равноценных путей при отправке пакетов маршрутизатором?
3. В каком командном режиме должен находиться маршрутизатор перед выполнением команды ipx routing?
4. С помощью какой команды можно проверить правильность назначения маршрутизатору IPX-адреса?
5. Какая команда отображает информацию о SAP-пакетах, получаемых или отправляемых протоколом IPX?
6. Novell IPX-адрес состоит из 80 битов: 32 для и 48 для
   A. Сетевого номера; IP-адреса.
   B. Номера узла; MAC-адреса.
   C. Номер сети; номер узла.
   D. MAC-адреса; номера узла.
7. В процессе конфигурирования IPX-сети иногда необходимо указать тип инкапсуляции _____.
   A. Только на Novell-серверах.
   B. Только на Cisco маршрутизаторах.
   C. Иногда на A и B.
   D. Всегда на A и B.
8. Novell NetWare использует протокол_____для облегчения обмена информацией о маршрутизации и протокол_____для объявления о сетевых службах
   A. NCP; RIP.
   B. RIP; SAP.
   C. SPX; NCP.
   D. SAP; RIP.
9. Какая из приведенных ниже команд используется для глобального конфигурирования Novell IPX?
   A. **ipx routing** [узел]
   B. **router ipx**
   C. **ipx route** [узел]
   D. **router rip**
10. Какими командами следует заполнить пропуски в утверждениях:

- _____отображает статус и параметры IPX;
- _____отображает содержимое таблицы маршрутизации IPX;
- _____отображает список серверов обнаруженных с помощью SAP-объявлений.

A. **show ipx traffic; show ipx route; show ipx routing activity.**
B. **show ipx interface; show ipx route; show ipx servers.**
C. **show ipx interface; show ipx; show ipx servers.**
D. **show ipx; show ipx route; show ipx.**

Основные термины

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

MAC-адрес, адрес управления доступом к передающей среде (Media Access Control address, MAC address). Стандартизованный адрес данных канального уровня, который требуется любому порту или устройству, подсоединенному к локальной сети. Другие устройства сети используют эти адреса для нахождения конкретных портов в сети, создания и обновления таблиц маршрутизации и структур данных. MAC-адреса имеют длину 6 байтов и контролируются IEEE. Их также называют адресами устройств адресами MAC-уровня или физическими адресами.

Запрос ближайшего сервера (Get Nearest Server, GNS). Пакет запроса, посланный клиентом по IPX-сети с целью нахождения ближайшего активного сервера требуемого типа. Клиент сети IPX делает GNS-запрос для получения непосредственного ответа от подсоединенного сервера или ответа от маршрутизатора, который сообщает, в каком месте сети можно получить требуемую услугу. GNS является частью IPX SAP.

Инкапсуляция (encapsulate). Процесс присоединения к данным заголовка конкретного протокола. Например, к данным Ethernet перед передачей присоединяется заголовок Ethernet. При использовании моста для сетей различного типа весь фрейм одной сети просто помещается в заголовок, используемый протоколом канального уровня другой сети.

Клиент (client). Узел или набор программного обеспечения (от начального до оконечного устройства), обращающийся за услугами к серверу.

Клиент/сервер (client/server). Архитектура соединения в сети рабочей станции и сервера.

Метрика маршрутизации (routing metric). Метод, используемый маршрутизатором для определения лучшего из нескольких маршрутов. Эта информация хранится в таблицах маршрутизации. Метрики могут использовать такие параметры, как ширина полосы пропускания, стоимость связи, величина задержки, количество переходов, нагрузка, MTU, стоимость пути и надежность. Часто называется просто метрикой.

Операционная система NetWare (NetWare). Широко распространенная операционная система, разработанная корпорацией Novell. Обеспечивает прозрачный доступ к удаленным файлам и многие другие сетевые услуги.

Подынтерфейс или вспомогательный интерфейс (subinterface). Один из нескольких виртуальных интерфейсов одного физического интерфейса.

Протокол NetWare служб канального уровня (NetWare Link Services Protocol, NCLP). Протокол маршрутизации канального уровня, базирующийся на IS-IS. Реализация NLSP в маршрутизаторах Cisco также включает в себя MIB-переменные, средства перераспределения маршрутизации и SAP-информации между NSLP и другими IPX-протоколами маршрутизации.

Протокол межсетевого обмена пакетами (Internetwork Packet Exchange, IPX). Протокол сетевого уровня NetWare, используемый для передачи данных от серверов к рабочим станциям. Протокол IPX аналогичен протоколам IP и XNS.

Протокол объявления служб (Service Advertising Protocol, SAP). IPX-протокол, предоставляющий средства оповещения клиентов через серверы и маршрутизаторы о доступных сетевых ресурсах и услугах.

Протокол последовательного обмена пакетами (Sequenced Packet Exchange, SPX). Надежный, ориентированный на установление соединения протокол, дополняющий Услуги по обработке дейтаграмм, предоставляемые протоколами сетевого уровня. Корпорация Novell разработала этот широко используемый транспортный протокол на основе протокола SPP из набора протоколов XNS.

Распределение нагрузки Qoad sharing). Использование двух или более путей для отправки пакетов к одному и тому же пункту назначения; при этом, за счет равномерного распределения нагрузки балансируется работа сети и повышается ее эффективность.

Расширенный протокол маршрутизации внутреннего шлюза (Enhanced Interior Gateway Routing Protocol, Enhanced IGRP). Расширенная версия протокола IGRP, разработанная корпорацией Cisco. Обеспечивает высокую степень конвергенции и операционной эффективности, объединяя преимущества протоколов канального уровня и дистанционно-векторных протоколов.

Сервер (server). Узел или программа, предоставляющие услуги клиентам.

Сетевая операционная система (Network Operating System, NOS). Операционная система, используемая для обеспечения работы сетей, таких, например, как Novell NetWare или Windows

NT.

Точка доступа к службе (service access point). Поле, определенное спецификацией IEEE, являющееся частью адресной спецификации.

Фрейм (frame). Логически сгруппированная информация, пересылаемая в качестве блока канального уровня по передающей среде.

Шестнадцатеричный (по основанию 16) (hexadecimal (base 16)). Числовое представление, использующее цифры от 1 до 9 в обычном значении и буквы от A до F для представления десятичных чисел от 10 до 15. В шестнадцатеричном представлении самая правая цифра обозначает единицы, следующая — числа, кратные 16, следующая — кратные 16^2=256 и т.д.

Ключевые темы этой швы

- Описываются цели использования и функции распределенных сетей
- Описываются различные устройства распределенных сетей
- Рассматривается работа распределенных сетей
- Описываются форматы инкапсуляции в распределенных сетях
- Описываются типы каналов в распределенных сетях

Глава 8

Распределенные сети

Введение

В вастоящей главе описываются, различные протоколы и технологии, используемые в **распределенных сетях (wide-area network,** WAN) В ней рассмотрены основные концепции, относящиеся к распределенным сетям, типы служб, форматы инкапсуляции и типы каналов. Описаны также каналы "точка-точка", коммутация цепей (каналов), коммутация пакетов, виртуальные сети, службы вызова и устройства распределенных сетей,

---

Вашингтонский проект: реализация распределенных сетей

Для передачи данных распределенная сеть Вашингтонского учебного округа должна соединять все школы и административные офисы с окружным офисом Информация, изложенная в настоящей главе, помогает понять принципы функционирования этой сети и спроектировать ее. По мере описания новых понятий станет возможной их реализация в проекте распределенной сети.

Обзор технологии распределенных сетей

Распределенная сеть представляет собой сеть передачи данных, сфера действия которой простирается за пределы локальной сети Одним из отличий распределенной от локальной является то, что для использования распределенной сети требуется заключить договор с внешним провайдером, таким, например, как **региональное отделение компании Bell (regional operating company Bell, RBOC)** Это позволяет в распределенной сети воспользоваться **услугами сетевых провайдеров (carrier network services)** В распределенной сети используются каналы данных, такие как интегрированные службы цифровых сетей (Integrated Services Digital Network, ISDN) и ретрансляция фреймов (Frame Relay), предоставляемые сетевыми провайдерами, для получения доступа к '"выделенной полосе пропускания в пределах области действия распределенной сети Распределенная сеть соединяет друг с другом отдельные офисы одной организации,офисы компании с другими организациями, с внешними службами (такими как базы данных) и с удаленными пользователями. Распределенные сети обычно передают данные различных типов, такие как звук, цифровые данные и видео.

Технологии распределенных сетей функционируют на трех нижних уровнях эталонной модели OSI — на физическом, канальном и сетевом. На рис. 8.1 показаны связи между технологиями распределенных сетей и эталонной моделью OSI.

Службы распределенных сетей

Чаше всего используются такие службы распределенных сетей, как телефонная связь и передача данных. Эти службы функционируют на участке между **точкой присутствия (point of presence, POP) и телефонной станцией (central office)** провайдера. Телефонная станция представляет собой офис местной телефонной компании, к которому подсоединены все локальные ответвления данного региона и в котором происходит коммутация линий абонентов.

Рис. 8.1. Технологии распределенных сетей функционируют на трех нижних уровнях эталонной модели OS1

Обзор среды распределенной сети (рис. 8.2) позволяет подразделить службы пр вайдера на три основных группы.

- **Вызов (call setup).** Эта служба устанавливает и прекращает связь между пользователями телефонов. Называемая также сигнализацией, служба установки вызова использует отдельный телефонный канал, который не используется для других целей. Для установки вызова чаще всего используется **система сигнализации** 7 **(Signaling System** 7, SS7), которая передает и принимает телефонные управляющие сообщения и сигналы на пути от точки передачи к пункту назначения.
- **Временное мультиплексирование (Time-division multiplexing, TDM).** Для передачи информации от многих источников используется полоса пропускания фиксированной ширины в одной и той же передающей среде. Метод коммутации каналов использует сигнализацию для определения маршрута вызова, который представляет собой выделенный путь между отправителем и получателем. Осуществляя мультиплексирование потоков данных в фиксированные временные промежутки, TDM позволяет избежать перегрузки устройств и изменения значений задержки. Каналы TDM используются базовой телефонной службой и ISDN.
- **Протокол Frame Relay.** Информация, содержащаяся во фреймах, передается по определенной полосе пропускания совместно с информацией от других подписчиков. Frame Relay является статистической мультиплексной службой, в отличие от TDM, которая использует идентификаторы 2-го уровня и постоянные виртуальные каналы. Кроме того, коммутация пакетов протоколом Frame Relay использует маршрутизацию 3-го уровня, при которой адреса отправителя и адресата содержатся в самом пакете.

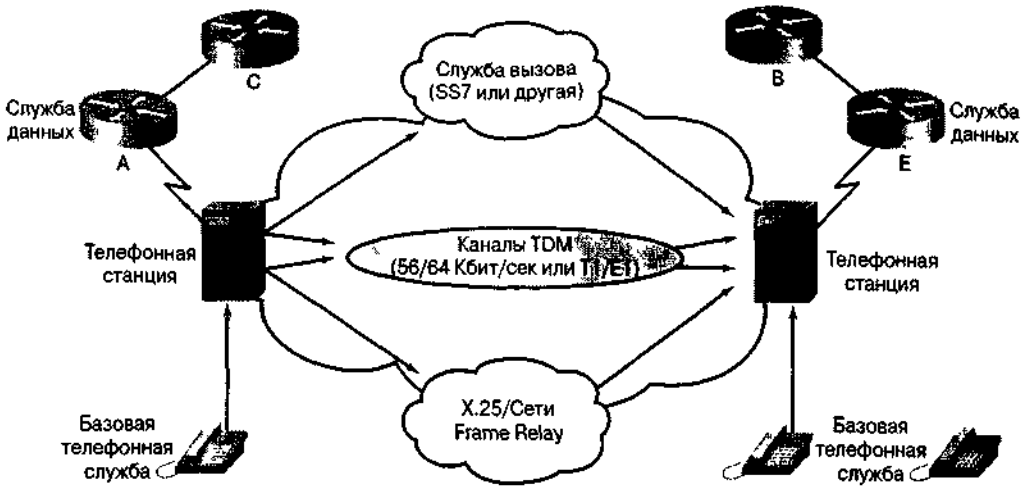


Рис. 8.2. В распределенных сетях имеется три типа провайдеров услуг

Провайдеры услуг распределенных сетей

Технологический прогресс последнего десятилетия сделал доступными для сетевых проектировщиков ряд новых решений. При выборе оптимального варианта распределенной сети необходимо оценить преимущества и стоимость услуг различных провайдеров.

При заключении договора организацией на использование ресурсов внешнего провайдера сетевых услуг последний предъявляет подписчику определенные требования к соединениям, касающиеся, в частности, типа оборудования, предназначенного для получения этих услуг.

Как показано на рис. 8.3, наиболее часто используемыми терминами, связанными с основными типами услуг в распределенных сетях, являются следующие.

- **Стационарное оборудование пользователя (Customer's premises equipment, CPE).**
- Устройства, физически расположенные в помещениях пользователя. Они включают в себя как устройства, принадлежащие потребителю, так и устройства, арендованные у провайдера.
- **Демаркация (или демарк) (Demarcation или demarc).** Точка, в которой заканчивается CPE и начинается локальное ответвление службы провайдера. Часто эта точка находится в точке присутствия здания.
- **Местное ответвление (или "последняя миля").** Кабель (обычно медный провод), ведущий от точки демаркации к телефонной станции провайдера.
- **Коммутатор телефонной станции (CO switch).** Коммутирующее устройство, которое представляет собой ближайшую точку присутствия для службы провайдера распределенной сети.
- **Платная часть сети (toll network).** Коммутаторы и другие устройства коллективного пользования (также называемые стволами, trunk) в среде провайдера. Поток данных клиента на своем пути к месту назначения может проходить по стволу к первичному центру, затем к районному центру и далее к региональному или международному центру.

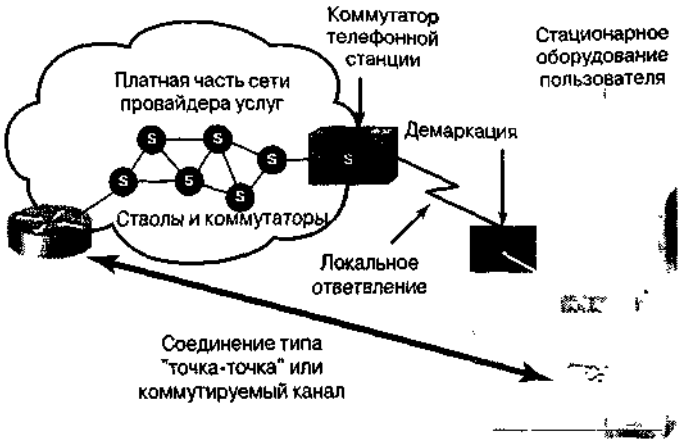


Рис. 8.3. Соединение организации с пунктом назначения осуществляется посредством вызова типа "точка-точка "

На участке пользователя основное взаимодействие происходит между **оборудованием терминала данных (data terminal equipment, DTE) и оборудованием конечной цепи (data circuit-terminating equipment, DCE).** Обычно DTE представляет собой маршрутизатор, а DCE является устройством, используемым для преобразования данных пользователя из формы, используемой DTE в форму, соответствующую устройству службы распределенной сети. Как показано на рис. 8.4, DCE представляет собой подсоединенный **модем (modem), модуль канальной службы/модуль службы данных (channel service unit/data service unit) или терминальный адаптер/сетевое окончание 1 (terminal adapter/network termination 1, TA/NT1).**

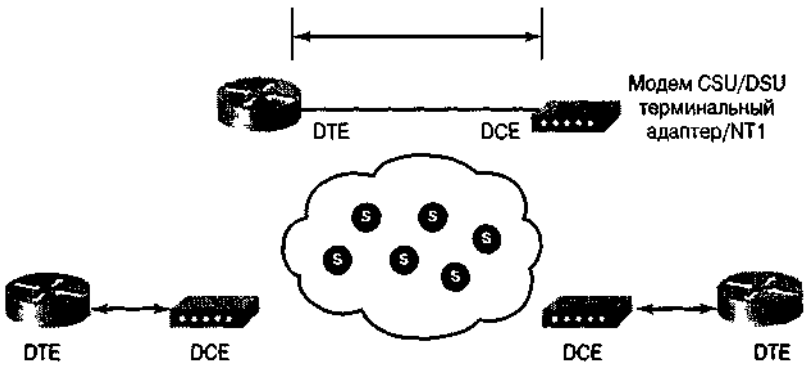


Рис. 8.4. При передаче данных по распределенной сети происходит соединение между собой DTE, вследствие чего они могут совместно использовать ресурсы, расположенные на обширной территории

Отрезок пути между двумя DTE называют каналом, цепью или линией. Сначала DCE обеспечивает интерфейс для доступа DTE к каналу среды распределенной сети. Интерфейс DTE/DCE выступает в качестве границы, на которой ответственность за передачу потока данных переходит от подписчика распределенной сети к провайдеру.

Интерфейс DTE/DCE использует различные протоколы (такие, например, как HSSI и v.3.5), которые устанавливают коды, используемые устройствами для взаимного обмена информацией. Этот интерфейс определяет, каким образом работает служба вызова и как поток данных пользователя проходит по распределенной сети.

Виртуальные каналы распределенных сетей

Виртуальный канал (virtual circuit) создается для обеспечения надежной связи между двумя сетевыми устройствами, В противоположность каналу типа "точка-точка" он представляет собой не физическую, а логическую цепь. Существуют два типа виртуальных каналов: **коммутируемые виртуальные каналы (switched virtual circuit) и постоянные виртуальные каналы (permanent virtual circuit).**

Коммутируемые виртуальные каналы создаются динамически по запросу и прекращают свое существование после окончания передачи. Процесс осуществления связи по коммутируемому виртуальному каналу состоит из трех этапов: создание канала, передача данных и отключение канала. Фаза установки канала включает в себя создание виртуальной цепи между устройствами источника и адресата. На этапе передачи данных осуществляется передача информации, а фаза окончания действия канала включает в себя разрыв связи между устройствами источника и получателя. Коммутируемые виртуальные каналы используются в ситуациях, когда обмен информацией между устройствами носит единичный характер. Такому каналу требуется большая полоса пропускания в связи с наличием фаз установки и разрыва связи, однако при этом обеспечивается снижение затрат по сравнению с ситуацией постоянно включенной виртуальной цепи.

Постоянный виртуальный канал имеет только один режим работы — передачу данных. Такие каналы используются в тех случаях, когда обмен данными между устройствами носит постоянный характер. Постоянные виртуальные каналы используют меньшую полосу пропускания за счет отсутствия фаз установки и разрыва цепи, но увеличивают расходы в связи с постоянной готовностью канала к передаче данных.

Вашингтонский проект: технологическое проектирование распределенной сети

В Вашингтонском округе требуется использовать постоянный виртуальный канал, работающий с протоколом Frame Relay. Этот канал необходимо добавить в Вашингтонский сетевой проект. Кроме того, необходимо создать канал доступа к Internet на базе протокола Frame Relay.

Стандарты сигнализации и скорости передачи в распределенных сетях

У провайдера распределенной сети можно заказать каналы с различной скоростью Передачи данных, которая измеряется в битах в секунду (бит/с). Эта скорость определяет, как быстро данные будут передаваться по распределенной сети. В США ширина полосы пропускания обычно регламентируется Северо-Американской классификацией цифровых линий (North American Digital Hierarchy), приведенной в табл. 8.1.

Таблица 8.1. Типы каналов и скорости передачи в распределенных сетях

Тип канала	Стандарт сигнала	Скорость передачи, бит/с
56	DSO	56 Кбит/с
64	DSO	64 Кбит/с
T1	DS1	1,544 Мбит/с
E1	ZM	2,048 Мбит/с
E3	M3	34,064 Мбит/с

Л	Y1	2,048 Мбит/с
Т3	DS3	44,736 Мбит/с
ОСИ	SONET	51, 84 Мбит/с
ОС-3	SONET	155,54 Мбит/с
ОС-9	SONET	466,56 Мбит/с
ОС-12	SONET	622,08 Мбит/с
ОСИ 8	SONET	933, 12 Мбит/с
ОС-24	SONET	1244, 16 Мбит/с
ОС-36	SONET	1866,24 Мбит/с
ОС-48	SONET	2488,32 Мбит/с

Устройства распределенных сетей

Распределенные сети используют различные типы устройств, включая следующие.

- Маршрутизаторы, выполняющие разнообразные функции, в частности, регулирование сетевых процессов и управление портами интерфейсов.
- Коммутаторы, осуществляющие передачу голосовых, цифровых и видеосигналов в пределах полосы пропускания распределенной сети
- Модемы, которые реализуют интерфейс для служб голосовых данных. Модемы включают в себя устройства CSU/DSU и TA/NT 1, поддерживающие интерфейс со службами ISDN.
- Коммуникационные серверы, основной задачей которых является установка и отключение связи с пользователем.

На рис. 8.5 показаны пиктограммы, используемые для изображения устройств распределенных сетей.

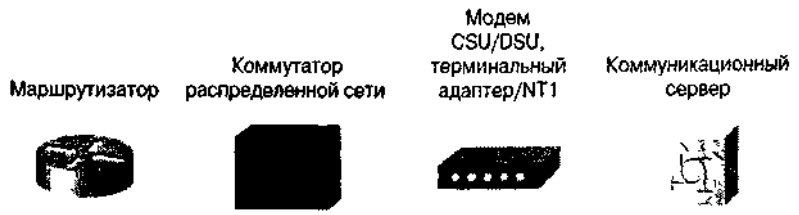


Рис 8 5 Основными устройствами распределенных сетей являются маршрутизаторы, коммутаторы, модемы и коммуникационные серверы

Маршрутизаторы

Маршрутизаторы представляют собой устройства, реализующие сетевые службы. Они обеспечивают интерфейс для различных каналов и подсетей в большом диапазоне скоростей. Мар-

шрутизаторы являются активными сетевыми узлами и поэтому могут осуществлять управление сетью. Это управление сетью осуществляется путем динамического контроля ресурсов и оценкой уровня выполнения сетью своих целей и задач. Такими целями являются надежная связь, эффективность, контроль управления и гибкость.

Коммутаторы распределенных сетей

Коммутаторы распределенной сети представляют собой сетевые устройства с несколькими портами, которые обычно коммутируют потоки данных таких протоколов, как Frame Relay, X 25 и коммутируемая мультимегабитная служба данных (Switched Multimegabit Data Service, SMDS). Коммутаторы распределенных сетей функционируют на канальном уровне эталонной модели OSI. На рис. 8 6 показаны два маршрутизатора, расположенных на разных концах распределенной сети и соединенных коммутаторами. В данном примере коммутаторы фильтруют, перенаправляют и поддерживают поток фреймов на основе адреса пункта назначения каждого фрейма

Вашингтонский проект: размещение коммутаторов

В качестве части проекта сети Вашингтонского учебного округа и его реализации необходимо определить требуемый тип коммутаторов, их количество и место размещения в сети В качестве возможных мест расположения следует рассмотреть MDF и IDF в помещениях школ и в главном окружном офисе.

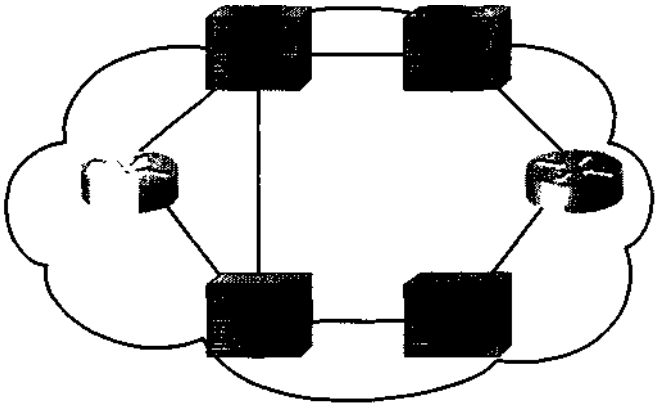


Рис 8 6 Коммутаторы распределенных сетей могут соединять два маршрутизатора, расположенных в разных концах сети

Модемы

Модемы представляют собой устройства, которые преобразуют друг в друга цифровые и аналоговые сигналы путем модуляции и демодуляции, что позволяет передавать Цифровые данные по обычным телефонным линиям У отправителя цифровые сигналы преобразуются в форму, требуемую для передачи данных по аналоговым каналам связи. В пункте назначения эти аналоговые сигналы преобразуются в первоначальную цифровую форму. На рис. 8.7 показан пример связи между модемами, осуществляв мой через распределенную сеть.

Рис. 8.7. Применение модемов позволяет распределенной сети работать как с аналоговыми, так и с цифровыми сигналами

Устройства CSU/DSU

CSU/DSU представляет собой устройство с цифровым интерфейсом (иногда два отдельных цифровых устройства), которое адаптирует физический интерфейс на устройстве DNE (таком, например, как терминал) к интерфейсу на DCE-устройстве (таком, как коммутатор) в сети с коммутируемым носителем. На рис. 8.8 показано размещение CSU/DSU в распределенной сети. Иногда CSU/CDU объединяются в | одном корпусе с маршрутизатором.

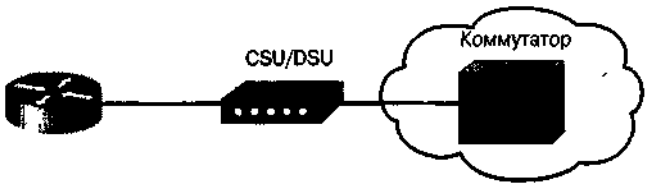


Рис. 8.8. В распределенной сети CSU/DSU размещаются между коммутатором и терминалом

Вашингтонский проект: размещение CSU/DSU

В качестве части проекта сети Вашингтонского учебного округа и его реализации необходимо определить требуемый тип CSU/DSU, их количество и место размещения в сети. В качестве возможных мест размещения можно рассмотреть школьные помещения и главный окружной офис, где будет заканчиваться распределенная сеть. Необходимо помнить о том, что CSU/DSU должны быть расположены по возможности ближе к маршрутизаторам.

Терминальные адаптеры ISDN

Терминальный адаптер ISDN представляет собой устройство, используемое для со-| единения интерфейса базовой скорости передачи (Basic Rate Interface, BRI) с другими| интерфейсами. Терминальный адаптер обычно представляет собой ISDN-модем. На рис. 8.9. показано размещение терминального адаптера в среде ISDN.

Рис 8 9. В распределенной сети терминальный адаптер соединяет ISDN с другими интерфейсами, такими, например, как коммутаторы

Распределенные сети и эталонная модель OSI

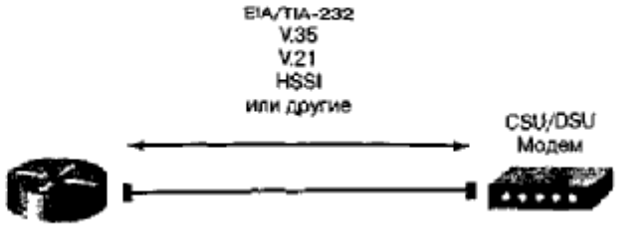
Распределенные сети используют для инкапсуляции уровневый подход эталонной модели OSI, так же как это делают виртуальные сети, однако в распределенных сетях эти операции сконцентрированы в основном на физическом и канальном уровнях. Стандарты распределенных сетей обычно описывают как методы доставки физического уровня, так и требования канального уровня, включая адресацию, управление потоком и инкапсуляцию. Стандарты распределенных сетей разрабатываются и поддерживаются рядом авторитетных организаций, часть из которых перечислена ниже.

- Отдел стандартизации при международном телекоммуникационном союзе (International Telecommunication Union-Telecommunication Standardization Sector, ITU-T). Ранее назывался Консультативным комитетом по международной телефонии и телеграфии (Consultative Committee for International Telegraph and Telephone, CCITT).
- Международная организация по стандартизации (ISO).
- **Инженерная группа по решению конкретной задачи в Internet (Internet Engineering task Force, IETF).**
- **Ассоциация электронной индустрии (Electronic Industries Association, EIA).**
- • Ассоциация индустрии телекоммуникаций (Telecommunications Industries Association, TIA)

Физический уровень распределенной сети

Протоколы физического уровня распределенной сети описывают работу служб распределенных сетей, осуществляющих электрические, механические, операционные и функциональные соединения. Большинство распределенных сетей требуют наличия соединения между собой, которое обеспечивается провайдером коммуникационной службы (таким, например, как RBOC), другим провайдером (таким, например, как провайдер услуг Internet) или **агентством почты, телеграфа и телефона (post, telegraph and telephone agency, FIT).**

Физический уровень распределенной сети также описывает интерфейс между DTE и DCE. Обычно OCE является провайдером службы, а DTE является подсоединенным устройством, как показано на рис. 8.10.



DTE
Оконечное устройство пользователя, подключенное к каналу распределенной сети

DCE
Оконечное устройство провайдера подключенное к коммуникационному устройству распределенной сети

Рис. 8.10. Канал провайдера услуги обычно заканчивается на DTE (например, на маршрутизаторе) и на DCE (например, на участке пользователя)

Требования, предъявляемые к интерфейсу между DTE и DCE, определяются несколькими протоколами физического уровня.

- EIA/TIA-232 — общий стандарт интерфейса физического уровня, разработанный EIA и TIA, который поддерживает несбалансированные сети со скоростью передачи до 64 Кбит/с. Он во многом аналогичен стандарту спецификации V.24 и был ранее известен как RS-232. Этот стандарт использовался в течение многих лет
- EIA/TIA-449 — популярный стандарт интерфейса физического уровня, разработанный EIA и TIA. Его можно рассматривать как более быструю версию (до 2 Мбит/с) протокола EIA/TIA-232, способную работать при большей длине кабеля
- EIA/TIA-612/613 — стандарт, описывающий высокоскоростной последовательный интерфейс (High Speed Serial Interface, HSSI), который обеспечивает доступ к службам со скоростями передачи: Т3 (45 Мбит/с), Е3 (34 Мбит/с) и к синхронной оптической сети STS-1 (Synchronous Optical Network, SONET) со скоростью 51,82 Мбит/с. Реальная скорость интерфейса зависит от внешнего DSU и от типа службы, к которой он подсоединен
- V.24 —стандарт ITU-T для интерфейса физического уровня между DTE и DCE
- V.35 —стандарт ITU-T, описывающий синхронный протокол физического уровня, используемый для осуществления коммуникации между устройством сетевого доступа и пакетной сетью. V.35 является наиболее распространенным в США и Европе протоколом и рекомендуется для скоростей передачи до 48 Кбит/с
- X.21 — стандарт ITU-T для последовательных соединений по синхронным цифровым линиям. Этот протокол используется главным образом в Европе и в Японии
- G.703 — электрическая и механическая спецификация ITU-T для осуществления связи между оборудованием телефонной компании и DTE с использованием английского морского соединителя (British Naval Connector, BNC), осуществляемой со скоростью линий типа E1
- EIA-530 — две реализации протокола EIA/TIA: RS-422 (для сбалансированной передачи) и RS-423 (для несбалансированной передачи).

Канальный уровень распределенной сети

Канальный уровень распределенной сети определяет способ инкапсуляции данных для передачи их на удаленные участки. Протоколы канального уровня распределенных сетей описыва-

ют, каким образом фреймы передаются от одной системы к другой.

На рис. 8.11 показаны основные типы инкапсуляции, используемые в каналах связи распределенных сетей.

- **Frame Relay.** Благодаря использованию упрощенной инкапсуляции без механизмов коррекции ошибок и передаче через высококачественные цифровые устройства Frame Relay может передавать данные со значительно большей скоростью, чем другие протоколы распределенных сетей.
- Протокол типа "точка-точка" (Point-to-Point Protocol, PPP). Описывается спецификацией RFC 1661; был разработан IETF. В заголовке PPP содержится специальное поле протокола, в котором указывается тип протокола сетевого уровня.
- ISDN. Набор цифровых служб для передачи голосовых и цифровых данных по существующим телефонным линиям.
- **Сбалансированный протокол доступа к каналу (Link Access Procedure, Balanced, LAPB).** Этот протокол используется в сетях с коммутацией пакетов для инкапсуляции пакетов на 2-м уровне стека X.25. Он также может быть использован в канале типа "точка-точка" в случае, когда канал обладает невысокой надежностью или имеет внутреннюю задержку, что происходит, например, в спутниковых каналах. Протокол LAPB обеспечивает высокую надежность передачи и управление потоком на основе соединениятипа "точка-точка".
- Cisco/IETF. Используется для инкапсуляции потоков данных протокола Frame Relay. Опция *Cisco* может быть использована только при обмене данными между маршрутизаторами Cisco
- Управление каналом данных высокого уровня (High-Level Data Link Control, HDLC). Несмотря на соответствие стандарту ISO, различные типы протоколов HDLC, приобретенные у разных производителей, могут оказаться несовместимыми друг с другом, поскольку каждый производитель может выбрать свой способ реализации этого протокола. Протокол HDLC поддерживает обе конфигурации: "точка-точка" и многоточечную.

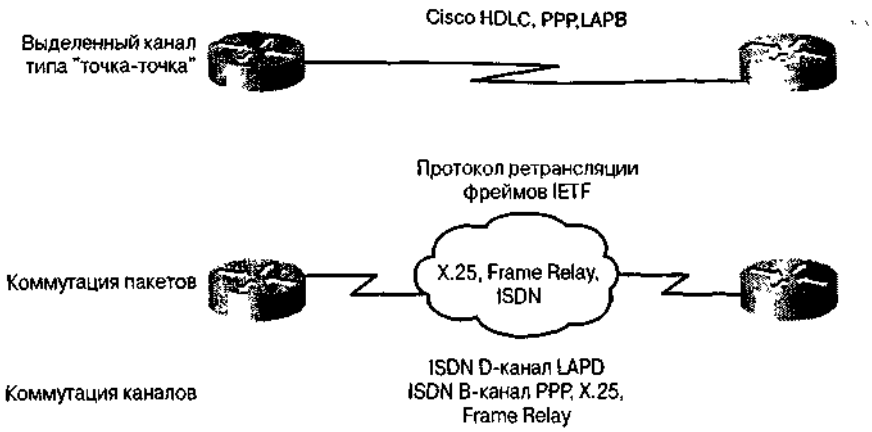


Рис. 8.11. Выбор протокола инкапсуляции зависит от технологии распределенной сети и от типа оборудования, осуществляющего связь

Форматы инкапсуляции фреймов в распределенных сетях

Двумя основными типами инкапсуляции типа "точка-точка" являются ЙВЬС и PPP. Все типы инкапсуляции в последовательных соединениях используют общий формат фрейма, который содержит следующие поля (рис. 8.12).

- Флаг — указывает начало фрейма; этому полю присваивается значение 7F **(в шестнадцатиричном виде, т.е. по основанию 16).**
- Адрес — поле из одного или двух байтов для адресации конечной станции в средах с множественной рассылкой.
- Управление — указывает на тип фрейма: информационный, служебный или ненумерованный. Содержит также конкретные коды функций.
- Данные — инкапсулированные данные.
- PCS — последовательность проверки фрейма (frame check sequence, PCS).
- Флаг — идентификатор трейлера; ему присваивается значение 7E.

PPP

Флаг	Адрес	Управление	Протокол	LSP	FCS	Флаг

HDL

Флаг	Адрес	Управление	Владелец	Данные	FCS	Флаг

Рис. 8.12. Инкапсуляция типа "точка-тонка " обычно используется в выделенных линиях распределенных сетей

Каждый тип соединения при передаче данных по каналам распределенной сети использует для инкапсуляции протокол 2-го уровня. Для того, чтобы быть уверенным в правильности протокола, используемого для инкапсуляции, необходимо задать тип конфигурации 2-го уровня для каждого последовательного интерфейса маршрутизатора. Выбор протокола инкапсуляции зависит от используемой технологии распределенной сети и от типа коммуникационного оборудования. PPP и HDLC представляют собой два типа протоколов инкапсуляции, которые можно использовать для соединений, описанных в настоящей главе.

Инкапсуляция протокола PPP

Протокол PPP предоставляет стандартный метод инкапсуляции для последовательных соединений (описан в стандартах RFC 1332 и RFC 1661). Этот протокол может, кроме всего прочего, проверять качество канала при установке связи. Протокол PPP также предоставляет возможность проверки аутентификации с помощью протокола проверки пароля (Password Authentication Protocol, PAP) или протокола аутентификации с предварительным согласованием вызова (Challenge Handshake Authentication Protocol, CHAP). Протокол PPP подробно описан в главе 10, "Протокол PPP".

Инженерный журнал: обсуждение канала PPP

Для обеспечения совместной работы версий программ, приобретенных у разных производителей, протокол PPP использует несколько дополнительных протоколов.

- Протокол LCP для согласования взаимодействия на основной линии.
- Семейство управляющих сетевых протоколов для согласования индивидуальных
  протоколов 3-го уровня и их IP-опций (таких, как управляющий IP-протокол, IP Control Protocol, IPCP) и других опций, таких как сжатие данных.

При согласовании параметров канала PPP сначала выбирается протокол управления каналом, а затем дополнительные управляющие сетевые протоколы.
Для проверки статуса LCP и управляющих сетевых протоколов можно использовать команду show interfaces, а для тестирования взаимодействия сетевых уровней могут быть использованы управляющие сетевые протоколы. Для устранения ошибок очень удобна команда debug ppp.
Для создания конфигурации последовательного соединения с использованием PPP используется команда encapsulation ppp:

```
Router(config)  #    interface    serial    0
Router(config-if)#  encapsulation ppp
```

Инкапсуляция протокола HDLC

HDLC представляет собой протокол канального уровня, созданный на базе использовавшегося ранее для инкапсуляции **протокола управления синхронным каналом данных (Synchronous Data Link Control).** HDLC-инкапсуляция является используемым по умолчанию типом инкапсуляции для последовательных каналов между маршрутизаторами Cisco. Реализация этого протокола является очень примитивной: отсутствуют окна и контроль потока, допускаются только соединения типа "точка-точка". В адресном поле все биты всегда равны единице. Кроме того, после управляющего поля вставлен 2-байтовый код производителя; это означает, что тип фреймов используемых HDLC несовместим с оборудованием других производителей.

Если на обоих концах выделенной линии расположены маршрутизаторы или серверы доступа, работающие с программным обеспечением операционной системы Cisco (Cisco Internetwork Operating System software, IOS), то для инкапсуляции обычно используется протокол HDLC. Поскольку методы инкапсуляции протокола HDLC не являются стандартными, для устройств, которые не используют программное обеспечение Cisco, необходимо использовать протокол PPP.

Вашингтонский проект: инкапсуляция PPP

Хотя для соединений типа "точка-точка" можно использовать оба типа протоколов — PPP и HDLC, в сети Вашингтонского учебного округа следует использовать каналы на основе протокола PPP. Этот протокол обладает следующими преимуществами.

- Совместимость с версиями других производителей.
- Возможность использования LCP для согласования взаимодействия с основной линией.
- Возможность использования семейства сетевых протоколов для согласования индивидуальных протоколов 3-го уровня.

Типы каналов распределенных сетей

Существуют два типа каналов, используемых в распределенных сетях: выделенные линии и коммутируемые соединения. Структура этих каналов показана на рис. 8.13. Коммутируемые соединения, в свою очередь, могут осуществлять коммутацию пакетов или каналов. В последующих разделах описываются эти типы каналов.

Выделенные линии

Выделенные линии, также называемые *арендованными линиями (leased lines),* обеспечивают постоянное пользование службой. Они обычно используются для передачи цифровых данных, голосовых данных и, иногда, видеоданных. При проектировании сети передачи данных выделенные линии обычно обеспечивают базовое или магистральное соединение между основными участками или промплощадками, а также связь между локальными сетями.

Использование выделенных линий считается основным вариантом при проектировании распределенных сетей. При использовании выделенных линий для осуществления связи с каждым удаленным участком необходимы порт маршрутизатора и канал, ведущий к этому участку.

После того, как две точки соединены выделенной линией, для каждой из них необходим порт маршрутизатора, CSU/CDU и реальная линия от провайдера службы. Стоимость поддержки вьщеленных линий может стать достаточно большой, если они используются для соединения между собой большого количества участков.

Связь по выделенной линии с постоянным доступом осуществляется по последовательным каналам типа "точка-точка". Соединения обычно осуществляются с использованием синхронных последовательных портов маршрутизаторов; при этом обычно используется до 2 Мбит/с (E1) полосы пропускания, что становится возможным благодаря использованию CSU/CDU. Различные методы инкапсуляции на канальном уровне обеспечивают гибкость и надежность при передаче данных пользователя. Выделенные линии такого типа являются идеальным решением для сред с передачей большого и стабильного количества данных. Однако использование выделенной линии может оказаться неэффективным в финансовом отношении, поскольку за нее приходится платить и в том случае, когда данные не передаются.

Рис. 8.13. Существуют различные типы соединений, использующих коммутацию пакетов или коммутацию каналов

Вашингтонский проект: выделенные линии

В Вашингтонском проекте выделенные линии следует использовать для создания ядра распределенной сети. В процессе проектирования необходимо определить требуемое количество таких линий и оборудование, которое необходимо для них приобрести (такое, как CSU/CDU).

Выделенные линии также часто называют каналами типа "точка-точка", потому что установленный для них путь является постоянным и фиксированным для каждой удаленной сети, доступ к которой обеспечивается сетевыми устройствами. Канал типа "точка-точка" обеспечивает отдельный, заранее установленный путь коммуникации в распределенных сетях от офиса пользователя через сеть носителей, такую, например, как телефонная компания, к удаленной сети. Провайдер услуг резервирует такой канал только для одного пользователя. На рис. 8.14 показан типичный канал типа "точка-точка", проложенный по распределенной сети.

Рис 8 14. Типовой канал "точка-точка" прокладывается по распределенной сети; он соединяет маршрутизаторы и оконечные устройства, расположенные на обоих концах канала

Соединения с коммутацией пакетов

Коммутация пакетов представляет собой такой метод коммутации в распределенных сетях, при котором сетевые устройства совместно используют отдельный канал типа "точка-точка" для транспортировки пакетов от источника к адресату через сеть-носитель, как показано на рис. 8.15. В качестве примера технологий с коммутацией пакетов можно привести Frame Relay, SMDC и X.25.

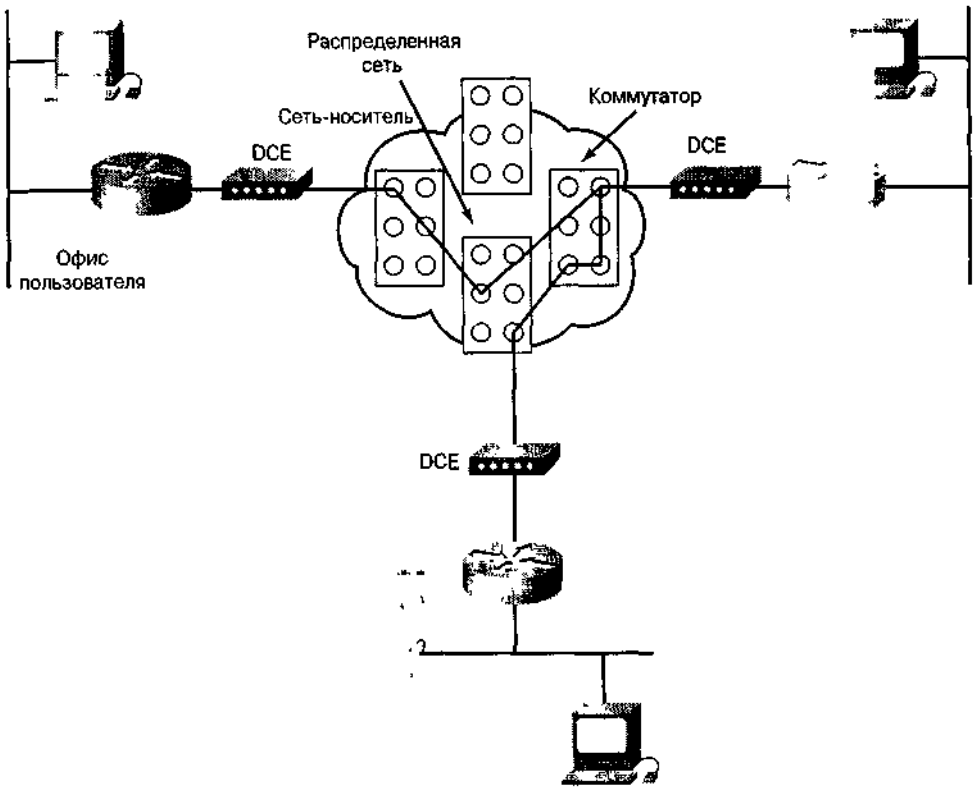


Рис 8 15 При пакетной коммутации пакеты передаются через сеть-носитель

Коммутируемые сети могут переносить фреймы (пакеты) переменного размера или ячейки постоянного размера. Наиболее типичным примером сети с коммутацией пакетов является сеть, использующая протокол Frame Relay.

Протокол Frame Relay

Протокол Frame Relay был разработан для работы в высокоскоростных и надежных каналах передачи данных. Такая постановка задачи привела к тому, что этот протокол не обладает мощными средствами для поиска ошибок и имеет невысокую надежность; для решения этих задач используются протоколы верхних уровней.

Frame Relay представляет собой пример коммуникационной технологии с коммутацией пакетов, которая позволяет подсоединить несколько сетевых устройств к многоточечной распределенной сети, как показано на рис. 8.16. Проектирование распределенной сети с использованием Frame Relay может оказать воздействие на работу протоколов верхнего уровня, таких как IP, IPX и AppleTalk, в частности, на расщепление горизонта. Протокол **Frame Relay** называется технологией множественного доступа без широковещания, поскольку в нем отсутствует возможности широковещания. Широковещательные сообщения передаются этим протоколом путем рассылки индивидуальных пакетов по всем пунктам назначения.

Рис. 8.16. Frame Relay представляет собой пример сетевой технологии с коммутацией пакетов Она была создана с целью обеспечения большей скорости и простоты в использовании, чем прежние технологии (такие, как X.25), предназначавшиеся для соединения между собой многочисленных сетевых устройств

Frame Relay определяет соединение между пользователем DTE и провайдером OCE. Обычно DTE представляет собой маршрутизатор, а DCE является коммутатором Frame Relay. (В данном случае DTE и DCE относятся не к физическому уровню, а к канальному). Frame Relay обеспечивает доступ со скоростями 56 Кбит/с, 64 Кбит/с или 1,544 Мбит/с.

Использование Frame Relay является эффективной в финансовом отношении альтернативой проектированию по методу "точка-точка". Каждый участок может быть соединен с любым другим посредством виртуального канала. Каждому маршрутизатору требуется только один физический интерфейс к провайдеру. Протокол Frame Relay обычно реализуется в виде услуги, предоставляемой провайдером, но он может также быть использован для частных сетей.

Ретрансляция фреймов обычно осуществляется через постоянные виртуальные каналы. Как канал передачи данных PVC обладает невысокой надежностью. **Идентификатор канального соединения (data-link connection identifier, DLCI)** используется для указания конкретного постоянного виртуального канала. Номер DLCI является локальным идентификатором в среде между DTE и DCE, описывающим логическую связь между устройствами отправителя и получателя. Соглашение о DLCI определяет **согласованную скорость передачи информации (committed information rate),** предоставляемую провайдером и измеряемую в битах в секунду. Она представляет собой скорость, с которой коммутатор Frame Relay обязуется передавать данные. (Эти вопросы рассмотрены более подробно в главе 12, "Протокол Frame Relay".).

Ниже, в главе 12 показано, что при использовании этого протокола могут быть реализованы две основные топологии.

- **Полно-сеточная топология (fully meshed technology).** В этой топологии каждое сетевое устройство имеет постоянную виртуальную цепь с любым другим устройством многоточечной распределенной сети. Каждое обновление, посланное каким-либо устройством, видно любому другому устройству. Если избран такой метод проектирования, то вся сеть ретрансляции фреймов может рассматриваться как один канал передачи данных.
- **Частично-сеточная топология (partially-meshed topology).** Такую топологию часто называют звездообразной топологией. В этой топологии не все устройства имеют постоянные виртуальные каналы с остальными устройствами.

Соединения с коммутацией каналов

Коммутация каналов представляет собой метод коммутации в распределенных сетях, при котором выделенная физическая линия устанавливается, поддерживается и ликвидируется для

каждого сеанса связи через сеть-носитель. Этот тип коммутации широко используется сетями телефонных компаний и действует во многом аналогично обычному телефонному вызову. Примером коммутации линий может служить протокол ISDN.

Соединения с коммутацией каналов устанавливаются при необходимости и обычно не требуют большой полосы пропускания. Соединения, построенные на основе обычных телефонных служб без уплотнения, как правило, используют ограниченную ширину полосы в 28,8 Кбит/с, а соединения протокола ISDN ограничены скоростями от 64 до 128 Кбит/с. Коммутация каналов используется в первую очередь для соединения удаленных и мобильных пользователей с корпоративной локальной сетью. Соединения с коммутацией каналов также используются в качестве запасных линий для высокоскоростных каналов, таких как Frame Relay и выделенные линии.

Маршрутизация с подключением по запросу

Маршрутизация с подключением по запросу (dial-on demand routing, DDR) представляет собой режим работы, при котором маршрутизатор может динамически инициировать и закрывать сеансы с коммутацией каналов в то время, когда это требуется передающим конечным станциям. Когда маршрутизатор получает поток данных, направленный в удаленную сеть, создается канал и поток направляется по нему обычным путем. Маршрутизатор поддерживает работу таймера занятости, который переустанавливается только тогда, когда получен требуемый поток данных (под требуемым потоком данных понимается поток, который маршрутизатор должен отправить). Однако, если время ожидания таймера истекло, то канал ликвидируется. Аналогично, если поступает посторонний поток данных, а канал для него отсутствует, то этот поток маршрутизатором отбрасывается. Если маршрутизатор получает важный поток данных, то создается новый канал.

Маршрутизация по запросу позволяет устанавливать стандартное телефонное соединение или соединение ISDN только в том случае, когда этого требует большой объем сетевых потоков. Она может оказаться более экономичной, чем выделенная линия или многоточечный вариант. Маршрутизация по запросу означает, что соединение устанавливается только в том случае, когда особый тип потока данных инициирует вызов или в случае, когда требуется резервная линия. Такого рода вызовы с коммутацией каналов, показанные пунктиром на рис. 8.17, выполняются с использованием сетей ISDN. Маршрутизация по запросу является эквивалентом выделенной линии в том случае, когда Не требуется постоянный доступ. Кроме того, такой тип маршрутизации может быть использован для замены каналов типа "точка-точка" и коммутируемых служб множественного доступа к распределенным сетям.

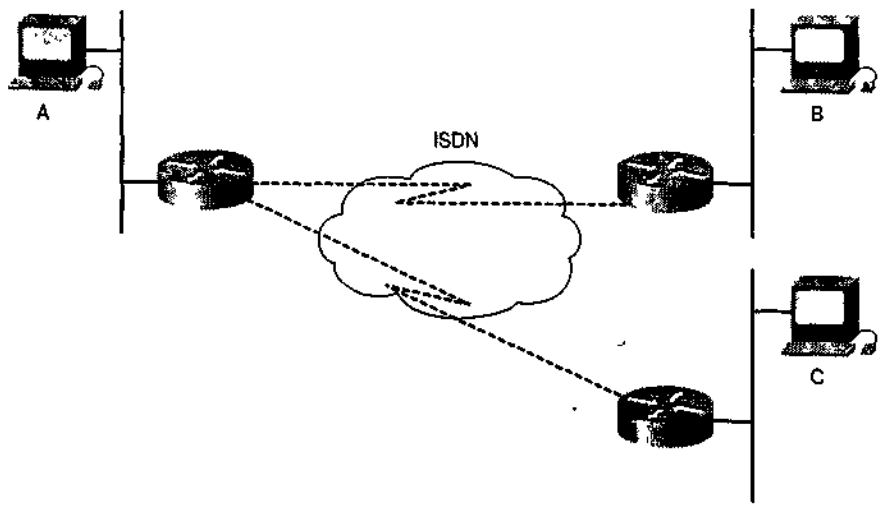


Рис. 8.17. Соединения ISDN устанавливаются только тогда, когда этого требует поток данных в сети

Коммутация по запросу может быть использована при необходимости перераспределения на-

грузки или в качестве резервного интерфейса. Например, предположим, что имеется несколько последовательных линий, но требуется, чтобы вторая линия использовалась только в том случае, когда первая линия загружена настолько, что может произойти перераспределение нагрузки. Когда распределенная сеть используется для критически важных приложений, может возникнуть необходимость в установке конфигурации, при которой линия с маршрутизацией по вызову включается в том случае, когда первая линия выходит из строя. В такой ситуации вторая линия позволяет обеспечить передачу данных.

По сравнению с локальными сетями или сетями предприятия поток данных, использующий DDR, имеет небольшой объем и носит периодический характер. Маршрутизация по запросу инициирует вызов удаленного участка только в том случае, когда имеются данные, которые требуется передать.

При установке конфигурации для DDR необходимо ввести конфигурационные команды, указывающие, какой тип пакетов должен инициировать запрос. Для этого необходимо внести в списки управления доступом директивы, определяющие адреса отправителя и адресата, и задать критерий выбора протокола, который будет инициировать вызов. После этого необходимо указать интерфейсы, с которых инициируется вызов DDR. Тем самым назначается группа набора (dialer group). Эта группа набора сопоставляет результаты сравнения пакетов с директивами списка управления доступом и интерфейсы маршрутизатора при осуществлении вызова в распределенной сети.

Протокол ISDN

Протокол ISDN был разработан телефонными компаниями с целью создания полностью цифровой сети. Устройства ISDN включают в себя следующее.

- Терминальное оборудование 1-го типа (TE1). Этот термин обозначает устройство, совместимое с сетью ISDN. Терминальное оборудование подключается к оборудованию NT 1-го или 2-го типа.
- Терминальное оборудование 2-го типа (TE2). Под ним понимается устройство, которое несовместимо с сетью ISDN и требует использования терминального адаптера.
- Терминальный адаптер (TA). Это устройство преобразует электрические сигналы в формат, используемый ISDN, в результате чего к сети ISDN могут быть подключены устройства, не относящиеся к ISDN-типу.
- NT-оборудование 1-го типа (NT1). Это устройство подсоединяет четырехпроводной кабель подписчика ISDN к обычному двухпроводному кабелю локального ответвления.
- NT-оборудование 2-го типа (NT2). Эти устройства направляют потоки данных на различные устройства подписчика и на оборудование типа NT1, а также в обратном направлении. NT2 представляет собой устройство, выступающее в качестве коммутатора и концентратора.

Как показано на рис. 8.18, особые точки интерфейса ISDN включают в себя следующее.

- Интерфейс S/T, который представляет собой интерфейс между TE1 и NT. S/T используется также в качестве интерфейса от терминального адаптера к NT.
- R-интерфейс представляет собой интерфейс между TE2 и NA.
- Под U-интерфейсом понимается двухпроводной интерфейс между NT и средой ISDN.

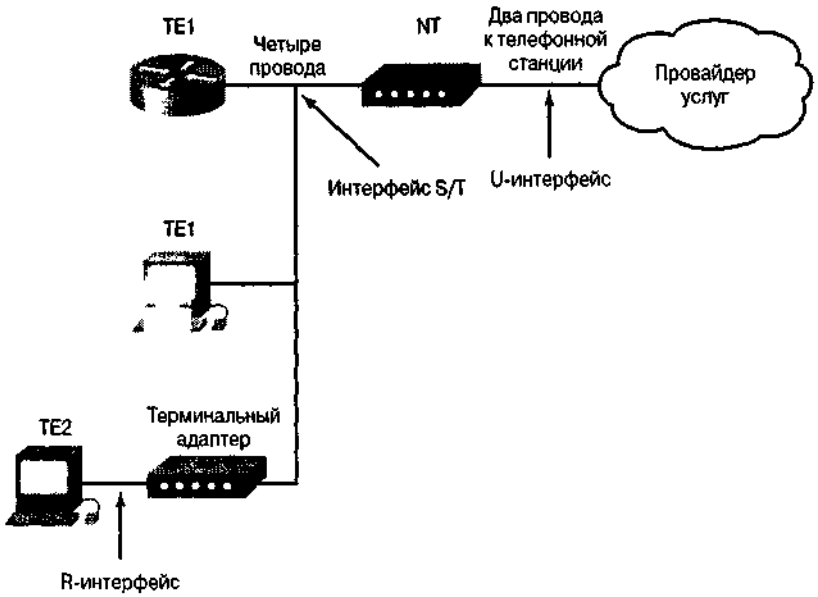


Рис. 8 18. ISDN представляет собой цифровую сетевую технологию, используемую для передачи голосовых, цифровых, факс-модемных и видеоданных от одного конца сети к другому

Имеются два вида служб ISDN: интерфейс базовой скорости (Basic Rate Interface, BRI) и интерфейс первичной скорости передачи данных (Primary Rate Interface, PRI). BRI работает главным образом с использованием витых медных пар телефонных проводов, уже установленных на данный момент. BRI разделяет общую ширину полосы пропускания 144 Кбит/с на три канала. Два из этих каналов, называемых **B-каналами** (bearer **channel, или канал-носитель),** работают со скоростью 64 Кбит/с и используются для передачи голосовых сообщений или для передачи цифровых данных. Третий канал, называемый **D-каналом (delta channel)** представляет собой сигнальный канал с полосой 16 Кбит/с и используется для передачи инструкций, указывающих телефонной сети режим работы с каждым из B-каналов. BRI часто обозначают как 2B+D. Протокол ISDN рассматривается более подробно в главе 11, "ISDN — цифровая сеть интегрированных служб".

Протокол ISDN предоставляет проектировщику сети большую гибкость, поскольку он позволяет использовать каждый из B-каналов для отдельных голосовых или цифровых приложений. Например, один B-канал ISDN, имеющий полосу пропускания 64 Кбит/с, может загружать большой документ из корпоративной сети, в то время как второй B-канал позволяет просматривать Web-страницу. При проектировании распределенной сети следует тщательно выбирать оборудование, которое способно эффективно использовать гибкость протокола ISDN.

Резюме

- Распределенные сети используются для связи между собой локальных сетей, находящихся на значительных расстояниях друг от друга.
- Распределенная сеть обеспечивает путь передачи данных между маршрутизаторами и локальными сетями, которые обслуживаются каждым из этих маршрутизаторов.
- Абонентам распределенной сети предоставляются различные виды услуг; при этом абонент должен знать, как получить доступ к службе провайдера распределенной сети.
- Устройства распределенных сетей включают в себя коммутаторы, модемы и терминальные адаптеры ISDN.
- Распределенные сети функционируют главным образом на физическом и канальном уровнях эталонной модели OSI.

- Для инкапсуляции *в* распределенных сетях используются форматы протоколов PPP и HDLC.
- В распределенных сетях используются такие типы каналов, как выделенные линии, соединения типа "точка-точка", соединения с коммутацией пакетов, (такие как Frame Relay) и соединения с коммутацией каналов (такие как DDR и ISDN).

Задачи проекта Вашингтонского учебного округа: распределенные сети

В настоящей главе были описаны технологии распределенных сетей, которые позволяют соединить все индивидуальные подразделения Вашингтонского учебного округа в единую распределенную сеть.

При этом необходимо решить следующие задачи.

1. Выбрать службы для окружной распределенной сети.
2. Определить количество и стоимость необходимых служб.
3. Описать в документации процесс проектирования распределенной сети.

Контрольные вопросы

Для проверки правильности понимания тем и понятий, описанных в настоящей главе, предлагается ответить на приведенные ниже вопросы. Ответы приведены в приложении А.

1. Сколько путей используется протоколами канального уровня распределенных сетей для переноса фреймов между системами?
   A. Два.
   B. Один.
   C. Четыре.
   D. Неопределенное количество.
2. На каком уровне эталонной модели OSI находится оборудование OCE и DTE?
   A. На сетевом уровне.
   B. На канальном уровне.
   C. На физическом уровне.
   D. На транспортном уровне.
3. На каком типе оборудования обычно используются CSU/CDU?
   A. Маршрутизатор.
   B. DTE.
   C. Коммутатор.
   D. DCE.
4. Какой из приведенных ниже типов инкапсуляции используется в синхронных последовательных каналах связи?
   A. PPP.
   B. HDLC.
   C. Frame Relay
   D. Ничто из перечисленного.
5. Какой тип инкапсуляции следует выбрать для канала в том случае, когда ско рость является самыми важным фактором?
   A. Frame Relay.
   B. PPP.
   C. HDLC.
   D. SLIP.

6. Устройства, расположенные на территории абонента, называются...
   A. оборудованием, собственником которого является потребитель.
   B. устройства подписчика.
   C. стационарное оборудование пользователя.
   D. стационарное оборудование подписчика.
7. Путь в распределенной сети между DTE называется...
   A. линией.
   B. цепью.
   C. каналом.
   D. Все перечисленное.
8. Какие службы распределенной сети могут быть использованы маршрутизатором?
   A. Frame Relay.
   B. ISDN.
   C. PPP.
   D. Все перечисленное.
9. Что из перечисленного ниже является примером протокола с пакетной коммутацией?
   A. ISDN.
   B. Frame Relay.
   C. PPP.
   D. HDLC.
10. Какой протокол использует PPP для установления и поддержания соединений типа "точка-точка"?
   A. HDLC.
   B. LCP.
   C. LAPD.
   D. Cisco IFTF.

Основные термины

B-канал или канал-носитель (bearer channel, B channel). Дуплексный канал ISDN-типа, работающий со скоростью 64 Кбит/с и используемый для передачи данных пользователя.

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

Ассоциация телекоммуникационной индустрии (Telecommunications Industries Association, TIA). Организация, разрабатывающая стандарты для телекоммуникационных технологий. TIA и EIA совместно формализовали стандарты, такие как EIA/TIA-232, определяющие электрические характеристики процесса передачи данных.

Ассоциация электронной индустрии (Electronic Industries Association, EIA). Группа, устанавливающая стандарты передачи данных. EIA и TIA совместно разработали большое количество стандартов коммуникации, включая стандарты EIA/TIA-232 и EIA/TIA-449.

Блок канального интерфейса/блок цифровой службы (channel service unit/digital service unit, CSU/DSU). Устройство цифровой связи, соединяющее оборудование конечного пользователя и ответвление локальной телефонной станции.

Виртуальный канал или виртуальная цепь (virtual circuit). Логический канал, создаваемый для обеспечения надежной связи между двумя сетевыми устройствами. Виртуальный канал определяется парой VPI/VCI и может быть постоянным (PVC) или коммутируемым (SVC). В виртуальных каналах используются протоколы ретрансляции фреймов и X.25. Иногда используется аббревиатура VC.

Временное мультиплексирование (time-division multiplexing, TDM). Сигнал коммутации канала, используемый для определения маршрута вызова, который является выделенным путем от отправителя к получателю.

Дельта-канал (D channel, delta channel). Дуплексный ISDN-канал работающий со скоростью 16 Кбит/с (BRI) или 64 Кбит/с (PRI).

Демаркация (demarcation). Точка, в которой заканчивается CPE и начинается местное ответвление службы. Часто находится в точке присутствия здания.

Идентификатор канального соединения (data-link connection identifier, DLCI). Идентификатор PVC или SVC в сети Frame Relay. В базовой спецификации Frame Relay DLCI имеют локальное значение (т.е. подсоединенные устройства могут использовать различные значения для одного и того же соединения). В расширенной спецификации LMI идентификаторы канального уровня являются глобальными (т.е. указывают на индивидуальные оконечные устройства).

Инженерная группа по решению конкретной задачи в Internet (Internet Engineering Task Force, IETF). Организация, состоящая из более чем 80 рабочих групп и отвечающая за развитие стандартов Internet. IFTF работает под руководством ISOC.

Канал типа "точка-точка" (point-to-point link). Канал, обеспечивающий отдельный, заранее установленный путь коммуникации от стационарного оборудования потребителя до удаленной сети через сеть провайдера, такую, например, как сеть телефонной компании. Также называется выделенной линией или арендованной линией.

Коммутируемый виртуальный канал (switched virtual circuit, SVC). Виртуальный канал, устанавливаемый динамически по требованию и ликвидируемый после окончания передачи. Коммутируемые виртуальные каналы используются в ситуациях спорадической передачи данных.

Маршрутизация с коммутацией по запросу (dial-on-demand routing, DDR). Вид маршрутизации, при которой маршрутизатор открывает и закрывает сеанс коммутации линий только тогда, когда в этом нуждаются оконечные передающие станции.

Местное ответвление (local loop). Кабель (обычно медный провод), идущий от линии демаркации до центрального офиса провайдера распределенной сети.

Модем (модулятор-демодулятор) (modern, modulator-demodulator). Устройство, преобразующее цифровые сигналы в аналоговые и наоборот. На станции-источнике модем преобразует цифровые сигналы в форму, соответствующую передаче по каналам аналоговой связи. В пункте назначения аналоговые сигналы преобразуются в цифровую форму. Модемы позволяют передавать цифровую информацию по телефонным линиям.

Надежность (reliability). Величина, представляющая собой отношение числа полученных подтверждений активности к числу ожидаемых. Чем больше это отношение, тем надежнее линия. Эта величина используется в качестве метрики при маршрутизации

Оборудование конечной цепи (data circuit-terminating equipment, DCE). Устройство, используемое для преобразования данных пользователя из формата DTE в формат, используемый оборудованием службы распределенной сети.

Оборудование терминала данных (data terminal equipment, DTE). Устройство, расположенное на пользовательском конце интерфейса "пользователь-сеть", которое может выступать в качестве источника данных, получателя данных или в качестве обоих. DTE соединяется с сетью данных посредством устройства DCE (например, модема) и обычно использует временные сигналы, генерируемые DCE. Оборудование терминала данных включает в себя такие устройства, как компьютеры, трансляторы протоколов и мультиплексоры.

Платная часть сети (toll network). Коллективные коммутаторы и другие устройства (называемые магистралями или стволами) в среде провайдера распределенной сети.

Полно-сеточная топология (fully meshed topology). Топология, в которой каждое устройство сети ретрансляции фреймов имеет PVC со всеми остальными устройствами многоточечной распределенной сети.

Постоянный виртуальный канал (permanent virtual circuit, PVC). Виртуальный канал, установленный на постоянный режим работы. Постоянные виртуальные каналы экономят полосу пропускания, затрачиваемую на создание канала и на его ликвидацию, в ситуациях, когда виртуальная цепь должна существовать постоянно.

Почта, телефон и телеграф (post, telephone and telegraph, PTT). Государственная организация, предоставляющая телефонные услуги. Филиалы PTT имеются в большинстве регионов за пределами США и обеспечивают местные, междугородные и международные телефонные услуги.

Протокол X.25. Стандарт ITU-T, определяющий способ поддержки соединений между DTE и DCE для удаленного терминального доступа и компьютерных коммуникаций в общедоступных сетях передачи данных. Протокол **Frame Relay** в определенной степени вытеснил X.25.

Протокол ретрансляции фреймов или протокол Frame Relay (Frame Relay). Стандартный промышленный коммутируемый протокол канального уровня, который обслуживает большое количество виртуальных цепей, используя HDLC-инкапсуляцию между соединенными устройствами. **Frame Relay** более эффективен, чем протокол X.25, и рассматривается в качестве его замены.

Распределенная сеть (wide-area network, WAN). Сеть передачи данных, обслуживающая пользователей, расположенных на обширном географическом пространстве; такие сети часто используют устройства передачи, предоставляемые общими провайдерами. Примерами технологий распределенных сетей могут служить Frame Relay, SMDS и X.25.

Региональное отделение компании Bell (Regional Bell operating company, RBOC). Местная или региональная телефонная компания, которая владеет и осуществляет управление телефонными линиями и коммутаторами в одном из семи регионов США. Эти компании были созданы при ликвидации компании AT&T.

Режим асинхронной передачи (Asynchronous Transfer Mode, ATM). Международный стандарт для передачи ячеек, в которых различные типы данных (такие, например, как аудио-и видеоданные) передаются в ячейках фиксированной длины (53 байта). Использование ячеек фиксированной длины позволяет обрабатывать их на стационарном оборудовании, сокращая тем самым транзитные задержки. ATM позволяет воспользоваться высокоскоростными передающими средами, такими как E3, SONET и T3.

Сбалансированный протокол доступа к каналу (Link Access Procedure, Balanced, LAPB). Протокол канального уровня в стеке протокола X.25. LAPB является бит-ориентированным протоколом, разработанным на базе протокола HDLC.

Сетевой терминатор 1 (network termination I, NT1). Устройство, поддерживающее интерфейс со службами ISDN.

Сеть провайдера (carrier network). Сеть провайдера услуг.

Сигнальная система 7 (Signaling System 7, SS7). Стандартная система сигнализации, разработанная корпорацией Bellcore. Она использует управляющие телефонные сообщения и сигналы при вызове пункта назначения.

Согласованная скорость передачи информации (committed information rate, CIR). Скорость передачи данных, измеряемая в битах в секунду, с которой Frame Relay соглашается передавать данные.

Стационарное оборудование пользователя (customer premises equipment, CPE). Оконечное оборудование, такое как терминалы, телефоны и модемы, устанавливаемое в помещениях пользователя и подсоединенное к сети телефонной компании.

Телефонная станция или центральный офис (Central office, CO). Офис местной телефонной компании, к которому подсоединены все локальные ответвления и в котором происходит коммутация линий подписчиков.

Терминальный адаптер (terminal adapter, TA). Устройство, используемое для подключения BRI-соединений службы ISDN к существующим интерфейсам, таким как EIA/TIA-232. Как правило, терминальный адаптер представляет собой ISDN-модем.

Топология типа "звезда" или звездообразная топология (star topology). Топология локальных сетей, в которой концевые точки сети подсоединены к общему центральному коммутатору каналами типа "точка-точка". Кольцевая звездообразная топология вместо каналов типа "точка-точка" реализуется в виде замкнутой звезды с одним направлением.

Точка присутствия (point of presence, POP). Точка соединения коммуникационных устройств, предоставляемых телефонной компанией, с главным распределительным центром здания.

Управление синхронным каналом данных (Synchronous Data Link Control, SDLC). SNA-протокол канального уровня коммуникации. SDLC является бит-ориентированным, дуплексным последовательным протоколом, ставшим основой для создания многих аналогичных протоколов, включая протоколы HDLC и LAPB.

Частично-сеточная топология (partially meshed topology). Топология, в которой не каждое устройство среды Frame Relay имеет PVC с остальными устройствами.

Шестнадцатеричный (по основанию 16) (hexadecimal (base 16)). Числовое представление, использующее цифры от 1 до 9 в обычном значении и буквы от A до F для представления десятичных чисел от 10 до 15. В шестнадцатеричном представлении самая правая цифра обозначает единицы, следующая - числа, кратные 16, следующая — кратные 16^2=256 и т.д.

Ключевые темы этой главы

- Описывается обмен информацией в распределенной сети
- Описываются процесс проектирования распределенной сети и требования к сети
- Описывается процесс сбора требований предъявляемых пользователями к распределенной сети
- Описываются преимущества использования иерархической модели проектирования и определяются три уровня этой модели
- Описывается размещение протоколов ISDN и Frame Relay,
- Описывается влияние способа размещения серверов предприятия и рабочих групп на характер потока данных, проходящего по распределенной сети
- Описываются требования магистральных служб
- Описываются преимущества коммутаторов и службы 2-го уровня
- Описываются преимущества маршрутизаторов и службы 3-го уровня
- Описывается много и одно-протокольная маршрутизация
- Определяются и описываются параметры надежности распределенной сети

Глава 9

Проектирование распределенной сети

Введение

В настоящее время сетевым администраторам приходится управлять сложными распределенными сетями (wide-area networks, WAN) для поддержания растущего числа приложений, которые базируются на протоколе IP и Web Таким распределенным сетям требуются ресурсы и высокоэффективные сетевые технологии Распределенная сеть представляет собой комплексную среду, включающую большое количество носителей, протоколов и соединений с другими сетями (например, с Internet) Распределенной сети требуется множество протоколов и функций для обеспечения своего роста и управляемости

Несмотря на повышение эффективности оборудования и расширение возможностей носителей, проектирование распределенных сетей становится все более трудным Тщательное проектирование распределенных сетей может уменьшить проблемы, связанные с их ростом Чтобы спроектировать надежную распределенную сеть, проектировщик должен постоянно помнить о наличии у каждой такой сети своих специфических требований Эта глава представляет собой обзор методологий, применяемых при проектировании распределенных сетей

Вашингтонский проект: проектирование распределенной сети

В этой главе описывается процесс проектирования распределенной сети позволяющий реализовать требования к службам в сети учебного округа Для осуществления обмена данными распределенная сеть округа соединит все школы и административные учреждения с центральным офисом округа

Обмен данными в распределенной сети

Обмен информацией в распределенной сети происходит между географически разделенными областями. Когда локальная конечная станция пытается обменяться данными с уда-

ленной конечной станцией (т.е. расположенной в другом участке распределенной сети), информация передается по одному или нескольким **каналам распределенной сети** (WAN **link).** Точками соединения в распределенной сети являются маршрутизаторы. Они определяют оптимальный путь через сеть, по которому пройдут требуемые потоки данных.

Как было сказано в главе 8, "Распределенные сети", обмен информацией в таких сетях обычно называется службой, поскольку сетевые провайдеры, обеспечивающие обмен, часто взимают плату с пользователей за этот сервис. **Коммутация пакетов (packet-switching) и коммутация каналов (circuit-switching)** представляют собой два типа служб в распределенных сетях. Каждый из этих двух типов имеет свои достоинства и недостатки. Например, сети с коммутацией каналов предоставляют пользователю выделенную полосу пропускания, которая не может использоваться другими пользователями. В отличие от этого, коммутация пакетов представляет собой метод коммутации в распределенной сети, при котором сетевые устройства совместно используют один канал типа "точка-точка" для транспортировки пакетов от отправителя к адресату через несущую сеть. Сети с коммутацией пакетов обычно обладают большей гибкостью и используют полосу пропускания эффективнее, чем сети с коммутацией каналов.

Традиционно распределенным сетям присущи относительно низкая пропускная способность, задержки и высокий уровень ошибок. Соединения в распределенных сетях характеризуются стоимостью аренды носителя (т.е. провода) у провайдера услуг, предоставляющего кабель для соединения двух или более групп зданий (campus) или промплощадок. Поскольку инфраструктура распределенной сети часто арендуется у провайдера, при проектировании сети необходимо оптимизировать стоимость и эффективность использования полосы пропускания. При разработке технологий распределенных сетей ставилась задача удовлетворения перечисленных ниже требований.

- Оптимизация полосы пропускания распределенной сети.
- Минимизация стоимости.
- Достижение максимальной эффективности службы для конечного пользователя.

В последнее время возросла нагрузка на традиционные сети с общей передающей средой. Это связано с появлением перечисленных ниже новых требований к сетям.

- Увеличение потребления сетевых ресурсов на предприятиях использующих для повышения производительности клиент/серверные, мультимедийные и другие приложения.
- Происходящее повышение уровня требований приложений (например, Push-технологии) и тенденция дальнейшего движения в этом направлении.
- Рост стоимости сети, приводящий к увеличению расходов.
- Повышенные требования приложений, предоставляющих услуги конечным пользователям, к качеству сетевых служб.
- Беспрецедентное количество соединений, устанавливаемых между разнообразными офисами, удаленными и мобильными пользователями, международными подразделениями, потребителями/поставщиками, и широкое использование Internet.
- Взрывной рост корпоративных сетей intranet и extranet значительно повысил требования к полосе пропускания.
- Значительно возросло использование серверов предприятий для удовлетворения коммерческих нужд организаций.

По сравнению с имеющимися распределенными сетями, новые сети должны быть более сложными по структуре, базироваться на новых технологиях и иметь возможность удовлетворять постоянно увеличивающиеся и быстро меняющиеся требования приложений с гарантированным уровнем обслуживания. Кроме того, в связи с увеличением сетевых потоков на 300%, ожидающимся в ближайшие пять лет, предприятиям придется приложить большие усилия по

сдерживанию роста накладных расходов на использование распределенных сетей.

Для удовлетворения этих новых требований проектировщики используют технологии распределенных сетей. Соединения распределенных сетей, как правило, передают важную информацию и оптимизируются по цене и эффективности использования полосы пропускания. Маршрутизаторы, соединяющие промплощадки, применяют оптимизацию потока данных, множественные пути для передачи избыточных данных, резервные соединения на случай аварий и средства повышения качества обслуживания (quality of service, QoS) для особо важных приложений. В табл. 9.1 обобщаются различные технологии распределенных сетей, которые позволяют удовлетворить указанные требования.

Таблица 9.1. Обзор технологий распределенных сетей

Технология	Применение
Выделенная линия	Выделенные линии могут использоваться в сетях, основанных на протоколе PPP (Point-to-Point Protocol). Кроме того, они могут применяться в топологиях типа "накопление-передача" (hub-and-spokes) или в качестве запасного варианта для других типов линий
Интегрированная сеть цифровых служб (ISDN)	ISDN используется для предоставления высокорентабельного удаленного доступа к корпоративным сетям. Эта технология обеспечивает передачу голосовых и видеоданных, а также используется в качестве запасного варианта для других типов линий
Протокол ретрансляции фреймов (Frame Relay)	Протокол ретрансляции фреймов обеспечивает высокорентабельную, скоростную передачу данных с низким уровнем задержек, используемую для связи между удаленными участками. Протокол Frame Relay может использоваться как в частных сетях, так и в сетях, предоставляемых провайдерами

Интеграция распределенных и локальных сетей

Распределенные приложения, требующие большей полосы пропускания, а также взрывной рост Internet подводят многие архитектуры локальных сетей к пределу их физических возможностей. Значительно возрос уровень обмена голосовыми данными, который все чаще используется в централизованных системах голосовой почты (voice mail system). Сеть является жизненно важным инструментом для поддержания информационного потока. От сетей требуется меньшая стоимость и одновременно поддержка все большего числа новых приложений и все большего количества пользователей с повышенными требованиями к эффективности работы сети.

До настоящего времени локальные и распределенные сети оставались логически разделенными. В локальных сетях полоса пропускания является бесплатной и возможности связи ограничиваются только аппаратным обеспечением и стоимостью реализации. В распределенных сетях оплата за использование полосы пропускания вызывает большую часть затрат, а данные, чувствительные к задержкам, например голосовые, передаются отдельно от остальных данных.

Internet-приложения, передающие речь и видео в реальном времени, требуют лучшей и более предсказуемой работы локальных и распределенных сетей. Подобные мультимедийные приложения быстро становятся основным средством повышения производительности труда. По мере того как предприятия начинают планировать развертывание новых intranet-приложений, мультимедийных приложений, таких как видеообучение, видеоконференции и передача голоса через IP-сети (voice over IP), интенсивно использующих полосу пропускания, нагрузка подобных приложений на существующую сетевую инфраструктуру вызывает граничит с пределами ее воз-

можностей.

Например, в случае, если компания полагается на свою корпоративную сеть для передачи особо важного для ее работы потока данных и желает использовать интерактивные видео приложения, то она должна быть способна обеспечить гарантированное качество обслуживания (QoS). Это означает, что сеть должна доставлять мультимедийные данные, не допуская при этом их "столкновения" с основными данными. Следовательно, проектировщикам сети необходимо проявить достаточную гибкость при решении многочисленных проблем межсетевого взаимодействия, не создавая при этом избыточных сетей и по возможности использовать уже существующие капиталовложения в коммуникации.

Первый этап проектирования распределенной сети

Проектирование распределенной сети может оказаться достаточно трудной задачей. В последующем обсуждении очерчены области, на которые следует обратить особое внимание при планировании распределенной сети. Выполнение описанных ниже рекомендаций поможет улучшить показатели стоимости и производительности распределенной сети. Предприятия могут непрерывно улучшать свои распределенные сети, используя эти рекомендации в процессе планирования.

Двумя основными целями проектирования и реализации распределенной сети являются следующие.

- *Доступность приложений.* Сети переносят данные приложений между компьютерами. Если приложения недоступны пользователям, то сеть не выполняет свои основные функции.
- *Снижение общей стоимости сети.* В США бюджеты отделов информационных систем часто составляют миллионы долларов. Поскольку крупные предприятия все более полагаются на электронные данные в управлении производственными процессами, общая стоимость компьютерных ресурсов будет постоянно возрастать. Хорошо спроектированная распределенная сеть способна помочь сбалансировать эти цели, а реализованная должным образом инфраструктура распределенной сети может оптимизировать доступность приложений и позволит более эффективно использовать существующие ресурсы в финансовом отношении.

В целом при проектировании распределенной сети следует учитывать три следующих основных фактора.

- *Переменные окружения.* Переменные окружения включают в себя расположение хостов, серверов, терминалов и других конечных узлов, проектируемый объем передачи данных через среду и предполагаемую стоимость доставки служб различных уровней.
- *Существующие ограничения производительности.* Они связаны с уровнем надежности сети, шириной полосы пропускания потока данных и быстродействием клиентских компьютеров (например, скорости доступа к сетевым адаптерам и жестким дискам).
- *Сетевые переменные.* Сетевые переменные включают в себя топологию сети, пропускную способность линии и объем потока данных. Характеристики потока данных чрезвычайно важны для успешного планирования распределенной сети, однако очень немногие проектировщики внимательно учитывают этот важнейший элемент проектирования, если вообще обращают на него внимание.

Инженерный журнал: характеристики потока данных

При проектировании распределенной сети огромное значение имеют тип потока данных, проходящих по сети.

Существуют следующие типы потоков данных:

- голосовые и факс-данные;
- данные транзакций (например, SNA);
- клиентские и серверные данные;
- сообщения (например, электронная почта);
- передача файлов;
- пакетные данные;
- управление сетью;
- видеоконференции.

Классификация и анализ типов передаваемых данных являются основой для принятия принципиальных решений при проектировании сетей. Объем потоков данных определяет пропускную способность сети, а последняя, в свою очередь, определяет стоимость. Проверенные временем процессы измерения и оценки объема потоков данных в традиционных сетях непригодны для распределенных сетей.

Характеристики потоков данных включают в себя:

- максимальный и средний объем;
- возможности установки соединений и объем потоков;
- ориентацию на типы соединений;
- допустимость задержек, включая их продолжительность и возможные изменения длительности;
- допуск на доступность сети;
- допустимый уровень ошибок;
- приоритет;
- тип протокола;
- средняя длина пакета.

Многие проектировщики не владеют методиками планирования и проектирования, необходимыми для работы со сложными и неопределенными потоками данных в распределенных сетях. Они обычно не оценивают, а угадывают ширину полосы пропускания, что приводит в конечном итоге к реализации дорогостоящих "перепроектированных" сетей или, напротив, "недопроектированных" сетей с низкой производительностью.

Общая цель проектирования распределенной сети состоит в том, чтобы минимизировать ее стоимость при соблюдении всех требований по обеспечению доступа. Проектировщик сталкивается с двумя основными проблемами: обеспечением доступа и стоимостью. Решения этих проблем, как правило, противоречат друг другу. Любое увеличение доступности отражается на росте стоимости. Следовательно, проектировщик должен тщательно оценить важность того или иного ресурса и общую стоимость.

Первым шагом в процессе проектирования является рассмотрение производственных требований, которое освещается в следующих параграфах. Требования к распределенной сети должны отражать цели, характеристики, производственные процессы и стратегию предприятия, на котором будет работать сеть.

Сбор требований

Проектирование распределенной сети необходимо начать со сбора данных о структуре и производственных процессах предприятия. Затем следует определить основных сотрудников предприятия, которые могут помочь в процессе проектирования сети. Проектировщик должен выяснить месторасположение основных пользователей, приложения, которыми они пользуются, и их планы на будущее. Окончательный проект сети должен отражать все требования пользователей.

Вообще пользователям прежде всего необходима доступность их приложений в сети. Основными компонентами доступности приложений являются время отклика (response time), пропускная способность и надежность.

- *Время отклика* — это время между вводом команды (или нажатием клавиши) и ее выполнением операционной системой хоста (или доставкой ответа с сервера). Приложения, предназначенные для интерактивной работы, например, автоматизированные кассы и торговые автоматы, следует считать критичными к быстрому отклику.

- Приложения, интенсивно использующие полосу пропускания, как правило, при работе совершают операции по передаче файлов. Однако обычно они предъявляют низкие требования к времени отклика. Эти приложения можно настроить на запуск в такое время, когда сокращается чувствительный ко времени отклика обмен данными (например, в нерабочее время).

- Хотя надежность важна всегда, некоторые приложения предъявляют требования, превышающие обычные. Организации, которые должны быть почти постоянно в полной готовности, проводят все операции по телефону или в реальном времени. Финансовые службы, торговля ценными бумагами, скорая помощь, полиция и военные операции — вот несколько примеров подобных организаций. Такие ситуации предъявляют очень высокие требования к аппаратному обеспечению и требуют наличия резервных вариантов. Учет стоимости времени простоя является основой при обеспечении необходимого уровня надежности такой сети.

Существует целый ряд способов изучения пользовательских требований. Чем больше пользователей включается в этот процесс, тем точнее будет оценка. В общем плане рекомендуется использовать следующие методы получения информации.

- *Профили пользовательских групп*. На первом этапе определения требований сети попытайтесь описать потребности различных групп пользователей. Хотя большая часть пользователей имеет примерно одинаковые требования к электронной почте, у некоторых из них могут быть специфические требования, например, у пользователей, совместно использующих серверы печати в финансовом отделе.

- *Интервью, фокус-группы* и *опросы* определяют принципиальный подход к реализации сети. Некоторым группам может потребоваться доступ к общим серверам. Другие могут выразить желание предоставить внешний доступ к специфическим внутренним вычислительным ресурсам. Для некоторых организаций может потребоваться поддержка со стороны информационного отдела, которая будет контролироваться определенным образом, согласно каким-либо внешним стандартам. Еще один способ получения информации — это проведение формальных опросов в наиболее важных группах пользователей. Также могут использоваться фокус-группы для сбора информации и организации дискуссий между разными предприятиями со сходными (или несходными) интересами. И, наконец, формальный опрос может использоваться для получения статистически достоверной интерпретации пожеланий пользователей относительно определенного уровня обслуживания.

- *Тестирование человеческого фактора*. Проведение лабораторного теста с привлечением представителей пользовательских групп — наиболее дорогой, отнимающий много времени но, возможно, наиболее эффективный метод изучения пользовательских требований. Он особенно полезен при оценке требований ко времени отклика. Например, можно установить работающую систему и привлечь пользователей для имитации в лаборатор-

ной сети обычной активности удаленных хостов. Изучая реакцию пользователя на "живой" отклик хоста, можно определить реальные значение требуемой производительности.

После сбора данных об организационной структуре необходимо определить информационные потоки компании, т.е. выяснить, где расположены данные, предоставленные для совместного доступа, и кто их использует. Необходимо также определить, необходим ли доступ к данным за пределами сети компании.

Проектировщику следует разобраться в проблемах существующей сети и, если позволяет время, проанализировать производительность этой сети.

Вашингтонский проект: понимание потребностей заказчика

Первое и главное — необходимо понять заказчика. В рассматриваемом случае учебного округа заказчиками являются преподаватели, студенты, обслуживающий персонал и администрация.

Необходимо определить, имеются ли в округе четко определенные правила и ответить на следующие вопросы.

- Есть ли в округе данные, жизненно важные для функционирования предприятия?
- Выполняются ли в округе операции, считающиеся жизненно важными?
- Какие протоколы можно использовать в сети округа?
- Все ли типы рабочих станций поддерживаются или только некоторые?

Жизненно важные данные и операции рассматриваются в качестве ключевых для функционирования сети, а доступ к ним является особенно важным при ежедневном выполнении стандартных операций. Далее следует определить, кто в организации обладает полномочиями на установку адресации, задание имен, на установку конфигурации и планирование топологии. В некоторых округах есть центральный департамент управления информационными системами (Management Information Systems MIS), который контролирует все эти вопросы. В других этот департамент очень мал и поэтому полномочия передаются отделам.

Анализ требований

При проектировании следует проанализировать предъявляемые к сети требования, включая технические и деловые цели заказчика. Какие новые приложения будут установлены? Существуют ли приложения, основанные на использовании Internet? Какие новые сети будут доступны? Что является критерием успеха (т.е. как узнать, успешен ли проект)?

Полезность сети измеряется ее доступностью. На доступность влияют многие факторы, такие как пропускная способность, время отклика и доступ к ресурсам. У каждого заказчика есть свое определение *доступности*. Доступность можно увеличить путем добавления ресурсов, но такой путь увеличивает стоимость. При проектировании сети необходимо искать способы обеспечения большей доступности с меньшими затратами.

Вашингтонский проект: анализ доступности

Необходимо выяснить, что означает понятие доступность для заказчиков, которыми в случае Вашингтонского учебного округа являются преподаватели, студенты, обслуживающий персонал и администрация. Анализируя технические требования, следует оценить нагрузку на сеть, вызванную работой приложений и обычным поведением протокола (например, при подключении нового узла к сети). Необходимо определить нагрузку

в худшем случае, то есть во время максимальной занятости пользователей, и во время запуска регулярных сетевых служб, таких как резервное копирование на файловом сервере. Все это поможет понять, что означает доступность для заказчика.

Цель анализа — определить для основных участков средний и максимальный объем данных, передаваемых за единицу времени. Следует попытаться охарактеризовать активность в течение обычного рабочего дня в следующих терминах: тип передаваемых данных, их объем, время отклика хостов, время выполнения передачи файлов т.д. Можно также понаблюдать за использованием существующего сетевого оборудования в течение периода тестирования.

Инженерный журнал: измерение объема потока данных

В зависимости от типа передаваемых данных можно использовать одну из четырех следующих методик анализа и измерения объема потока данных.

- Сетевое управляющее программное обеспечение. В некоторых случаях это программное обеспечение можно использовать для анализа статистики передаваемых данных.
- Измерения *в* уже существующих сегментах сети. Можно разместить оборудование для сетевого *анализа* на серверах и для существующего сегмента сети исследовать статистические данные, приходящие с маршрутизатора.
- Процесс оценки. В случаях, когда измерения в существующих сегментах применить нельзя (например, еще нет будущего приложения), можно использовать качественную оценку. В тесном сотрудничестве с администраторами сети и разработчиками программного обеспечения необходимо оценить количество транзакций, их величину и длительность для получения статистических характеристик потока данных.
- Метод сравнительных источников (comparative sources). Вероятно, существует возможность найти источники, имеющие сходные характеристики и, основываясь на них, определить соответствующие статистические характеристики потока данных.

Если характеристики протестированной сети близки к аналогичным параметрам новой сети, то можно попытаться оценить число пользователей, приложений и топологию этой новой сети. В случае отсутствия необходимых инструментов описанный выше метод является наилучшим подходом для приблизительной оценки характеристик потока данных.

В добавление к пассивному мониторингу существующей сети, можно измерить активность и поток данных, который генерируется известным количеством пользователей, подключенных к тестовой сети, а затем сделать выводы, ориентируясь на ожидаемую численность пользователей.

Одной из сложностей при расчете рабочих нагрузок в сетях является то, что практически невозможно определить величину потока данных и производительность устройств в сети как функцию числа пользователей, типов приложений и географического расположения. Особенно часто это случается при отсутствии реальной сети.

Вашингтонский проект: анализ сетевой нагрузки и проблем, связанных с потоками данных

Перед разработкой сети округа и установкой аппаратного обеспечения необходимо определить нагрузку от потока данных, который должен обрабатываться распределенной сетью. Следует определить все источники данных и параметры, которые необходимо

установить для них. На этом этапе очень важно получить характеристику источников, достаточную для оценки или измерения величины потока данных. Кроме того, необходимо опробовать приложения, которые могут вызвать в распределенной сети учебного округа проблемы, связанные с передачей данных. Ниже представлен ряд приложений, которые могут генерировать большие объемы данных и таким образом привести к проблемам, например, к перегрузке сети:

- доступ к Internet;
- компьютеры, загружающие программное обеспечение с удаленного сервера;
- передача изображений или видеоинформации;
- доступ к центральной базе данных;
- файловые серверы отделов.

Необходимо заранее предусмотреть введение в распределенную сеть новых источников или приложений наряду с вероятным уровнем роста. Этот шаг может потребовать продолжительных консультаций с конечными пользователями округа и разработчиками приложений. Наконец, не стоит забывать о таком важном источнике, как управляющая информация, используемая сетью округа, которая может составлять более 15 процентов от общего потока данных.

Рассмотрим следующие факторы, влияющие на динамику сети.

- Зависимость характеристик доступа в сеть от времени. Пиковые периоды могут меняться, и измерения должны проводиться в том числе и в период времени, включающий пиковые запросы.
- Различия, связанные с типом передаваемых данных. Потоки данных мостов и| маршрутизаторов связаны с различными запросами к сетевым устройствам и протоколам. Некоторые протоколы чувствительны к потерянным пакетам, а определенные типы приложений требуют большей полосы пропускания.
- Случайная природа характеристик потока данных в сети. Нельзя предсказать точное время прибытия и специфические эффекты передаваемых данных.

У каждого источника данных есть своя метрика, которую необходимо прообразовать в скорость (количество битов в секунду). Проектировщику следует стандартизировать оценку количества передаваемых данных с целью определения удельного объема потока данных на одного пользователя. Наконец, следует применить какие-либо коэффициенты для учета непроизводительных затрат протокола, фрагментации пакетов, роста потока и проблем безопасности. Изменяя эти коэффициенты, можно проводить анализ потока данных и прогнозировать его. Например, можно запустить Microsoft Office на сервере и затем анализировать объем данных, генерируемых пользователями, совместно использующими это приложение в сети. Полученное значение поможет определить полосу пропускания и требования к серверу для установки Microsoft Office в сети.

Проверка чувствительности к отказам

С практической точки зрения, проверка чувствительности к отказам сводится к наблюдению последствий разрыва стабильных соединений. Это относительно просто реализуется во время работы с тестовой сетью. Можно нарушить работу сети путем удаления какого-либо активного интерфейса и затем проследить, как сеть обрабатывает произошедшие перемены — как происходит перемаршрутизация потока данных, какова скорость конвергенции, не теряется ли связь и не возникают ли проблемы при обработке специфических типов данных. Можно также изме-

нить уровень потока данных в сети для того, чтобы определить, как влияет на сеть объем потока данных, вызывающий насыщение передающей среды.

Определение и выбор возможностей сети

После анализа предъявляемых к сети требований проектировщик должен идентифицировать, а затем выбрать конкретные решения, соответствующие вычислительной среде. Информация, приведенная в следующих разделах поможет осуществить эти действия.

Идентификация и выбор сетевой модели

Иерархические модели сетевого проектирования позволяют осуществлять поуровневое проектирование сетей. Для понимания важности разделения на уровни рассмотрим эталонную модель взаимодействия открытых систем (OSI), которая является иерархической моделью, облегчающей понимание и реализацию компьютерных коммуникаций. Благодаря подразделению на уровни, эталонная модель OSI упрощает задачи, которые необходимо решить для осуществления обмена информацией между двумя компьютерами. Иерархические модели сетевого проектирования также используют уровни для упрощения задач, возникающих при организации межсетевого взаимодействия. Каждый уровень специализируется на выполнении присущих именно ему функций, что позволяет проектировщику выбирать соответствующие конкретному уровню системы и характеристики.

Использование иерархического проектирования может облегчить внесение изменений в архитектуру сети. Модульность проектирования сети позволяет создать такие элементы проекта, которые могут быть отдельно изменены в случае роста сети. Поскольку каждый элемент проекта сети требует изменений, стоимость и комплексность усовершенствований в значительной степени зависит от небольшой части сети. В крупной сети с простой или замкнутой архитектурой перемены оказывают воздействие на большое количество систем. Структурируя сеть на небольшие, простые для понимания элементы, можно облегчить нахождение аварийных участков сети. При этом администраторам сети значительно легче определить ключевые точки переходов, что, в свою очередь, помогает определить места, в которых произошли сбои.

Иерархическая модель проектирования сети

Проекты сетей имеют тенденцию следовать одной из двух общих стратегий проектирования: замкнутой или иерархической. В замкнутой структуре сетевая топология проста. Все маршрутизаторы выполняют в целом одинаковые функции и обычно нет четкого определения участков сети, в которых выполняются специфические функции. Расширение сети в этом случае происходит, как правило, случайным и произвольным образом. В случае иерархической структуры сеть разделена на уровни, каждый из которых выполняет специфическую функцию. Ниже представлены преимущества использования иерархической модели проектирования.

- *Расширяемость.* Сети, построенные на базе иерархической модели, могут увеличиваться без нанесения ущерба контролю или управляемости. Это связано с тем, что функциональность сети локализована и потенциальные проблемы распознаются значительно проще. Примером крупномасштабного иерархического сетевого проекта может служить общедоступная коммутируемая телефонная сеть.
    - *Простота реализации.* Иерархическое проектирование предписывает каждому уровню выполнение его специфических функций, облегчая реализацию сети.
    - *Простота устранения неисправностей.* Поскольку функции каждого уровня четко определены, упрощается поиск источника возникших проблем. Облегчается также временное сегментирование сети для сужения круга поиска проблем.

- *Предсказуемость*. Сеть, разработанная с использованием функциональных уровней, является достаточно предсказуемой, что значительно облегчает планирование пропускной способности, учитывая рост сети в будущем. Такой подход при проектировании также облегчает моделирование требуемой производительности сети для аналитических целей.
- *Поддержка протоколов*. Объединение текущих и будущих приложений и протоколов гораздо легче осуществить в сетях, которые следуют принципам иерархического проектирования, поскольку основная инфраструктура таких сетей уже логически организована.
- *Управляемость*. Все описанные преимущества иерархической модели проектирования способствуют большей управляемости сети.

Использование иерархической модели проектирования

Иерархическое проектирование сетей включает в себя следующие три уровня.

- *Основной уровень* (core layer), который также называется магистральным. Этот уровень обеспечивает оптимальную транспортировку данных между участками распределенной сети.
- *Уровень распределения* (Distribution layer), который обеспечивает связь, основанную на использовании политик доступа.
- *Уровень доступа* (Access layer), который обеспечивает доступ рабочих групп и |пользователей к сети.
- На рис. 9.1 схематически представлены различные аспекты иерархического проектирования сети.

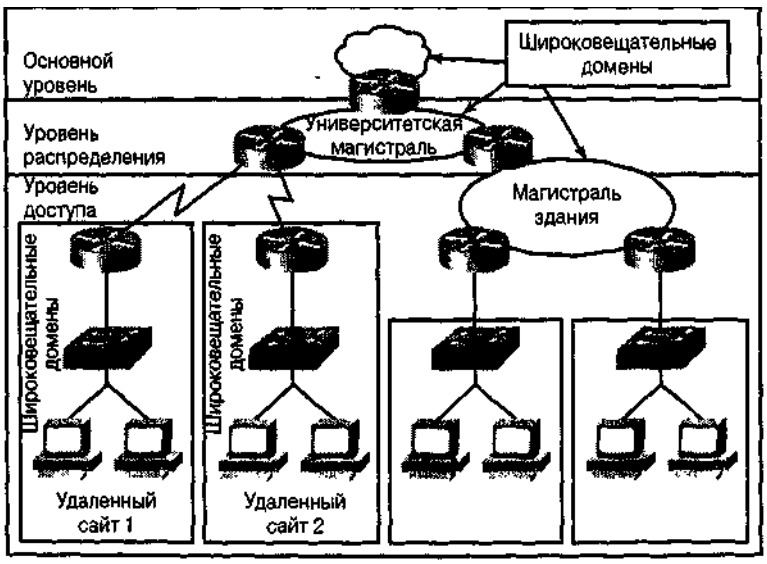


Рис. 9.1. Иерархическое сетевое проектирование представлено тремя уровнями: основным уровнем, уровнем распределения и уровнем доступа. Каждый из этих уровней обеспечивает выполнение присущих именно ему функций

Компоненты трехуровневой модели

Уровень можно определить как область сети, в границах которой функционирует 3-й (сетевой) уровень эталонной модели OSI. Три уровня ограничены устройствами сетевого уровня или другими устройствами, которые разделяют сеть на широковещательные домены. Как показано на рис. 9.1, трехуровневая модель состоит из основного уровня, уровня распределения и уровня доступа. На каждом из этих уровней выполняются свои, специфические для данного уровня функции.

- *Основной уровень*. Уровень, обеспечивающий скоростные, протяженные соединения между географически удаленными участками, связывая несколько промплощадок (групп зданий) в распределенную сеть предприятия или корпорации. Каналы центрального уровня обычно представляют собой связи типа "точка-точка" и подключение отдельных хостов непосредственно к этим каналам является достаточно редким явлением. Службы центрального уровня (например, T1/T3, Frame Relay, SMDS) обычно предоставляются в аренду провайдерами телекоммуникационных услуг.
- *Уровень распределения*. Предоставляет сетевые службы для локальных сетей внутри распределенной сети. На этом уровне находится магистраль распределенной сети. Уровень распределения часто базируется на Fast Ethernet. Этот уровень обычно реализуется в крупных участках и используется для соединения зданий.
- *Уровень доступа*. Уровень, обычно представляющий собой локальную сеть или группу локальных сетей (часто Ethernet или Token Ring), обеспечивающий пользователям доступ к сетевым службам. На этом уровне происходит подключение к сети почти всех хостов, включая серверы всех видов и рабочие станции пользователей. В главе 4, "Проектирование локальных сетей", основное внимание уделяется вопросам проектирования на уровне доступа.

Трехуровневая модель способна удовлетворить требования большинства сетей предприятий. В то же время не все сети требуют полной трехуровневой иерархии — одно- или двухуровневые проекты также имеют право на существование. Однако даже в этом случае необходимо поддерживать иерархическую структуру, чтобы дать возможность одно- или двухуровневым сетям расширяться до трехуровневой реализации, если это потребуется в будущем . В следующих параграфах более подробно обсуждаются функции всех трех уровней. Затем рассматриваются одно- и двухуровневые иерархии сетей.

Функции основного уровня

Главная функция основного уровня — это обеспечение скоростного канала связи между удаленными участками, как показано на рис. 9.2. На этом уровне не следует осуществлять какие-либо операции с пакетами, такие как фильтрация или использование списков управления доступом, поскольку они замедляют коммутацию. По этой причине основной уровень обычно реализуется распределенной сетью. Для такой сети может потребоваться организация резервных (избыточных) путей, которые обеспечат функционирование сети даже в случае возникновения разрывов в отдельных каналах связи. Другими важными задачами, решаемыми на этой стадии проектирования, являются распределение нагрузки и быстрая конвергенция протоколов маршрутизации. Практически всегда на основном уровне необходимо добиваться эффективного использования полосы пропускания.

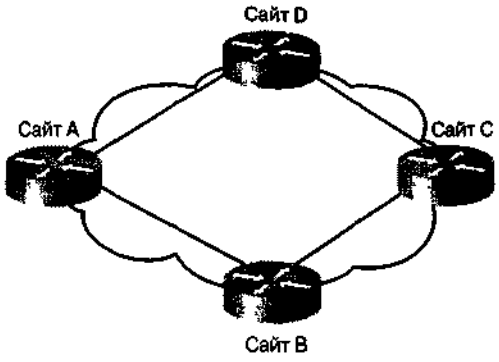


Рис. 9.2. Основной уровень оптимизирует транспортировку данных между удаленными участками путем создания резервных (избыточных) путей, распределения нагрузки, обеспечения эффективного использования полосы пропускания и быстрой конвергенции

Вашингтонский проект: основной уровень распределенной сети

Основа распределенной сети Вашингтонского учебного округа должна представлять собой магистраль, которая спроектирована для коммутации пакетов с максимально возможной скоростью. Школы должны подключаться к магистрали распределенной сети, основываясь на близости расположения к этой магистрали.

Функции уровня распределения

Уровень распределения представляет собой границу между основным уровнем и уровнем доступа и помогает определять и выделять основной уровень. Целью уровня распределения является определение границ; на этом уровне также происходят операции с пакетами. В среде распределенной сети на этом уровне может выполняться несколько функций, таких как:

- обработка адресов;
- доступ рабочих групп или отделов;
- определение широковещательных доменов и доменов многоадресных рассылок;
- маршрутизация локальных сетей (виртуальных локальных сетей);
- переход на любую необходимую среду передачи данных;
- безопасность.

Уровень распределения включает в себя также магистраль группы зданий со всеми подключенными маршрутизаторами, как показано на рис. 9.3. Поскольку стратегия обеспечения доступа обычно реализуются на этом уровне, можно сказать, что уровень распределения обеспечивает связь, основанную на стратегии доступа. Понятие связи, основанной на стратегии доступа означает, что маршрутизаторы 3-го уровня запрограммированы пропускать по университетской магистрали только те потоки данных, которые определены администратором сети как допустимые. Следует заметить, что

опытные проектировщики обычно не размешают конечных станций (таких как серверы) на магистрали. Это дает возможность магистрали функционировать исключительно в качестве транзитного пути для потоков данных, проходящих между рабочими группами в разных зданиях или от рабочей группы к университетским серверам.

Рис. 9.3. Уровень распределения определяет метрики путей и управляет доступом к службам и сетевыми уведомлениями

В сетях без групп зданий уровень распределения может быть точкой перераспределения между доменами маршрутизации или между протоколами статической и динамической маршрутизации. Он также может быть точкой доступа удаленных участков к корпоративной сети. Обобщая сказанное выше, можно сказать, что уровень распределения представляет собой уровень, который обеспечивает связь, основанную на стратегии обеспечения доступа.

Функции уровня доступа

Уровень доступа представляет собой точку, в которой локальные пользователи получают доступ в сеть, как показано на рис. 9.4. Кроме того, на этом уровне могут использоваться списки управления доступом или фильтры для дальнейшей оптимизации потребностей определенной группы пользователей. В сетях предприятий функции этого уровня включают в себя:

- совместно используемую полосу пропускания;
- коммутируемую полосу пропускания;
- фильтрацию MAC-уровня;
- микросегментацию.

Уровень доступа подключает пользователей к локальным сетям и локальные сети к магистралям или каналам распределенной сети. Такой подход позволяет проектировщикам распределять работу служб по процессорам (CPU) устройств, которые функционируют на этом уровне. Уровень доступа позволяет осуществить логическую сегментацию сети и группировке пользователей в зависимости от выполняемых ими функций. Традиционно такая сегментация основывается на организационном делении (например, отдел маркетинга, администрация или техническая служба). Однако с точки зрения управления сетью и перспектив контроля, главная функция уровня доступа—это изоляция широковещательных потоков данных к отдельной рабочей группе или локальной сети. Этот уровень более подробно рассматривался в главе 4, "Проектирование локальных сетей". В сетях, не включающих в себя групп зданий, этот уровень предоставляет доступ к корпоративной сети для удаленных участков посредством какой-либо технологии распределенных сетей, такой как Frame Relay, ISDN или выделенные линии, которые описываются в следующих главах.

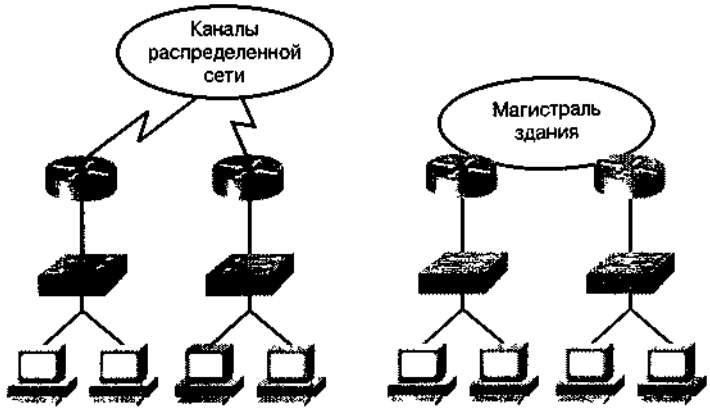


Рис. 9.4. Уровень доступа соединяет рабочие группы с магистралями

Разработка одноуровневой сети

Не все сети требуют трехуровневой иерархии. Ключевым моментом при разработке является определение места расположения серверов: они могут быть распределены по нескольким локальным сетям или сконцентрированы в районе центрального сервера. На рис. 9.5 показан вариант сети с распределенными серверами. Одноуровневая сеть обычно применяется в случае, если в компании имеется небольшое количество удаленных подразделений, а доступ к приложениям в основном осуществляется через локальную сеть к файловому серверу участка. Каждый участок представляет собой отдельный широковещательный домен.

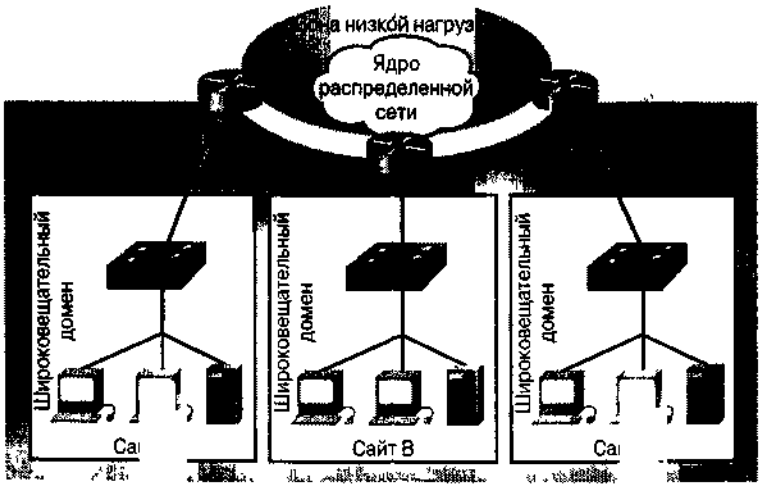


Рис. 9 5 Одноуровневое проектирование приемлемо для многих небольших сетей

Разработка двухуровневой сети

В случае двухуровневого варианта каналы распределенной сети используются для соединения отдельных участков, как показано на рис. 9.6. Внутри участка могут применяться многочисленные локальные сети, каждый сегмент которых является отдельным широковещательным до-

меном Маршрутизатор участка А является точкой концентрации каналов распределенной сети.

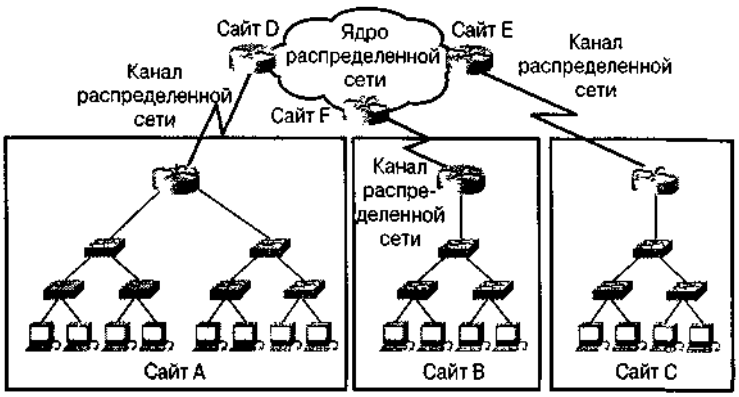


Рис. 96В двухуровневых проектах для создания отдельных логических сетей могут организовываться виртуальные локальные сети

Вашингтонский проект: двухуровневая иерархическая модель

При проектировании распределенной сети Вашингтонского учебного округа следует взять за основу двухуровневую иерархическую модель Для формирования оптимальной распределенной сети необходимо установить три региональных концентратора — по одному в окружном офисе, сервисном центре и начальной школе Shaw Butte

---

Преимущества иерархического проектирования распределенной сети

Одним из преимуществ иерархического проектирования распределенной сети является создание возможности управления структурой потока данных. Это преимущество реализуется путем внедрения в сеть точек маршрутизации 3-го уровня. В связи с тем, что маршрутизаторы обладают способностью определять пути от хоста-источника к хостам-адресатам, основываясь при этом на адресации 3-го уровня, поток данных проходит вверх по иерархии сети только тот путь, который необходим для отыскания пункта назначения (рис 9 7)

Если бы хосту А было необходимо установить связь с хостом В, то поток данных прошел бы через маршрутизатор 1 и был бы отправлен обратно вниз к хосту В. Из рис. 9.8 видно, что для этого соединения не требуется прохождения данных по каналу между маршрутизатором 1 и маршрутизатором 2 и, таким образом, полоса пропускания этого канала сохраняется.

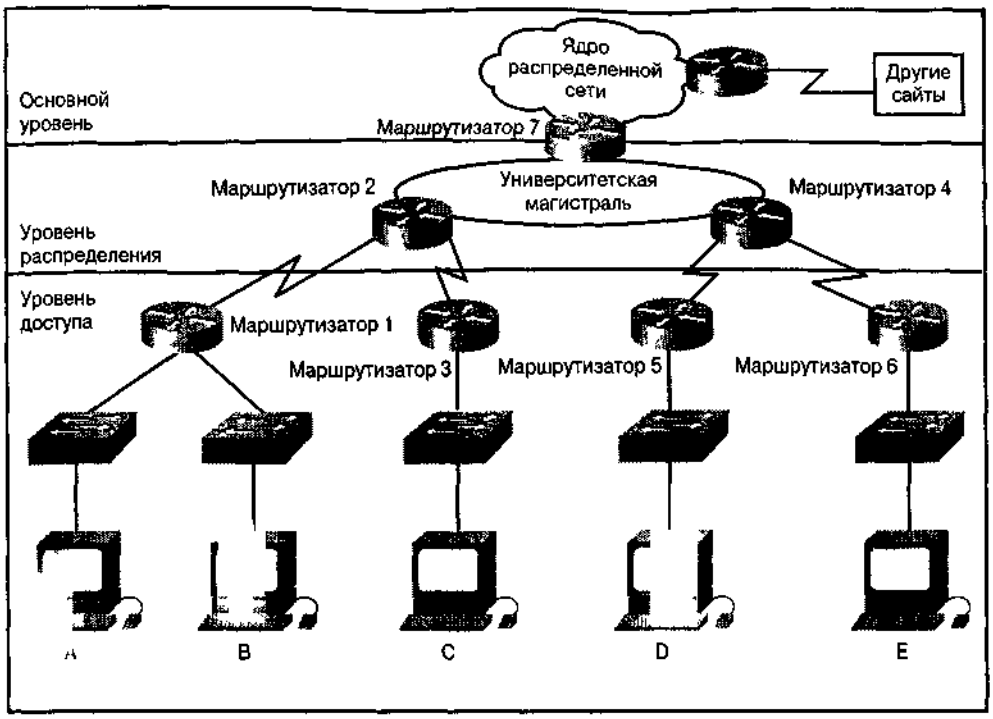


Рис. 9.7. Маршрутизаторы являются точками, в которых определяются пути прохождения данных

В двухуровневой иерархии распределенной сети, которая показана на рис. 9.9, поток данных проходит вверх по иерархической структуре только расстояние, необходимое для того, чтобы найти пункт назначения, сохраняя тем самым полосу пропускания каналов распределенной сети.

Место расположения сервера

Известно, что размещение сервера связано с расположением пользователей, имеющих к этому серверу доступ. По этой причине место расположения сервера значительно влияет на структуру потока данных в распределенной сети. Если разместить сервер предприятия на уровне доступа участка 1, как показано на рис. 9.10, то весь поток данных вынужденно направится по каналам между маршрутизаторами 1 и 2. Это займет значительную часть полосы пропускания участка 1.

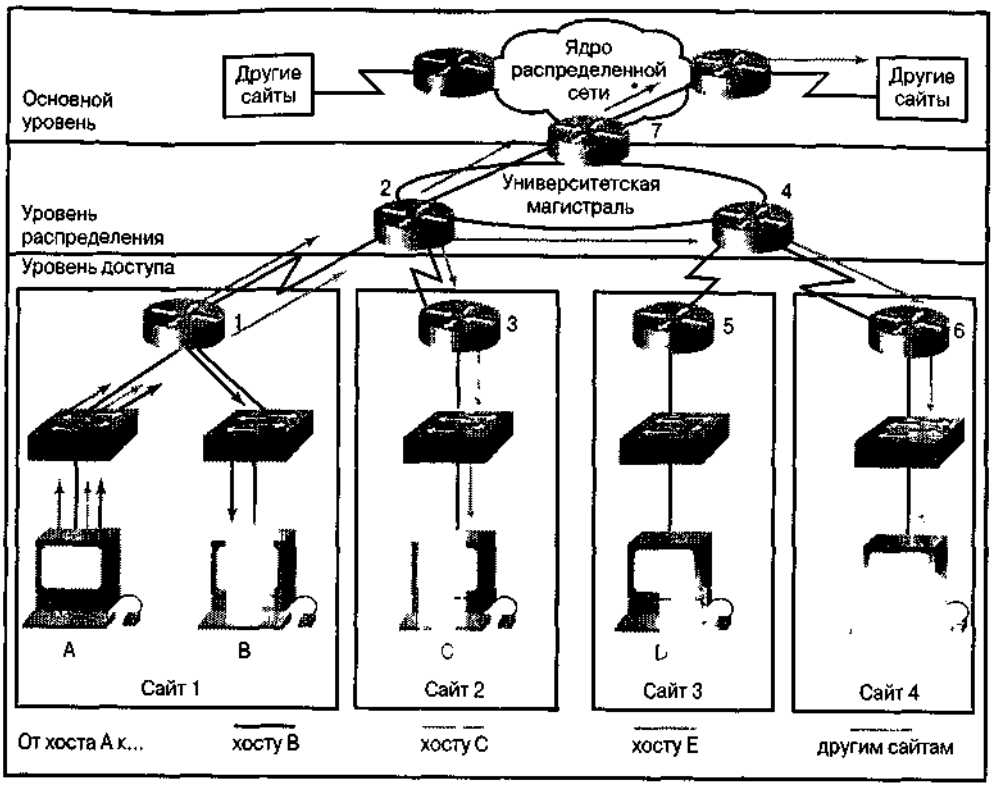


Рис. 9.8. Поток данных следует вверх по иерархии, основываясь на адресах источника и/или пункта назначения

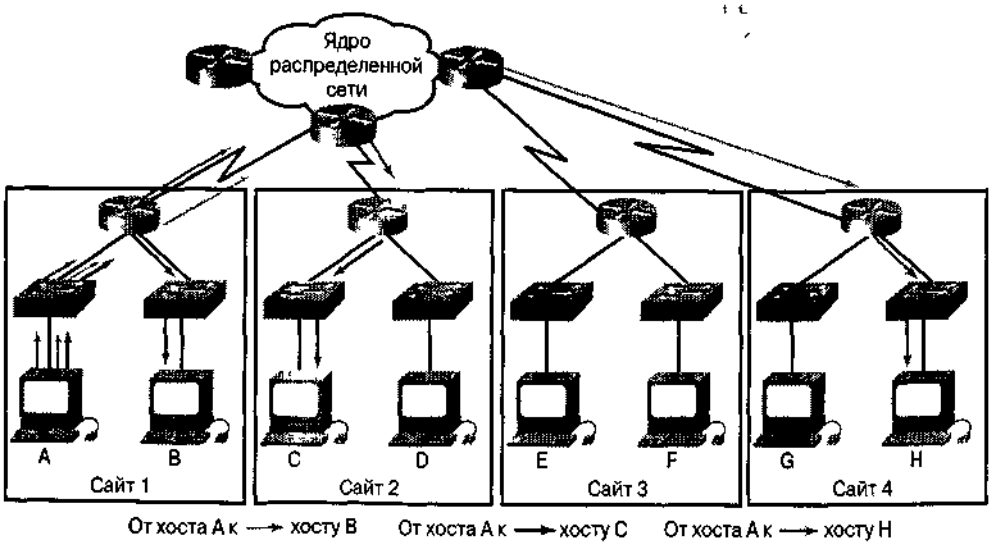


Рис. 9 9. Структура потока данных в двухуровневой иерархии распределенной сети определяется адресами хостов источника и пункта назначения, а также маршрутизатором, который определяет путь прохождения пакетов

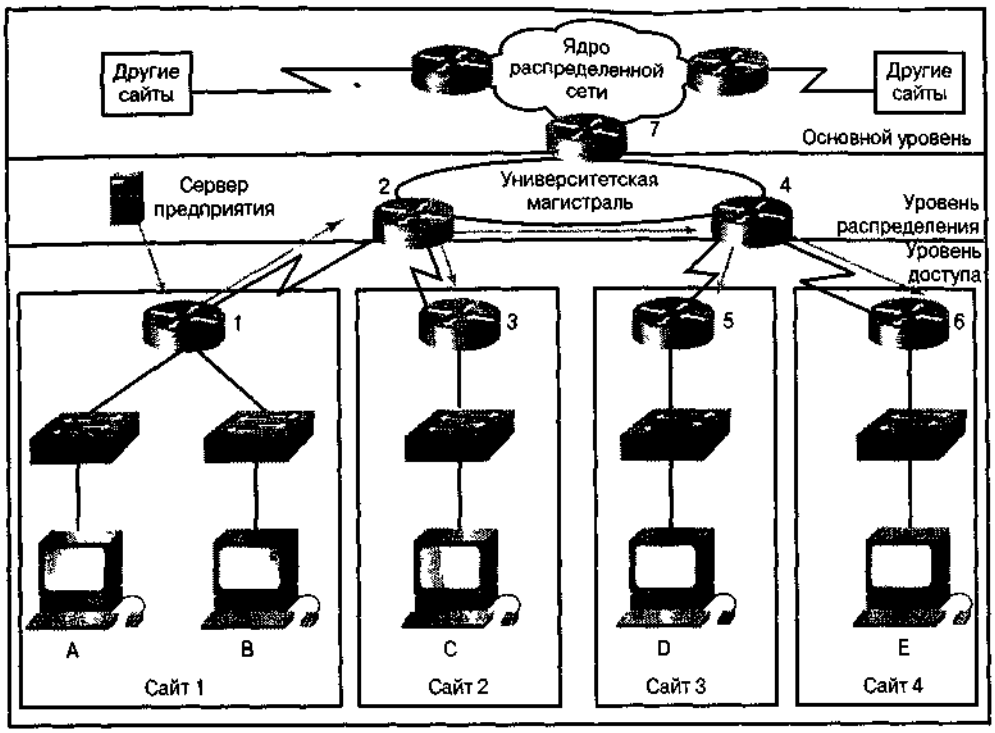


Рис 9 10 Излишний поток данных занимает полосу пропускания Сервер размещен неверно, что и привело к генерации ненужного потока данных

Если разместить сервер предприятия на более высоком уровне в иерархии, как показано на рис 9 11, то поток данных в канале между маршрутизаторами 1 и 2 уменьшится, что даст возможность пользователям участка 1 воспользоваться другими службами На рис 9 12 сервер рабочей группы расположен на уровне доступа участка, где плотность пользователей наибольшая, и поток данных, направляющийся по каналам распределенной сети к этому серверу, ограничен. Таким образом, для доступа к ресурсам за пределами участка предоставляется большая полоса пропускания.

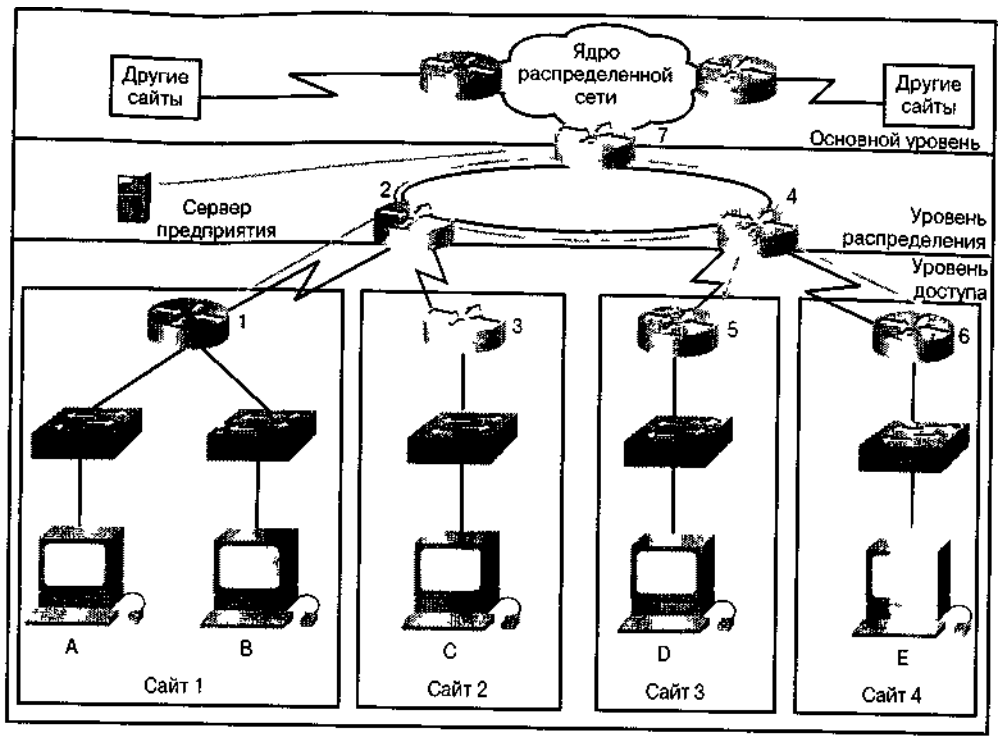


Рис 9 11 Перемещение сервера в правильно выбранную точку освобождает полосу пропускания

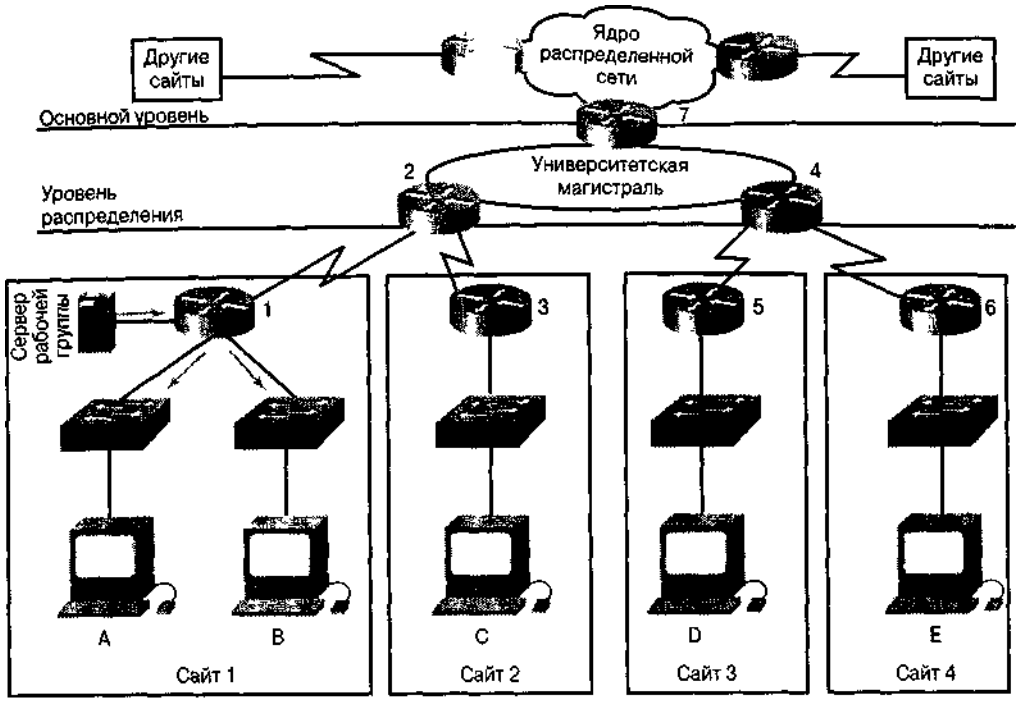


Рис 9 12 Размещение серверов должно основываться на потребностях пользователей

Протокол Frame Relay и каналы ISDN в распределенной сети

Довольно часто для доступа из удаленных участков к основному уровню распределенной сети применяются технологии, отличные от выделенных линий. Как показано 9 на рис. 9.13, протокол Frame Relay и ISDN представляют собой две такие альтернативы. Если удаленный участок небольшой и его потребность в доступе к корпоративной сети невелика, то в этом случае целесообразно применение ISDN. Предположим, что другой удаленный участок не может получить доступ к выделенным каналам распределенной сети через своего провайдера, но у него есть доступ к сети Frame Relay. В любом случае необходима точка входа этих типов соединений на магистраль распределенной сети. Точки входа следует устанавливать на маршрутизаторе, который непосредственно связан с этой магистралью. Это позволит удаленным участкам получить полный доступ к сети предприятия без дополнительной генерации излишнего потока данных к другим участкам.

Вашингтонский проект: канал Frame Relay

Для обеспечения доступа к Internet и другим внешним сетевым соединениям через офис Вашингтонского учебного округа следует использовать канал Frame Relay В целях безопасности необходимо запретить другие виды соединений.

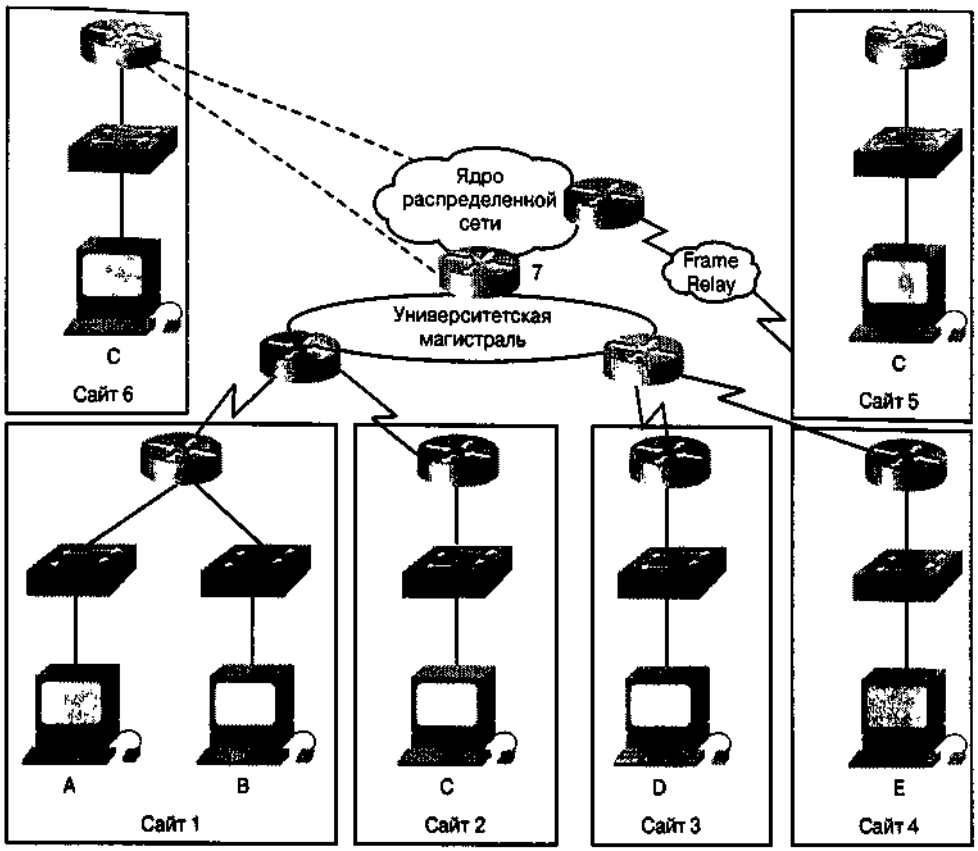


Рис. 9.13. Для доступа к основной магистрали распределенной сети могут использоваться различные технологии распределенных сетей

Резюме

- Проектирование распределенной сети включает в себя сбор и анализ требований, таких как доступность и сетевая нагрузка.
- Легче всего поддается расширению иерархическая модель распределенной сети, в которой каждый из уровней выполняет определенную функцию.
- Иерархическая модель состоит из основного уровня, уровня распределения и уровня доступа.
- Распределенные сети предприятий могут использовать несколько различных технологий, таких как Frame Relay и ISDN.
- Для управления структурой потока данных в распределенной сети особенно важным является вопрос размещения серверов.

Задачи проекта Вашингтонского учебного округа: проектирование распределенной сети

В настоящей главе рассказывалось о процессе проектирования распределенной сети. Изложенный материал позволяет объединить все подразделения Вашингтонского учебного округа в единую распределенную сеть, которая удовлетворит требования всех е пользователей. При этом

необходимо решить следующие задачи.

1. Создать проект распределенной сети, включающий в себя следующее:

   - скорости каналов распределенной сети и путь обновления;
   - модель движения потока данных между школами для двух- или трехуровневой иерархии распределенной сети;
   - список дополнительного оборудования, такого как CSU/DSU и интерфейсы маршрутизатора, необходимого для реализации распределенной сети округа;
   - список дополнительного (резервного) оборудования, необходимого для обеспечения гарантированной продолжительности работы распределенной сети.

(Совет: рекомендуется обратиться к техническим требованиям проекта Вашингтонского учебного округа.)

2. Записать все команды, необходимые для установки новой конфигурации маршрутизаторов при реализации распределенной сети.
3. Зафиксировать в технической документации влияние распределенной сети на обмен маршрутной информацией между маршрутизаторами.

Контрольные вопросы

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

1. Что из перечисленного ниже является первой задачей при проектировании распределенной сети?
   - A. Определить, требуется ли доступ к данным за пределами компании.
   - B. Определить, кто, с точки зрения заказчика, будет вовлечен в разработку проекта.
   - C. Определить, где находятся и кем используются данные, предоставленные для совместного доступа.
   - D. Все перечисленное.

2. В какой момент времени следует проверить наибольший объем потока данных в сети при анализе требований, касающихся сетевой нагрузки?
   - A. Во время наибольшей загруженности сети.
   - B. Во время наименьшей загруженности сети.
   - C. Во время резервного копирования.
   - D. По окончании рабочего времени.

3. Где в распределенной сети следует размешать серверы приложений?
   - A. В корпоративной магистрали.
   - B. В непосредственной близости от пользователя
   - C. Рядом с точкой присутствия.
   - D. На усмотрение проектировщика.

4. Что из перечисленного ниже не является преимуществом иерархической модели проектирования?
   - A. Расширяемость.
   - B. Простота реализации.
   - C. Простая топология.
   - D. Простота устранения неисправностей.

5. В чем (в большинстве случаев) заключается главная задача при проектировании основного уровня?
   - A. Эффективное использование полосы пропускания.
   - B. Обеспечение доступа рабочих групп.
   - C. Размещение сервера.
   - D. Размещение сервера предприятия.

6. Какое из перечисленных ниже устройств следует размещать в сетевой магистрали?
   A. Сервер.
   B. Маршрутизаторы.
   C. Рабочие станции.
   D. Серверы приложений.
7. На каком уровне происходит подключение пользователей к локальной сети?
   A. Уровень рабочих групп.
   B. Основной уровень.
   C. Уровень доступа.
   D. Уровень распределения.
8. На каком уровне происходит подключение локальной сети к каналу распределенной сети?
   A. Уровень распределения.
   B. Уровень рабочих групп.
   C. Основной уровень.
   D. Уровень доступа.
9. Размещение какого устройства является наиболее важным вопросом при одноуровневом проектировании?
   A. Сервера.
   B. Маршрутизатора.
   C. Рабочей станции.
   D. Коммутатора.
10. В случае двухуровневого проектирования какое устройство используется для разделения локальной сети на отдельные широковещательные домены?
   A. Коммутатор.
   B. Маршрутизатор.
   C. Концентратор.
   D. Повторитель.

Основные термины

T1. Цифровой носитель в распределенной сети, который передаёт данные в формате DS-1 со скоростью 1,544 Мбит/с по коммутируемой телефонной сети, используя кодирование AMI или B8ZS.

T3. Цифровой носитель в распределенной сети, который передает данные в формате DS-3 со скоростью 44,736 Мбит/с по коммутируемой телефонной сети.

Выделенная линия (leased line). Линия передачи, зарезервированная поставщиком коммуникационных услуг для частного использования заказчиком. Является подтипом выделенного канала.

Выделенный канал (dedicated link). Коммуникационный канал, зарезервированный для передачи на неопределенное время. Такой канал качественно отличается от канала, коммутируемого при появлении необходимости в передаче данных.

Канал (link). Сетевой канал связи, состоящий из линии или пути передачи данных от отправителя к получателю и соответствующего оборудования. Этот термин наиболее часто употребляется в контексте распределенной сети. Иногда называется линией или каналом передачи данных.

Канал распределенной сети (WAN **link).** Коммуникационный канал распределённой сети, состоящий из линии или пути передачи данных от отправителя к получателю и соответствующего оборудования.

Коммутация каналов (circuit switching). Система коммутации, при которой во время сеанса связи должен существовать физический канал между отправителем и получателем. Широко используется в сетях телефонных компаний. С технологической точки зрения коммутацию каналов можно рассматривать как противоположность коммутации пакетов и сообщений, а с точ-

ки зрения методов доступа — как противоположность конкуренции и передаче маркеров.

Коммутация пакетов (packet switching). Сетевая технология, при которой узлы совместно используют полосу пропускания путем передачи пакетов данных.

Основной уровень (core layer) . Уровень, который обеспечивает быстрое соединение между географически удаленными точками, соединяя несколько локальных сетей в распределённую сеть корпорации или предприятия.

Протокол ретрансляции фреймов (Frame Relay). Стандартный промышленный коммутируемый протокол канального уровня, который поддерживает несколько виртуальных каналов связи между соединенными устройствами, используя HDLC-инкапсуляцию. Протокол Frame Relay является более эффективным, чем X.25, и в целом рассматривается в качестве его замены.

Сеть предприятия (enterprise network). Сеть предприятия, агентства, школы или другой организации, объединяющая их данные, коммуникации, вычислительные мощности и файловые серверы.

Уровень доступа (access layer). Уровень, на котором локальная сеть или группа локальных сетей, обычно Ethernet или Token Ring, обеспечивают пользователю прямой доступ к сетевым службам.

Уровень распределения (distribution layer). Уровень, на котором происходит распределение сетевых служб для отдельных локальных сетей, входящих в распределённую сеть. На этом уровне обычно находится магистраль распределённой сети. Обычно основывается на Fast Ethernet.

Цепь (circuit). Коммуникационный путь между двумя или более точками.

Ключевые темы этой главы

- Определены и описаны основные компоненты, используемые протоколом PPP ("point-to-point", "точка-точка").
- Описано использование протоколом PPP LCP- и NCP-фреймов
- Объясняется, как настроить параметры протокола PPP и проверить качество его работы.
- Описан и объяснен процесс аутентификации в протоколе PPP
- Описано использование протокола CHAP

Глава 10

Протокол PPP

Введение

В главе 8, "Распределенные сети", были описаны технологии создания распределенных сетей. В настоящей главе описаны соединения распределенных сетей, управляемые протоколами, основные функции которых совпадают с теми, которые выполняли протоколы 2-го уровня для локальных сетей, таких как Ethernet. В среде локальных сетей для обеспечения доставки данных при их перемещении между двумя узлами или маршрутизаторами требовалось выбрать путь для данных и привести в действие прои*- ">ы управления потоком данных. Аналогичным образом обстоит дело и в расг еденных сетях, где используются соответствующие протоколы распределенных и.

В настоящей главе описаны основные компоненты, процессы и операции, определяющие функционирование **протокола PPP ("точка-точка", Point-to-Point Protocol, PPP)** Кроме того, в этой главе обсуждается использование фреймов, созданных **в протоколе управления каналом (Link Control Protocol, LCP) и в протоколе управления сетью (Network Control Protocol)** В заключение будет описана процедура настройки параметров и проверки качества работы протокола PPP. Наряду с процедурой аутентификации PPP будут рассмотрены **протокол аутентификации паролем (Password Authentication Protocol, PAP) и протокол аутентификации с предварительным согласованием вызова (Challenge Handshake Authentication Protocol, CHAP).**

Вашингтонский проект: применение протокола PPP

В главе 8, "Распределенные сети", был описан процесс проектирования распределенных сетей и разработан проект распределенной сети Вашингтонского учебного округа, позволяющей устанавливать связь между всеми участками округа. Поскольку в распределенных сетях отсутствует протокол 2-го уровня, такие физические сети не имеют механизмов для передачи данных и управления потоком. В настоящей главе описано применение PPP в качестве протокола канального уровня, который можно будет использовать в распределенной сети округа

Общие сведения о протоколе PPP

В конце 80-х годов сложилась ситуация, при которой использование протокола SLIP (Serial

Line Internet Protocol, протокол Internet для последовательного канала) стало тормозить рост сети Internet. Протокол PPP был создан для решения проблем установки удаленной связи с Internet. Кроме того, протокол PPP был нужен для динамического назначения IP-адресов и обеспечения возможности использования нескольких протоколов сетевого уровня. Этот протокол обеспечивает установку соединений между маршрутизаторами и подсоединение хоста к сети как по синхронным, так и по асинхронным каналам (рис. 10.1).

Протокол PPP является наиболее популярным среди протоколов распределенных сетей и используется чаще всех остальных, поскольку он обеспечивает проектировщику сети следующие возможности:

- управление каналом данных;
- назначение IP-адресов и управление ими;
- мультиплексирование сетевого протокола;
- установку параметров канала и тестирование качества его работы;
- обнаружение ошибок;
- выбор дополнительных возможностей, таких как согласование адреса сетевого уровня и необходимости сжатия данных.

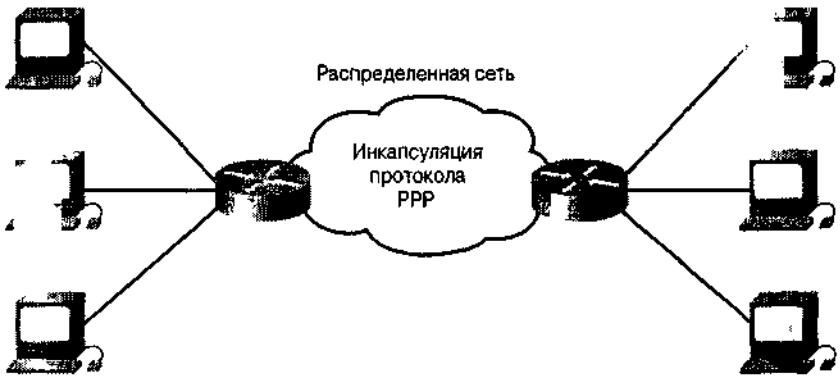


Рис. 10.1. Протокол PPP обеспечивает надежное соединение между маршрутизаторами

Компоненты протокола PPP

Для решения проблем установки связи с Internet протокол PPP использует три основных компонента, перечисленные ниже.

- Метод инкапсуляции дейтаграмм при передаче их по последовательным каналам. Протокол PPP использует в качестве основы при инкапсуляции дейтаграмм в каналах типа "точка-точка" протокол HDLC (High-Level Data Link Control, управление высокого уровня каналом связи).
- Протокол LCP для установки, конфигурирования и тестирования соединения на канальном уровне.
- Семейство протоколов NCP для установки и конфигурирования различных протоколов сетевого уровня. При проектировании протокола PPP ставилась задача обеспечить возможность использования нескольких протоколов сетевого уровня. В настоящее время протокол PPP поддерживает, кроме протокола IP, другие протоколы, в частности протокол межсетевого обмена пакетами (Internetwork Packet Exchange, IPX) и протокол DECNet. Как показано на рис. 10.2, протокол PPP использует свой компо-

нент NCP для инкапсуляции различных протоколов.

Рис. 10.2. Используя NCP, протокол PPP может передавать пакеты различных протоколов

Функции PPP различных уровней

Протокол PPP использует уровневую архитектуру, как показано на рис. 10.3. Его функции нижнего уровня позволяют использовать:

- синхронную передающую среду, аналогичную той, которая соединяет между собой подсети цифровой сети интегрированных служб (Integrated Services Digital Network), описанной в главе 11, "ISDN — цифровая сеть интегрированных служб";
- асинхронную передающую среду, подобную той, которую используют базовые телефонные службы для установки связи через модем.

Используя свои функции верхнего уровня, протокол PPP переносит пакеты из нескольких протоколов сетевого уровня в NCP. Эти протоколы верхнего уровня включают в себя:

- BCP — протокол управления мостом (Bridge Control Protocol);
- IPCP — протокол управления работой в Internet (Internet Protocol Control Protocol);
- IPXCP — протокол управления межсетевым обменом пакетов (Internetwork Packet Exchange Control Protocol).

Стандартизованные коды этих протоколов вводятся в функциональное поле для указания типа протокола, который PPP будет использовать при инкапсуляции данных.

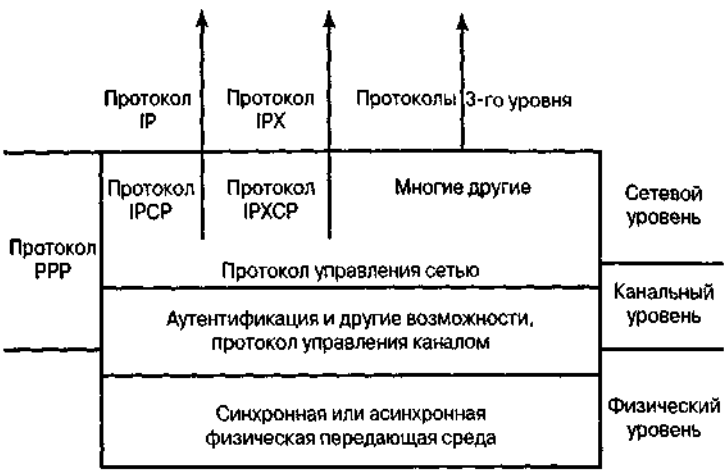


Рис. 10.3. Протокол PPP представляет собой протокол канального уровня со службами сетевого уровня

Форматы фреймов протокола PPP

Как показано на рис. 10.4, фрейм протокола PPP включает в себя следующие поля.

- *Флаг.* Указывает на начало или конец фрейма и представляет собой двоичную последовательность 01111110.
- *Адрес*. Состоит из стандартных широковещательных адресов, представляющих собой двоичную последовательность, состоящую из всех единиц (11111111). Протокол PPP не назначает станциям индивидуальные адреса.
- *Управление.* Один байт, содержащий последовательность двоичных чисел 00000011, которая вызывает передачу данных пользователя, находящихся в неупорядоченном фрейме. При этом обеспечивается канальная связь без установки соединения, аналогичная связи протокола управления логическим каналом **(Logical Link Control, LLC)** первого типа.
- *Протокол.* Два байта, которые идентифицируют тип протокола пакета, инкапсулированного в поле данных фрейма.
- *Данные*. Ноль или больше байтов, которые содержат дейтаграмму протокола, указанного в поле протокола. Конец поля данных устанавливается путем поиска последовательности закрывающего флага и выделения двух байтов для контрольной последовательности фрейма. По умолчанию максимальная длина поля данных равна 1500 байтов.
- *FCS.* Обычно состоит из 16 битов (2 байта). Относится к дополнительным символам, добавляемым к фрейму для обнаружения ошибок.

Размер поля в байтах	1	1	1	1	Поле переменной	2 или 4
	Поле флага	Поле адреса	Поле управления	Поле протокола	Поле данных	FCS

Рис. 10.4. Протокол PPP использует фреймовую структуру HDLC-процедур Международной организации стандартизации (International Organization for Standardization, ISO)

Установка сеанса связи в протоколе PPP

Протокол PPP предоставляет средства для установки, конфигурирования, поддержки и прекращения работы соединения типа "точка-точка". При установке связи по каналу типа "точка-точка" последовательно проходятся следующие четыре различных стадии.

1. *Создание канала и согласование конфигурации.* Первичный узел протокола PPP посы лает LCP-фреймы для конфигурирования и тестирования канала передачи данных.

2. *Проверка качества работы канала.* Канал устанавливается и согласовываются его параметры. Отметим, что эта стадия не является обязательной.

3. *Согласование конфигурации протокола сетевого уровня*. Первичный узел прото кола PPP рассылает NCP-фреймы для выбора и установки конфигурации про токолов сетевого уровня, таких как TCP/IP, Novell IPX и AppleTalk. Только по сле этого могут пересылаться пакеты указанных протоколов сетевого уровня.

4. *Окончание работы канала*. Конфигурация канала связи сохраняется до тех пор, пока LCP- или NCP-фреймы не закроют канал, или до какого-либо внешнего события (например, истечения времени таймера простоя или вмешательства пользователя).

Используются три типа LCP-фреймов.

- *Фреймы установки канала связи*. Используются для создания и конфигурирования канала.
- *Фреймы закрытия канала*. Используются для прекращения работы канала.
- *Фреймы поддержки работы канала*. Используются для отладки канала и для управления им.

LCP-фреймы используются на всех четырех стадиях работы протокола LCP, описанных в последующих разделах.

Стадия 1. Создание канала и согласование его параметров

На стадии создания канала и согласования его параметров каждое устройство PPP рассылает LCP-пакеты для конфигурирования и тестирования канала связи. Пакеты LCP содержат поле дополнительных параметров конфигурации, которое позволяет согласовать использование опций, таких как максимальная величина принимаемого модуля, сжатие некоторых полей PPP или протокол аутентификации канала. Если в пакет LCP не включена некоторая опция конфигурации, то для нее принимается значение по умолчанию.

До передачи дейтаграмм сетевого уровня (например, IP-дейтаграмм), протокол LCP должен установить связь и согласовать параметры конфигурации. Эта стадия заканчивается после отправки фрейма запроса на подтверждение конфигурации и получения соответствующего ответа.

Стадия 2. Проверка качества работы канала

Протокол LCP позволяет выполнить необязательную проверку качества работы канала после его создания и согласования параметров конфигурации. На этой стадии канал тестируется с целью выяснения, обеспечивает ли он достаточное качество для работы протоколов сетевого уровня.

Кроме того, после установки связи и принятия решения о протоколе аутентификации можно проверить подлинность клиента или рабочей станции. Проверка подлинности, если она выполняется, происходит до того, как начнется настройка параметров протоколов сетевого уровня. LCP может задержать передачу информации протокола сетевого уровня до окончания этой стадии.

PPP поддерживает два протокола аутентификации: PAP и CHAP. Оба эти протокола подробно описаны в спецификации RFC 1334. Они также описаны в одном из следующих разделов этой главы.

Стадия 3. Согласование параметров протокола сете-

вого уровня

После того как протокол LCP заканчивает проверку качества работы канала, протоколы сетевого уровня могут быть отдельно сконфигурированы соответствующими NCP-фреймами и включены и выключены в любой момент времени.

На этой стадии устройства PPP рассылают пакеты NCP для выбора и конфигурирования одного или нескольких протоколов сетевого уровня (таких как IP). После того как установлены параметры конфигурации всех выбранных протоколов сетевого уровня, от каждого из них по каналу могут быть отправлены дейтаграммы. Если LCP закрывает какой-либо из каналов, то об этом информируются все остальные протоколы сетевого уровня, которые могут в этом случае предпринять соответствующие действия. После того как произведена настройка параметров протокола PPP, проверка состояния LCP и NCP может быть выполнена с помощью команды show interfaces.

Стадия 4. Закрытие канала

Протокол LCP может закрыть канал в любое время. Обычно это делается по запросу пользователя, но может также произойти вследствие некоторого физического события, например в связи с повреждением носителя или истечением заданного промежутка времени.

Вашингтонский проект: задание PPP-инкапсуляции

Протокол PPP может применяться на последовательных линиях для инкапсуляции дейтаграмм протокола IP или других протоколов сетевого уровня. Для этого в режиме установки конфигурации интерфейса необходимо выполнить команду encapsulation ppp.

- Войти в режим установки конфигурации для требуемого интерфейса.
- Сконфигурировать интерфейс для PPP-инкапсуляции:

```
Router(config)#   encapsulation ppp
```

Аутентификация сеанса PPP

Как было сказано ранее, стадия аутентификации сеанса PPP не является обязательной. После установления связи и принятия решения о протоколе аутентификации может быть выполнена проверка подлинности другой стороны, участвующей в сеансе связи. Если такая проверка выполняется, то она проводится до начала установки параметров конфигурации протокола сетевого уровня.

Опции аутентификации требуют, чтобы вызывающая сторона канала ввела информацию по проверке подлинности, которая позволит убедиться, что данный пользователь имеет разрешение сетевого администратора на вход в сеть. Маршрутизаторы одного ранга обмениваются сообщениями об аутентификации.

При настройке параметров аутентификации протокола PPP можно выбрать проверку с помощью протоколов PAP или CHAP. Как правило, предпочтение отдается протоколу CHAP. Ниже кратко описаны эти два протокола.

- *Протокол PAP*. Как показано на рис. 10.5, PAP предоставляет удаленному узлу простой способ подтвердить свою идентичность путем использования двухэтапного квитирования (handshake). После того как стадия создания PPP-канала закончена, удаленный узел регулярно посылает по каналу имя пользователя и его пароль до тех пор, пока идентичность не будет подтверждена или канал не будет закрыт.

  Протокол PAP не является строгим протоколом аутентификации. Пароли передаются по каналу в виде открытого текста, и отсутствует защита от повторного воспроизве-

дения или повторных атак с целью случайным образом пробиться в сеть. Однако попытки подключения, их частота и время регистрируются удаленным узлом.

- *Протокол CHAP.* Протокол CHAP используется для периодической проверки подлинности удаленного узла с использованием метода трехэтапного квитирования, как показано на рис. 10.6. Такая проверка осуществляется после создания первоначального канала и может быть повторена в любой момент времени. Для обеспечения безопасности протокол CHAP позволяет выполнять такую проверку регулярно, что делает его более эффективным, чем PAP. Протокол PAP выполняет такую проверку только один раз, что делает его уязвимым перед атакой хакеров или воспроизведением сигналов модема. Кроме того, PAP позволяет вызывающей стороне попытаться пройти проверку подлинности по своему желанию (без предварительного вызова), что делает его уязвимым перед прямолинейной попыткой проникнуть в сеть, в то время как CHAP не позволяет вызывающей стороне пытаться пройти проверку подлинности без предварительного вызова.

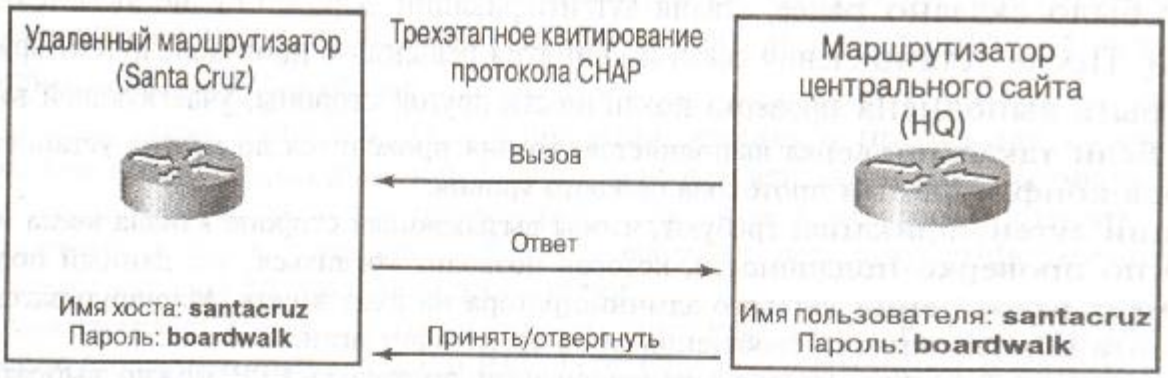


Рис. 10.6. Протокол CHAP используется при создании канала и регулярно после этого для проверки подлинности удаленного узла путем трехэтапного квитирования

После создания канала PPP хост посылает сообщение о вызове на удаленный узел. Удаленный узел посылает в ответ соответствующее значение. Хост сравнивает его с имеющимся у него значением и, если они совпадают, подлинность подтверждается. В противном случае связь прекращается.

Протокол CHAP обеспечивает защиту от атак повторного воспроизведения путем использования значения переменной вызова, которое уникально и непредсказуемо. Повторные вызовы применяются для уменьшения до минимума периода уязвимости при попытке несанкционированного входа в сеть. Локальные маршрутизаторы (или серверы проверки аутентичности, такие, например, как коммерческий сервер Netscape) фиксируют частоту и время поступления вызовов.

Настройка параметров аутентификации протокола

PPP

Для настройки параметров аутентификации протокола PPP необходимо выполнить следующие действия.

Этап 1. На каждом маршрутизаторе необходимо задать имя и пароль пользователя, которые ожидаются от удаленного маршрутизатора:

Router (config) # **username** имя **password** *пароль*

Параметры команды имеют следующее значение:

- *имя* — имя хоста или удаленного маршрутизатора; следует обратить внимание на то, что символы имени чувствительны к регистру;
- *пароль* — при использовании маршрутизаторов Cisco пароль должен быть одинаковым для обоих маршрутизаторов.

Инженерный журнал: добавление имени пользователя

Каждой удаленной системе, с которой локальный маршрутизатор поддерживает связь, и от которой требует подтверждения аутентичности, следует сообщить имя пользователя. Удаленное устройство должно также быть "прописано" на локальном маршрутизаторе.

Для того чтобы локальный маршрутизатор мог ответить на вызов удаленного CHAP, имя пользователя должно совпадать с именем хоста, которое уже было назначено устройству. При использовании протокола CHAP следует использовать пароли, которые известны только пользователю и соответствующему устройству.

Этап 2. Необходимо войти в режим установки конфигурации требуемого интерфейса.

Этап 3. Необходимо установить PPP-тип инкапсуляции на этом интерфейсе:

```
Router(config-if)#  encapsulation ppp
```

Этап 4. Следует задать режим аутентификации протокола PPP:

```
Router(config-if)# ppp authentication {chap | chap pap | pap chap | pap }
```

Этап 5. Если включены CHAP и PAP, то первый из указанных методов используется на стадии согласования параметров канала. Если партнер по связи предлагает использовать второй метод или просто отказывается использовать первый метод, то делается попытка использовать второй из указанных методов.

Этап 6. В версии операционной системы Cisco 11.1 ив более поздних при выборе PAP и конфигурировании маршрутизатора, который будет посылать информацию PAP (иными словами, маршрутизатора, отвечающего на запрос PAP), необходимо установить PAP для данного интерфейса. По умолчанию он отключен; для его включения необходимо выполнить команду:

```
Router (config-if )# ppp pap sent-username имя password пароль
```

Настройка параметров аутентификации протокола CHAP

Для упрощения настройки параметров конфигурации протокола CHAP на маршрутизаторе можно использовать следующие методы.

- Можно использовать одно и то же имя хоста для различных маршрутизаторов. Если желательно, чтобы удаленные пользователи при проверке подлинности полагали, что

они подсоединены к одному и тому же маршрутизатору, то следует использовать одно и то же имя хоста на всех маршрутизаторах:

```
Router (config-if )# ppp chap hostname имя
```

- Для проверки подлинности неизвестного хоста может быть использован пароль. Для уменьшения количества строк типа "имя пользователя — пароль" на маршрутизаторе следует задать пароль, который будет послан на все хосты, желающие проверить его подлинность:

  Router(config-if)# **ppp chap password** *пароль*

Этот пароль не используется, когда маршрутизатор проводит проверку подлинно-; сти удаленного устройства.

Резюме

- Протокол PPP является часто используется в распределенных сетях.
- Протокол PPP решает вопросы установки связи посредством LCP и семейства протоколов NCP, с помощью которых согласовываются параметры конфигурации и используемые устройства.
- Сеанс работы протокола PPP состоит из следующих четырех стадий:
- установка связи;
- анализ качества работы канала;
- конфигурирование протокола сетевого уровня;
- окончание работы канала.
- При конфигурировании процедур проверки подлинности протокола PPP можно выбрать протокол PAP или CHAP.
- Протокол PAP не является строгим протоколом проверки аутентичности.
- Протокол CHAP обеспечивает защиту от попыток повторного воспроизведения путем использования значения переменной вызова, которое является уникальным и непредсказуемым.
- Конфигурация интерфейса для PPP-инкапсуляции может быть установлена командой encapsulation ppp.
- После того как параметры протокола PPP установлены, состояние его LCP и NCP может быть проверено командой show interfaces.

Задачи проекта Вашингтонского учебного округа: протокол PPP

В настоящей главе были описаны основные понятия и процесс конфигурирования, которые помогают задать параметры конфигурации сети Вашингтонского учебного округа. Установка параметров конфигурации включает в себя, в частности, решение следующих задач.

- Применение протокола PPP в существующем проекте распределенной сети.
- Занесение в соответствующие учетные документы изменений в конфигурации маршрутизаторов, сделанных при установке на них протокола PPP.

- Запись команд маршрутизатора, необходимых для реализации PPP на интерфейсах маршрутизаторов.

Контрольные вопросы

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

1. Наследником какого протокола считается протокол PPP?
2. Какие физические интерфейсы поддерживает протокол PPP?
3. Какой из перечисленных ниже протоколов сетевого уровня поддерживается протоколом PPP?
   A. Novell IP.
   B. TCP/IP.
   C. AppleTalk.
   D. Все перечисленные.
4. Для выполнения какого из перечисленных ниже действий протоколом PPP ис пользуется NCP?
   A. Создание канала.
   B. Мультипротокольная инкапсуляция.
   C. Конвертирование пакетов в ячейки.
   D. Установка соединений.
5. Какое поле фрейма PPP указывает на использование для инкапсуляции прото кола IPX или TCP/IP?
   A. Поле флага.
   B. Поле управления.
   C. Поле протокола.
   D. Поле FCS.
6. За что из перечисленного ниже отвечает LCP при использовании протокола PPP?
   A. Установка, поддержание и прекращение связи типа "точка-точка".
   B. Поддержка нескольких каналов.
   C. Обновление маршрутной информации.
   D. Сжатие данных.
7. Сколько стадий включает в себя установка сеанса связи PPP?
   A. Одну.
   B. Две.
   C. Три.
   D. Четыре.
8. Какой тип квитирования используется в том случае, когда в качестве протокола проверки подлинности выбран PAP?
   A. Одностороннее.
   B. Двустороннее
   C. Трехстороннее.
   D. Четырехстороннее.
9. Какую команду маршрутизатора следует использовать для проверки состояния LCP и NCP?
   A. `Router>show interfaces`
   B. `Router(config)# show interfaces`
   C. `Router# show interfaces`
   D. `Router(config-if)# show interfaces`
10. В каком из перечисленных ниже случаев наиболее вероятно использование на локальной рабочей станции протокола PPP для выхода в Internet?
    A. Когда рабочая станция непосредственно подсоединена к локальной сети.
    B. Когда рабочая станция непосредственно подсоединена к маршрутизатору.

C. Когда рабочей станции требуется доступ в Internet по коммутируемому каналу связи.
D. Протокол PPP никогда не используется на рабочих станциях.

Основные термины

Serial Line Internet Protocol (протокол Internet для последовательного канала, SLIP). Стандартный протокол последовательных соединений типа "точка-точка" с использованием различных вариантов протоколов TCP/IP. Предшественник PPP.

Асинхронный канал (asynchronous circuit). Канал, по которому сигналы передаются без точной синхронизации. Такие сигналы обычно имеют различные частоты и фазы. При асинхронной передаче отдельные символы обычно инкапсулируются в управляющие биты (называемые битами начала и остановки), которые указывают на начало и конец каждого символа.

Протокол аутентификации паролем (Password Authentication Protocol, PAP). Протокол проверки подлинности, который позволяет устройствам одного ранга распознать друг друга. От удаленного маршрутизатора, который пытается подсоединиться к локальному маршрутизатору, требуется, чтобы он послал запрос на проверку подлинности. В отличие от CHAP, PAP передает пароль, имя хоста или имя пользователя в виде открытого текста (т.е. незашифрованным). Сам по себе PAP не предотвращает несанкционированный доступ, но идентифицирует пункт назначения; после этого маршрутизатор или сервер доступа определяет, разрешен ли доступ данному пользователю. PAP поддерживается только на линиях PPP.

Протокол аутентификации с предварительным согласованием вызова (Challenge Handshake Authentication Protocol, CHAP). Средство обеспечения безопасности, которое предотвращает несанкционированный доступ за счет использования инкапсуляции PPP. Сам по себе CHAP не предотвращает несанкционированный доступ, но идентифицирует удаленный пункт назначения; после этого маршрутизатор или сервер доступа определяет, разрешен ли доступ данному пользователю.

Протокол логического канала (logical link protocol, LLC). Верхний из двух подуровней канального уровня, определенных ШЕЕ. Подуровень LLC выполняет контроль ошибок, управление потоком, создание фреймов и адресацию MAC-подуровня. Наиболее часто используется LLC-протокол IEEE 802.2, который существует в двух вариантах: с установлением соединения и без него.

Протокол типа "точка-точка" (Point-to-point Protocol, PPP). Разработанный как замена протокола SLIP, протокол PPP обеспечивает соединение между маршрутизаторами и соединение хоста с сетью по синхронным и асинхронным каналам.

Протокол управления каналом (Link Control Protocol, LCP). Протокол, обеспечивающий средства установки, поддержки и окончания соединения типа "точка-точка"

Протокол управления сетью (Network Control Protocol, NCP). Протокол, осуществляющий маршрутизацию и управление потоком данных между коммуникационным контроллером и другими сетевыми ресурсами.

Синхронный канал (synchronous circuit). Канал, по которому сигналы передаются в режиме синхронизации. Такие сигналы имеют одну и ту же частоту. При синхронной передаче отдельные символы инкапсулируются в управляющие биты (называемые битами начала и остановки), которые указывают на начало и конец каждого символа.

Ключевые темы этой главы

- Описывается технология ISDN и ее компоненты
- Описываются стандарты ISDN
- Описывается инкапсуляция ISDN
- Описывается использование ISDN
- Описываются интерфейс базовой скорости (Basic Rate Interface, BRI) и интерфейс первичной скорости (Primary Rate Interface, PRI)
- Рассматриваются задачи установки конфигурации ISDN
- Описывается маршрутизация с предоставлением канала по запросу (dial-on demand routing)

Глава 11

ISDN — цифровая сеть интегрированных служб

Введение

Для решения проблем связи компаний, которым необходим доступ к географически удаленным подразделениям, могут применяться различные типы технологий распределенных сетей. В главе 10, "Протокол PPP", был описан протокол "точка-точка" (pomt-to-point, PPP) В настоящей главе будут описаны службы, стандарты, компоненты, принцип действия и конфигурация цифровой сети интегрированных служб (Integrated Services Digital Network, ISDN) ISDN специально разрабатывалась для решения проблем небольших офисов или пользователей с коммутируемым доступом, которые нуждались в большей полосе пропускания, чем та, которая предоставлялась традиционными телефонными службами. В настоящее время ISDN также предоставляет резервные линии связи.

Телефонные компании разрабатывали ISDN в расчете на создание полностью цифровой сети ISDN была разработана для использования существующих телефонных кабельных систем и работает подобно телефонной связи. При осуществлении ISDN-вызова на время сеанса связи устанавливается соединение с распределенной сетью, которое отключается после завершения сеанса связи. Это чем-то напоминает обычный телефонный звонок, поднятие трубки, разговор и, наконец, опускание телефонной трубки на рычаг аппарата в конце разговора.

Вашингтонский проект: ISDN-связь

В этой главе будут описаны основные концепции и процесс установки конфигурации, используемые при реализации ISDN-соединений в распределенной сети Вашингтонского учебного округа Ставится задача обеспечить ISDN-соединение для удаленного участка, которому необходимы периодические кратковременные соединения с округом

Общие сведения о технологии ISDN

ISDN была разработана для предоставления услуг цифровой связи, или цифровых служб через существующую телефонную кабельную систему. Цифровые службы могут осуществлять доставку не только голосовых данных, но и текста, графики, музыки, видео и других данных. ISDN обычно рассматривается в качестве альтернативы выделенным линиям, которые могут использоваться для телекоммуникации и объединения в локальные сети небольших и удаленных офисов.

Телефонные компании разрабатывали ISDN как часть совместной акции по стандартизации абонентских служб, **интерфейса "пользователь-сеть" (User-Network Interface, UNI)** и характеристик сети. Стандартизация абонентских служб делает более реальным обеспечение международной совместимости. Стандарты ISDN определяют аппаратное обеспечение и схемы установки непосредственной цифровой связи. Эти стандарты гарантируют простой обмен информа-

цией между ISDN-сетями, что, в свою очередь, позволяет говорить об организации связи в мировом масштабе.

Способность ISDN предоставлять цифровую связь для удаленных участков позволяет реализовать целый ряд преимуществ, среди которых можно выделить следующие.

- Сеть ISDN может передавать данные различных типов. Она обеспечивает доступ к цифровому видео, к пакетно-коммутируемым данным и службам телефонной сети.
- ISDN предлагает более быстрый, по сравнению с модемными соединениями метод установки сеанса связи, используя при этом внешнюю (out-of-band) сигнализацию (D-channel или дельта-канал). Например, некоторые ISDN-сеансы (calls) могут быть установлены менее чем за секунду.
- ISDN обеспечивает более быструю передачу данных, чем модемы, за счет использования несущего канала (B-канала). За счет использования нескольких B-каналов ISDN предоставляет пользователям большую полосу пропускания в распределенных сетях (например, два B-канала обеспечивают скорость передачи 128 Кбит/с), чем некоторые выделенные линии.

ISDN также может предоставить чистый канал передачи данных, через который устанавливаются PPP-соединения.

Однако еще на стадии проектирования следует убедиться в том, что выбранное оборудование имеет характеристики, позволяющие реализовать преимущество гибкости ISDN-сетей. Кроме того, необходимо помнить о следующих проблемах ISDN.

- *Проблемы безопасности.* Поскольку сетевые устройства могут соединяться посредством общедоступной коммутируемой телефонной сети (Pubic Switched Telephone Network, PSTN), важной задачей при проектировании является достижение высокого уровня безопасности для защиты сети от несанкционированного доступа.
- *Проблема снижения затрат на содержание сети.* Главная цель выбора для сети ISDN — избежать затрат на круглосуточное обслуживание (неизбежных при использовании выделенной линии или Frame Relay). Поэтому очень важно оценить объемы передачи данных в сети и осуществить мониторинг использования ISDN, чтобы гарантировать окупаемость затрат на поддержку доступа к распределенной сети.

Компоненты ISDN

Компоненты ISDN включают в себя терминалы, **терминальные адаптеры (terminal adapter, TA),** устройства сетевой нагрузки (network-termination devices, NT), оборудование линейной нагрузки (line-termination equipment), оборудование обменной нагрузки (exchange-termination equipment). В табл. 11.1 представлен обзор ISDN-компонентов. ISDN-терминалы делятся на два типа (рис. 11.1). Специализированные ISDN-терминалы также называются **терминальным оборудованием 1-го типа (terminal equipment type 1, TE1).** Терминалы типов, отличных от ISDN, такие как терминальное оборудование передачи данных (data terminal equipment, DTE), которые предшествовали ISDN-стандартам, называются **терминальным оборудованием 2-го типа (terminal equipment type** 2, **TE2).** Терминальное оборудование 1-го типа подключается к сети ISDN посредством цифровой линии на базе четырехпроводной витой пары. Терминальное оборудование 2-го типа подключается к сети ISDN через терминальные адаптеры. Терминальный адаптер ISDN может быть либо независимым устройством, либо платой в составе терминального оборудования 2-го типа. Если терминальное оборудование 2-го типа реализовано как отдельное устройство, то оно подсоединяется к терминальному адаптеру через стандартный интерфейс физического уровня. Следующая соединительная точка в сети ISDN после устройств терминального оборудования 1-го и 2-го типа — это **сетевая нагрузка 1-го типа (network-termination type I, NT1)** или устройство **сетевой нагрузки 2-го типа (network-termination type** 2, **NT2).** Сетевая нагрузка 1-го и 2-го типа — это устройства, посредством ко-

торых четырехпроводное абонентское устройство подключается к стандартной двухпроводной линии местного ответвления. В США сетевая нагрузка 1-го типа — это устройство, размещаемое на территории заказчика (customer premises equipment, CPE). За пределами североамериканского континента, сетевая нагрузка 1-го типа в большинстве случаев является частью сети, предоставляемой провайдером. Сетевая нагрузка 2-го типа — более сложное устройство, обычно входящее в состав цифровой **учрежденческой (или местной) АТС (private branch exchange, PBX).** Сетевая нагрузка 2-го типа предоставляет службы протоколов второго и третьего уровней. Также существуют объединенные устройства сетевой нагрузки 1-го и 2-го типа (NT1/2), которые совмещают функции устройств 1-го и 2-го типов.

Таблица 11.1. Компоненты ISDN

Компонент	Описание
Терминальное оборудование 1-го типа	Устройство, совместимое с сетью ISDN; TE1 подключается к сетевой нагрузке либо 1-го либо 2-го типа
Терминальное оборудование 2-го типа	Устройство, несовместимое с сетью ISDN и требующее наличия терминального адаптера
Терминальный адаптер	Преобразует стандартные электрические сигналы в форму, используемую ISDN, таким образом, что устройства других типов могут подсоединятся к сети ISDN
Сетевая нагрузка 1-го типа	Подключает четырехпроводное абонентское устройство к стандартному устройству двухпроводной местной линии
Сетевая нагрузка 2-го типа	Осуществляет обмен данными между разными абонентскими устройствами и NT1 NT2 является интеллектуальным устройством, которое осуществляет коммутацию и концентрацию

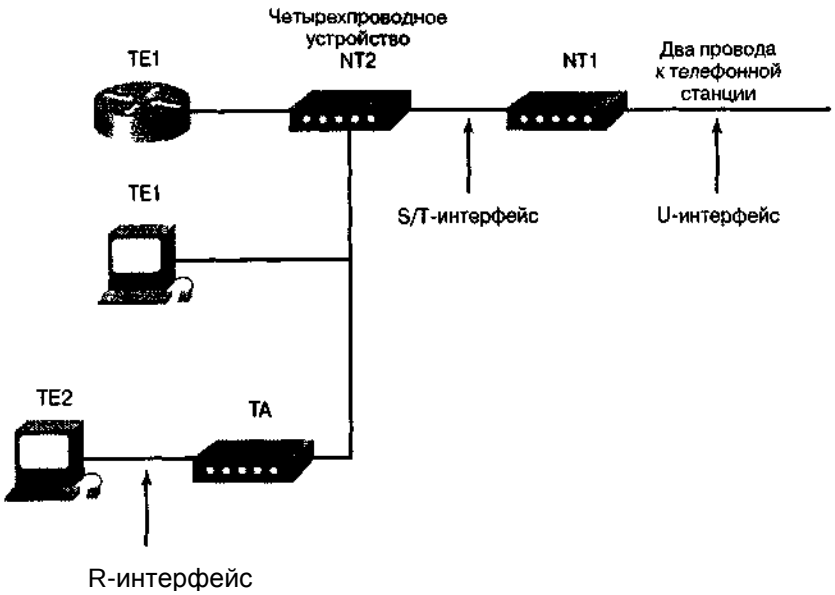


Рис 11.1. Компоненты ISDN позволяют создавать соединения между двумя устройствами

Соединительные точки ISDN

Для соединения устройств, которые предоставляют определенные функции, необходимо обеспечить поддержку этими устройствами специфических интерфейсов. Поскольку с помощью CPE реализуется одна или несколько функций, они могут использовать различные интерфейсы для подключения к устройствам, которые поддерживают другие типы функций. Вследствие этого в стандартах не определяются интерфейсы с точки зрения оборудования. Вместо этого в стандартах речь идет о **соединительных точках (reference point).** Соединительные точки представляют собой ряд спецификаций, которые определяют соединения между конкретными устройствами в зависимости от их функций в сквозных (end-to-end) соединениях. Знание этих типов интерфейсов весьма важно, поскольку устройство заказчика, такое как маршрутизатор, может поддерживать несколько типов соединительных точек, что, в свою очередь, может вызвать потребность в дополнительном оборудовании.

В табл. 11.2 представлен обзор соединительных точек, которые влияют на работу клиентской части ISDN-соединения (рис. 11.2).

Таблица 11.2. Соединительные точки ISDN

Соединительная точка	Описание
R	Соединение между несовместимым с ISDN устройством и терминальным адаптером
S	Точки, подключенные к сетевой нагрузке 2-го типа или к коммутирующему устройству на стороне клиента Этот интерфейс позволяет осуществлять вызовы между различными частями CPE
T	Электрически идентичен S-интерфейсу и представляет собой внешнее соединение от сетевой нагрузки 2-го типа к сети ISDN или к сетевой нагрузке 1-го типа
U	Соединение между сетевой нагрузкой 1-го типа и ISDN-сетью телефонной компании. Эта соединительная точка характерна только для США, где функции сетевой нагрузки 1-го типа не предоставляются провайдером услуг

Пример конфигурации ISDN-сети приведен на рис. 11.3. Три устройства подсоединены к ISDN-коммутатору телефонной станции (Central Office, CO). Два из этих устройств являются ISDN-совместимыми и поэтому могут быть подсоединены к устройствам сетевой нагрузки 2-го типа через соединительную точку S. Третье устройство (обычный, не ISDN-телефон) подключается к терминальному адаптеру через соединительную точку R. Такие же пользовательские станции (на рисунке не показаны) подсоединены к правому ISDN-коммутатору.

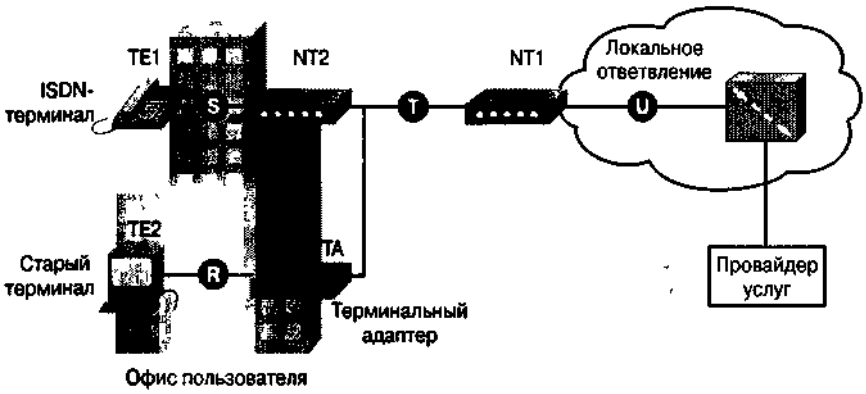


Рис. 11.2. Соединительные точки определяют логические интерфейсы между функциональными группами, такими как терминальные адаптеры и устройства сетевой нагрузки 1-го типа

Вашингтонский проект: ISDN-оборудование и передающая среда

Для проекта распределенной сети Вашингтонского учебного округа необходимо определить, какое дополнительное оборудование и передающая среда потребуются при реализации ISDN-линии.

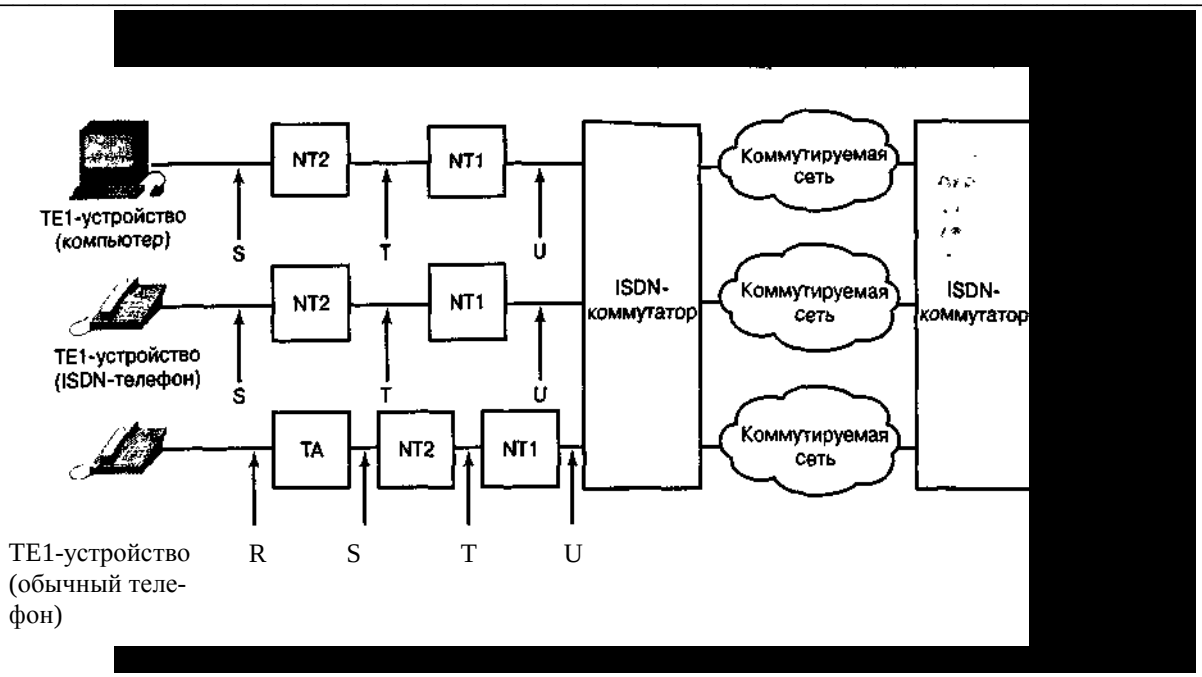


Рис. 11.3. Несколько устройств могут получить доступ к различным типам сетей через ISDN- коммутатор

Типы коммутаторов ISDN

Для обеспечения правильной работы сети ISDN важное значение имеет правильная конфигурация типа коммутатора на устройстве ISDN. Провайдеры ISDN используют для предоставления своих услуг несколько различных типов коммутаторов. Услуги, предоставляемые провайдерами, значительно различаются в зависимости от страны и конкретного региона. Так же как и модемы, различные типы коммутаторов имеют некоторые отличия в работе и предъявляют раз-

личные требования к установке вызова. Вследствие этого перед подключением маршрутизатора к некоторой службе ISDN необходимо знать тип коммутатора, установленного на телефонной станции. Эта информация указывается при конфигурировании маршрутизатора для того, чтобы он мог разместить вызовы сетевого уровня ISDN и пересылать данные.

Профильные идентификаторы услуг ISDN

Кроме типа коммутатора, используемого провайдером, необходимо также знать, какие **профильные идентификаторы услуг (service profile identifiers, SPID)** назначены данному соединению. Провайдер ISDN обеспечивает SPID для идентификации линии, используемой службой. SPID представляет собой последовательность символов (похожую на телефонный номер), которая идентифицирует вызывающее устройство на коммутаторе телефонной станции. После такой идентификации коммутатор связывает заказанную службу с соединением.

Стандарты ISDN

Работа над стандартами ISDN началась в конце 60-х годов. Полный набор рекомендаций ISDN был опубликован в 1984 году и постоянно обновляется Консультативным комитетом по международной телефонии и телеграфии (Consultative Committee for International Telegraph and Telephone, CCITT, в настоящее время — отдел стандартизации при международном телекоммуникационном союзе, ITU-T). ITU-T группирует и организует протоколы ISDN как показано в табл. 11.3.

Таблица 11.3. Протоколы ISDN

Протоколы, названия которых начинаются на букву	Описание
E	В этих протоколах рекомендуются телефонные сетевые стандарты для ISDN. Например, протокол E 164 описывает международную адресацию для ISDN
I	В этих протоколах описаны принципы, терминология и общие методы. Серия 1.100 включает в себя общие понятия ISDN и структуру других рекомендаций I-серии, серия I.200 описывает служебные аспекты ISDN; серия I 400 описывает установку UNI
Q	В этих протоколах описано, как должна осуществляться коммутация и сигнализация. Термин **"сигнализация" (signaling)** в данном случае означает используемый тип вызова Протокол Q.921 описывает **процедуры канального доступа к D-каналу (Link Access Procedure on the D channel, LAPD),** которые работают как процессы 2-го уровня эталонной модели OSI. Протокол Q 931 задает функции 3-го уровня эталонной модели

Протокол Q.931 рекомендует, чтобы сетевой уровень располагался между терминальной конечной точкой и локальным коммутатором ISDN. Этот протокол не накладывает жестких ограничений на весь путь от источника до получателя. В зависимости от провайдера и используемо-

го типа коммутатора могут быть реализованы различные варианты протокола Q.931. Причина такого разнообразия состоит в том, что до утверждения окончательного стандарта этого протокола были созданы другие типы коммутаторов.

Поскольку типы коммутаторов не стандартизованы, при конфигурировании маршрутизатора необходимо указать тип коммутатора ISDN, к которому осуществляется подключение. Кроме того, маршрутизаторы Cisco используют команду debug для контроля процессов в Q.931 и Q.921 в моменты начала или окончания вызова ISDN.

ISDN и эталонная модель OSI

Ряд стандартов ITU-T распространяет на ISDN понятия физического, канального и сетевого уровней эталонной модели OSI.

- *Физический уровень*. ISDN-спецификация **интерфейса базовой скорости (Basic Rate Interface, BRI)** определена стандартом ITU-T 1.430. ISDN-спецификация **интерфейса первичной скорости (Primary Rate Interface, PRI)** определена стандартом ITU-T 1.431.
- *Канальный уровень*. ISDN-спецификация канального уровня основана на LAPD и формально определена стандартами ITU-T Q.920 и ITU-T Q.921.
- *Сетевой уровень*. Этот уровень ISDN определен стандартами ITU-T Q.930 и ITU-T Q.931.

Физический уровень ISDN

Форматы ISDN-фреймов физического уровня (1-й уровень) различаются в зависимости от того, является ли фрейм выходным (от терминала в сеть, формат фрейма NT) или входным (от сети к терминалу, формат фрейма TE). Оба типа фреймов содержат 48 битов, из которых 36 представляют собой данные. Оба формата фреймов показаны на рис. 11.4. Биты фреймов физического уровня имеют следующие значения.

- Бит синхронизации (F) — обеспечивает синхронизацию между фреймами.
- Бит балансирования нагрузки (L) — изменяет среднее битовое значение.
- Эхо предыдущего бита D-канала (E) — используется для разрешения конфликта, возникающего в том случае, когда несколько терминалов на пассивной шине претендуют на один и то же канал.
- Бит активизации (A) — активизирует устройства.
- Вакантный бит (S) — не назначен.
- Биты канала B1, биты канала B2 и биты канала D используются для данных пользователя.

Длина поля,

бит	1	1	8	1	1	1	1	1	8	1	1	1	8	1	1	1	8	3

B

	L	D	L	B1	L	D	L	L	D	L	B1	L	D	L	B2	…	

NT-фрейм (от сети к терминалу)

Длина поля,

бит	1	1	8	1	1	1	1	1	8	1	1	1	8	1	1	1	8	3
	F	L	B1	E	D	A	F	F	B2	E	D	S	B1	E	D	S	B2	...

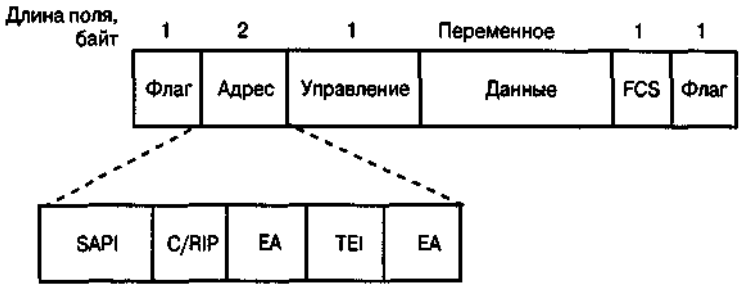
TE-фрейм (от терминала к сети)

A = Бит активации
B1= Биты канала B1
B2= Биты канала B2
D= Биты канала D (4 бита x 4000 фреймов/сек=16 Кбит/сек)
E= Эхо предыдущего D-бита
F= Бит синхронизации

К одной линии могут быть подключены несколько устройств пользователя. В этом случае при попытке одновременной передачи возникает коллизия. Во избежание этого ISDN использует средства определения приоритета. Эти средства являются частью D-канала ISDN, который будет более подробно описан в настоящей главе.

Канальный уровень ISDN

В качестве 2-го уровня сигнального протокола ISDN выступает LAPD. Протокол LAPD аналогичен протоколу управления каналом данных высокого уровня *(High-Level* Data Link Control, HDLC) и **сбалансированной процедуре канального доступа (Link Access Procedure, Balanced, LAPB).** Как следует из расшифровки аббревиатуры LAPD (Link Access Procedure on the D channel, или процедура доступа к каналу D), ее целью является обеспечение того, чтобы управляющая и сигнальная информация проходила по каналу D и принималась требуемым образом (рис. 11.5).



SAPI = Биты идентификации точки доступа к службе (6 битов)
C/RIP = Бит запроса/отклика
EA = Биты расширенной адресации
TE = Идентификатор конечной точки терминала

Рис. 11.5. Формат фрейма LAPD во многом аналогичен формату HDLC

Поля *флаг (flag)* и *управление (control)* идентичны аналогичным полям фрейма HDLC. Поле *адреса (address)* может иметь длину 1 или 2 байта. Если в первом байте установлен бит расширения адреса EA, то поле адрес имеет длину 1 байт, в противном случае — 2 байта. Первый байт адресного поля содержит *идентификатор точки доступа к услуге (service access point identifier, SAPI),* который указывает на портал, на котором 3-му уровню предоставляются услуги LAPD. Бит запроса/ответа (command/response, C/R) показывает, содержится ли во фрейме запрос или ответ. Идентификатор *конечной терминальной точки (terminal endpoint identifier, TEI)* указывает на один или несколько терминалов. Если в TEI все биты равны единице, то это указывает на широковещательное сообщение.

Сетевой уровень ISDN

Для сигнальных целей ISDN используются две спецификации 3-го уровня: ITU-T 1.450 (также известная как ITU-Q.930) и ITU-T I.451 (также известная как ITU-Q.931). Вместе взятые, эти протоколы поддерживают соединения типа "пользователь-пользователь", соединения по коммутируемой линии и пакетно-коммутируемые. В них определен ряд сообщений об установке вызова, окончании вызова, информационные и другие, в частности, установка, соединение, выключение, информация пользователя, отмена, состояние и отключение. На рис. 11.6. показаны типичные стадии линейно-коммутируемого вызова ISDN.

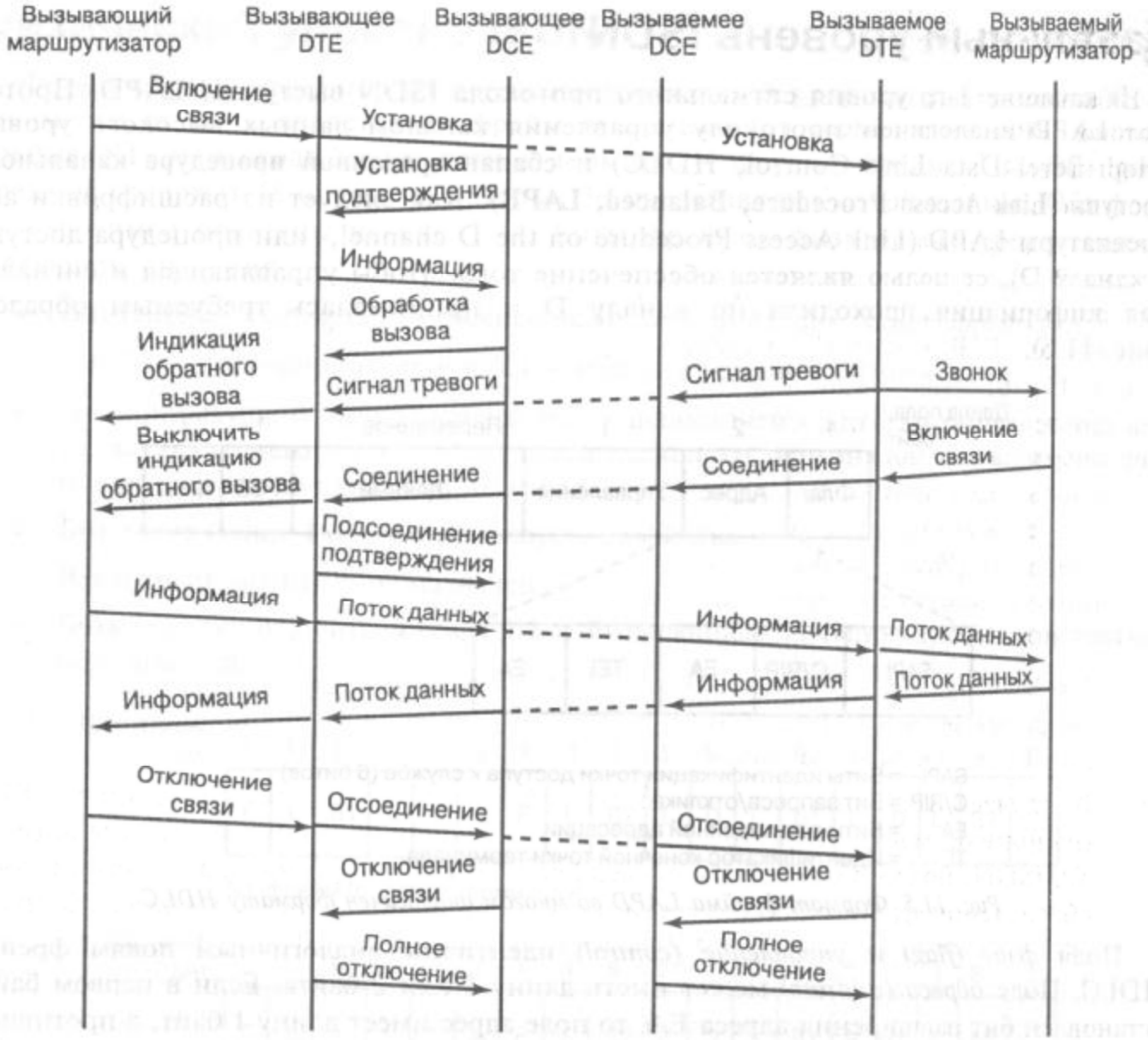


Рис. 11.6. Переключение линий в ISDN включает в себя ряд стадий вызова

Инкапсуляция ISDN

Для обеспечения удаленного доступа возможны различные решения. Наиболее часто используются протоколы PPP и HDLC. По умолчанию в ISDN выбирается rlDLC. Однако PPP имеет гораздо большие возможности в обеспечении надежности соединения, поскольку он имеет прекрасный механизм аутентификации и согласования совместимости каналов и конфигурации протоколов. При использовании PPP можно активизировать протокола аутентификации с предварительным согласованием вызова (CHAP) для отображения вызова на экране. Другим вариантом инкапсуляции при сквозном ISDN-соединении является использование протокола LAPD.

Интерфейсы ISDN позволяют использовать только один тип инкапсуляции. После того как ISDN-вызов был принят, маршрутизатор может использовать среду ISDN для передачи трафика любого требуемого протокола сетевого уровня, например, протокола IP, в несколько пунктов назначения.

Протокол PPP

В большинстве случаев при проектировании сетей для инкапсуляции используется протокол PPP. Этот протокол представляет собой мощный и многофункциональный одноранговый механизм, используемый для установки соединений, обеспечения безопасности и инкапсуляции потока данных. Использование протокола PPP согласовывается одноранговыми сетевыми устройствами при каждой установке соединения. Каналы PPP могут быть использованы сетевыми протоколами, такими как IP и IPX, для установки в сети соединений.

Протокол PPP представляет собой открытый стандарт, определяемый спецификацией RFC 1661. При создании в него были заложены определенные свойства, делающие его особенно полезным при организации удаленного доступа к сети. Для установки первоначальной связи и достижения соглашения о конфигурации в протоколе PPP используется протокол состояния канала связи (Link State Protocol, LCP). В этом протоколе есть внутренние средства обеспечения безопасности. Протокол аутентификации паролем (Password Authentication Protocol, PAP) и протокол CHAP облегчают достижение безопасности при проектировании сети.

Протокол PPP включает в себя несколько компонентов.

- *Создание фреймов.* В спецификации RFC 1662 обсуждается реализация PPP при создании фреймов типа HDLC. В синхронных и асинхронных каналах реализации PPP несколько различаются.

  В случае, когда на одном конце канала используется синхронный PPP (например, маршрутизатор ISDN), а на другом — асинхронный (например, TA ISDN, подсоединенный к последовательному порту), возможны два способа обеспечения фреймовой совместимости. Предпочтительнее использовать средства преобразования фреймов "синхронный-асинхронный" в TA ISDN.

- Протокол LCP. Он обеспечивает способ установки, конфигурирования, поддержки и разрыва соединения типа "точка-точка". До того, как начнется обмен сетевыми дейтаграммами (например, по протоколу IP), LCP должен сначала открыть сеанс связи и согласовать параметры конфигурации. Эта фаза заканчивается после того, как фрейм подтверждения конфигурации был отправлен и получен.

- Средства аутентификации. Проверка аутентификации является первичным средством обеспечения безопасности ISDN и других каналов с PPP-инкапсуляцией. Протоколы аутентификации (PAP и CHAP) определены стандартом RFC 1334 (более подробно см. главу 10, "Протокол PPP). После того, как LCP установил PPP-соединение, можно активизировать дополнительный протокол аутентификации до согласования и установки протокола управления сетью (Network Control Protocol). Если требуется выполнить аутентификацию, то это должно быть согласовано на стадии установки LCP. Процесс аутентификации может быть двусторонним (каждая из сторон проверяет друг друга) или односторонним (одна сторона, обычно вызываемая, проверяет другую).

Включение режима аутентификации производится командой интерфейса **`ppp authentication`**. Для аутентификации могут быть использованы протоколы PAP и CHAP. CHAP считается более развитым средством проверки, поскольку он использует трехэтапное квитирование с целью избежать отправки пароля открытым текстом по каналу PPP.

Использование ISDN

Как показано на рис. 11.7, ISDN имеет много применений. В последующих разделах обсуждаются следующие применения ISDN:

- удаленный доступ;
- удаленные узлы;
- соединения типа **малый офис/домашний офис (small office/home office, SOHO).**

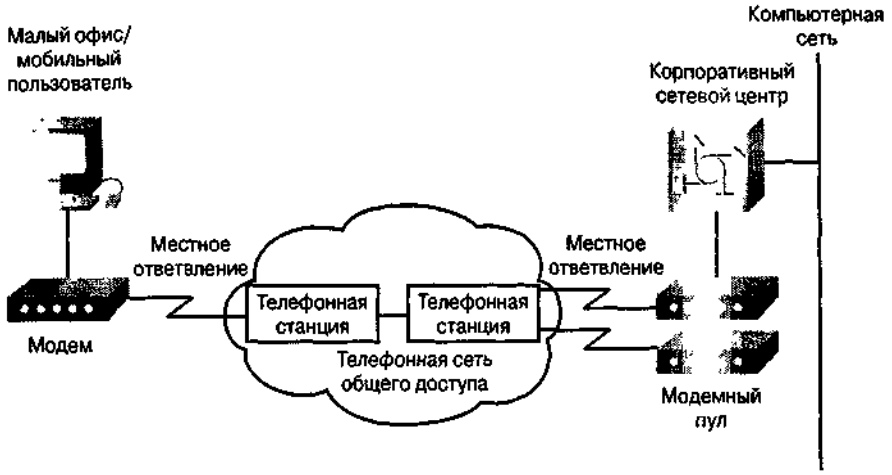


Рис. 11.7. Одним из применений ISDN является обеспечение коммутируемых соединений типа "малый офис/домашний офис"

Удаленный доступ

Удаленный доступ включает в себя соединение между собой пользователей, расположенных в удаленных местах, посредством коммутируемых соединений. Этим удаленным местом может быть дом, номер в отеле, где остановился мобильный пользователь, или малый удаленный офис. Коммутируемое соединение может осуществляться посредством установки аналогового соединения через базовую телефонную службу или через ISDN. Характеристиками соединения являются скорость, стоимость, расстояние и доступность.

Каналы удаленного доступа обычно представляют собой линии с самыми низкими скоростями, поэтому желательно увеличение их скорости. Стоимость удаленного доступа обычно относительно невелика, особенно при использовании базовой телефонной службы. Оплата услуг ISDN значительно варьируется в зависимости от географического региона, доступности службы и типа оплаты. При коммутируемом доступе, особенно при использовании ISDN, возможны ограничения по расстоянию, в частности, может быть ограничен выход за пределы области доступа.

Удаленные узлы

При использовании метода удаленных узлов, как показано на рис. 11.8, на время обмена данными пользователи подсоединяются к локальной сети корпоративного сетевого центра. Во всем, кроме низкой скорости соединения пользователь ощущает себя как обычный пользователь локальной сети. Как правило, доступ к локальной сети осуществляется посредством сервера доступа. Это устройство обычно объединяет в себе функции модема и маршрутизатора. При подключении удаленного пользователя последний может получить доступ к серверу локальной сети как если бы он находился в этой локальной сети.

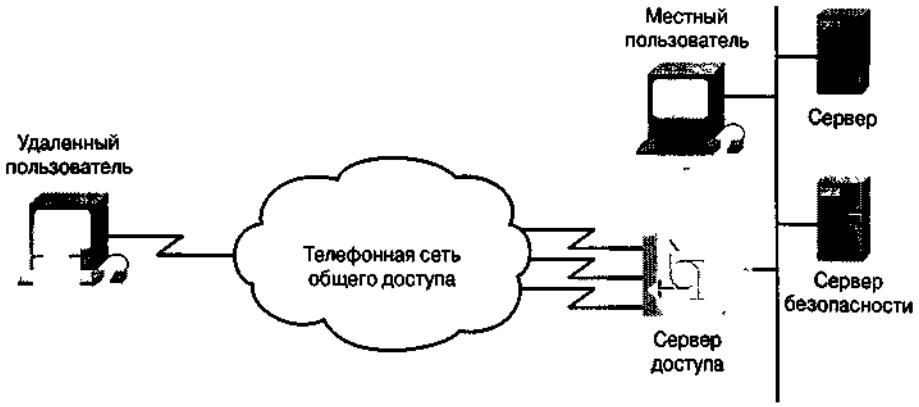


Рис. 11.8. При использовании ISDN удаленный пользователь может считаться обычным локальным сетевым узлом

Этот метод имеет много преимуществ. Он наиболее надежный и гибкий, а также предлагает самые удобные средства расширения сети. Удаленному пользователю требуется только один персональный компьютер и несколько клиентских программ. Единственным дополнительным устройством, требуемом на удаленном участке, является модем. Недостатком этого метода является дополнительный обмен административными данными, необходимый для поддержки удаленного пользователя. Вследствие указанных выше преимуществ далее в примерах этой главы рассматривается именно такой способ.

Удаленный пользователь часто работает вне своего дома. Обычно ему требуется практически постоянный доступ к сети предприятия. Такая связь должна быть надежной и постоянно доступной. Такие требования обычно побуждают к использованию ISDN (рис. 11.9). При выборе такого решения соединение ISDN может быть использовано для предоставления услуг телефонной связи и как средство подключения рабочей станции пользователя к сети предприятия.

Вашингтонский проект: требования ISDN

Периодически требуется обеспечить доступ с удаленного участка к распределенной сети Вашингтонского учебного округа. Следует использовать технологию ISDN для превращения малого участка в удаленный узел распределенной сети.

Подключение малого офиса

Малый или домашний офис, используемый несколькими пользователями, требует установки соединения, которое было бы более быстрым и надежным, чем обычное аналоговое коммутируемое соединение. В конфигурации, показанной на рис. 11.10, все пользователи удаленного участка сети имеют равноправный доступ к службам, неположенным в корпоративном офисе, через ISDN-маршрутизатор. Такой способ позволяет пользователям малого офиса подключаться к корпоративной сети или к Internet с гораздо большей скоростью, чем при выходе в сеть с помощью телефонной линии и модема.

Мо

Рис. 11 9 Для осу
клиентское п

Малый офис/
домашний офис

Рис 11 10 ISDN предлагает экономичный способ поддержки малых офисов

В проектах по подключению пользователей малого офиса обычно предусматривается использование только коммутируемого соединения, инициатором которых является малый офис. При этом для упрощения процесса проектирования и поддержки сети можно воспользоваться традиционными технологиями преобразования адресов. Используя эти технологии, удаленный сайт может поддерживать несколько сетевых устройств, но для корпоративного сервера он будет выглядеть как один узел, которому назначен один IP-адрес.

Инженерный журнал: резервное коммутируемое соединение

ISDN может быть использована в качестве резервной службы при соединении по выделенной линии между удаленными офисами и центральным офисом Если первичное соединение выходит из строя, то устанавливается коммутируемое ISDN-соединение и поток данных направляется через ISDN. После восстановления основного канала поток данных изменяет направление, а ISDN-соединение разрывается.
Резервная служба ISDN может также быть сконфигурирована на основе порогового значения для объема потока или других ограничений первичной выделенной линии. Если мощность потока превышает определенное пользователем значение, то активизируется ISDN-линия для увеличения полосы пропускания между двумя участками, как показано на рис. 11.11.

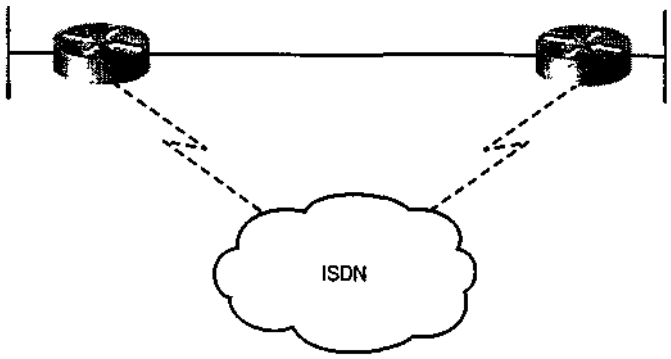


Рис. 11.11 ISDN может выступать в качестве резервного канала

Службы ISDN: интерфейс базовой скорости (BRI) и интерфейс первичной скорости (PRI)

ISDN имеет две службы: BRI и PRI. Служба BRI предлагает два B-канала и один D-канал как это показано на рис. 11.12. Вместе они часто обозначаются как 2B+D. Служба BRI предоставляет общую ширину полосы пропускания 144 Кбит/с, которая разделена на три отдельных канала. Служба B-канала работает на скорости 64 Кбит/с и предназначена для работы с данными пользователя. Два B-канала работают со скоростью 64 Кбит/с и используются для передачи голосовых данных или данных пользователя.

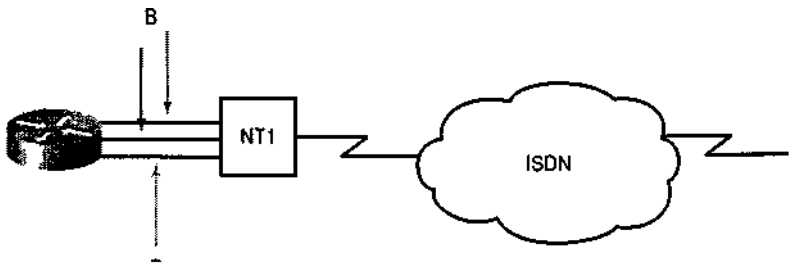


Рис. 11.12. BRI, используемый для служб ISDN, предлагает два B-канал и один D-канал

ISDN обеспечивает большую гибкость при проектировании сетей ввиду возможности использования каждого из B-каналов для отдельных голосовых приложений и/или приложений, передающих данные пользователя. Например, из корпоративной сети по одному из B-каналов со скоростью 64 Кбит/с может загружаться большой документ, в го время как другой B-канал используется для просмотра Web-страницы.

Третий канал, типа D, представляет собой сигнальный канал шириной 16 Кбит/с и используется для передачи инструкций, указывающих телефонной сети, как следует обрабатывать B-каналы. Хотя служба BRI канала D предназначена в первую очередь для передачи управляющей и сигнальной информации, при определенных условиях она может использоваться и для передачи данных. Сигнальный протокол D-канала функционирует на уровнях 1-3 Эталонной модели OSI.

Терминалы не могут передавать данные в канал D до тех пор, пока они не обнаружат требуемое количество единиц (означающих отсутствие сигнала), соответствующее заранее заданному приоритету. Если TE обнаруживает в эхо-канале (E) бит, отличающийся от его D-битов, то передача должна быть немедленно прекращена. Этот простой механизм позволяет достичь того, чтобы в конкретный момент времени только один терминал мог передавать D-сообщение. После успешной передачи D-сообщения приоритет терминала понижается, поскольку ему требуется

вновь найти непрерывную последовательность единиц перед началом передачи. Терминалы не могут повысить свой приоритет до тех пор, пока все остальные устройства на этой же линии не получат возможность передать свои D-сообщения. Телефонные соединения имеют более высокий приоритет, чем все остальные службы, а сигнальная информация имеет более высокий приоритет, чем несигнальная.

В Северной Америке и Японии PRI-служба ISDN предлагает 23 канала типа B и один канал типа D, что в суммарном выражении составляет 1,544 Мбит/с (D-канал PRI работает со скоростью 64 Кбит/с). PRI-служба ISDN в Европе, Австралии и других странах предлагает 30 каналов типа B и один канал типа D со скоростью 64 Кбит/с, что в суммарном выражении составляет 2048 Мбит/сек.

Установка соединений BRI

Выбор службы BRI или PRI осуществляется на основе требований приложений и имеющейся организации потоков данных. Требования, связанные с потоками данных, могут привести к установке нескольких соединений BRI или PRI. После подключения к сети ISDN с помощью BRI- или PRI-интерфейсов необходимо спроектировать сквозные службы ISDN.

Местное ответвление BRI заканчивается в помещении пользователя в NT1. Интерфейс локального ответвления в NT1 называется соединительной точкой U-типа. На рис. 11.13 показана типичная схема соединения BRI.

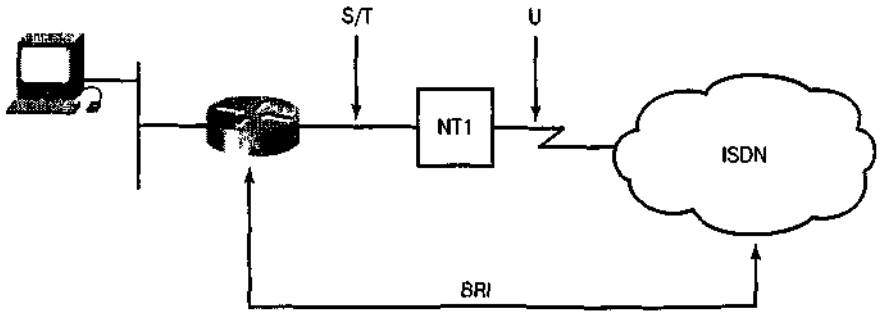


Рис 11 13. Локальное ответвление BRI подсоединено к сети ISDN

Оборудование BRI

Для служб BRI используются два основных типа ISDN CPE: маршрутизаторы локальных сетей и терминальные адаптеры (TA). Некоторые устройства BRI предлагают для аналоговых телефонов интегрированные NT1 и интегрированные TA.

ISDN-маршрутизаторы локальных сетей обеспечивают маршрутизацию между BRI ISDN и локальной сетью с использованием маршрутизации с подключением по запросу (dial-on-demand routing, DDR). DDR автоматически устанавливает и прекращает коммутируемые вызовы, обеспечивая прозрачные соединения с удаленными участками сети, исходя из структуры и объема потоков данных. DDR также управляет включением и отключением вторичных B-каналов на основе пороговых значений нагрузки. При использовании нескольких B-каналов для объединения их данных в одной полосе пропускания используется многоканальный протокол PPP. Некоторые ISDN-приложения требуют прямого контроля пользователя над вызовами ISDN.

Терминальные адаптеры персональных компьютеров подсоединяются к рабочим станциям через шину компьютера или внешним образом через коммуникационные порты (такие, как RS-232) и могут быть использованы так же как и аналоговые (такие как V.34) внутренние или внешние модемы.

TA могут предоставлять отдельному пользователю ПК прямой контроль над инициацией се-

анса ISDN и прекращением его, также как и аналоговые модемы. Для обеспечения возможности добавления или удаления вторичных. B-каналов необходимы автоматические механизмы. Для предоставления пользователю персонального компьютера услуг ISDN применяются адаптеры серии Cisco 200.

Вопросы установки параметров конфигурации ISDN

Для подготовки маршрутизатора к работе в среде ISDN необходимо задать его глобальные параметры и параметры интерфейса.

Установка глобальных параметров включает в себя следующее.

- Выбор коммутатора, который соответствовал бы коммутатору провайдера ISDN на телефонной станции. Это необходимо ввиду того, что несмотря на наличие стандартов, конкретные характеристики сигнализации значительно варьируются в разных странах и регионах.
- Установка параметров получателя. Этот шаг включает в себя указание статических маршрутов от маршрутизатора к другим получателям ISDN и задание критерия отбора требуемых пакетов, которые бы инициировали ISDN-вызов к соответствующему получателю.

Установка параметров интерфейса включает в себя следующее.

- Выбор спецификаций интерфейса. При этом необходимо задать тип интерфейса BRI и номер данного BRI-порта. Этот интерфейс использует IP-адрес и маску подсети.
- Конфигурирование ISDN-адресации с помощью DDR-информации о наборе и идентификаторов соединений, предоставляемых провайдером ISDN. При этом необходимо указать, что этот интерфейс входит в группу набора, используя набор пакетов в глобальной форме. Дополнительные команды размещают вызов ISDN в соответствующем пункте назначения.
- Используя существующую конфигурацию интерфейса, можно задать дополнительные параметры, например, время ожидания носителя ISDN перед ответом на вызов или время бездействия в секундах до того момента, когда маршрутизатор отключит вызов.
- Кроме того, конфигурирование интерфейса включает в себя конфигурирование ISDN, выбор типа коммутатора и SPID. В следующем разделе приведены примеры и описания задач конфигурирования ISDN.

Инженерный журнал: команды ISDN

Команда interface bri номер назначает интерфейс, используемый ISDN на маршрутизаторе, выступающем в качестве TA1. Если маршрутизатор не имеет собственного BRI (т.е. является устройством TE2), то он должен использовать внешний терминальный адаптер. На маршрутизаторе TE2 следует использовать команду interface serial *номер.*

Если требуется установить инкапсуляцию PPP на интерфейсе ISDN, то следует выполнить команду encapsulation ppp Это происходит в тех случаях, когда желательно воспользоваться богатым набором опций, предлагаемых протоколом PPP (например, протокол аутентификации CHAP). Если будут приниматься вызовы от более чем одного источника, то необходимо использовать средства PAP или CHAP протокола PPP.

Конфигурирование BRI

Для входа в режим установки конфигурации интерфейса и конфигурирования BRI используется команда interface BRI в режиме глобальной конфигурации. Полный синтаксис команды: interface bri номер

Аргумент *номер* описывает порт, соединитель или номер карты интерфейса. Эти номера присваиваются при изготовлении во время установки или добавления к системе и могут быть отображены на мониторе с помощью команды show interfaces.

В листинге 11.1 для интерфейса BRI 0 устанавливается вызов и прием вызовов с двух участков, использование PPP для исходящих звонков и использование протокола CHAP для аутентификации входящих звонков.

Листинг 11.1. Прием вызовов с двух участков

```
interface bri 0
encapsulation ppp
no keepalive
dialer map ip 131.108.36.10 name EB1 234
dialer map ip 131.108.36.9  name EB2 456
dialer-group 1
isdn spidl 0146334600
isdn spidl 0146334610
isdn T200 1000
ppp authentication chap
```

Определение типа коммутатора

До использования BRI ISDN необходимо выполнить глобальную команду isdn switch-type для задания типа коммутатора телефонной станции, к которому будет подсоединен маршрутизатор. Вывод по команде ОС Cisco isdn switch-type в листинге 112 сообщает типы B RI-коммутаторов (в Северной Америке основными типами являются 5ESS, DMS100 и N1-1).

Листинг 11.2. Типы коммутаторов, поддерживаемые BRI

```
kdt-3640(config)# isdn switch-type ?
basic-ltr6     1TR6 switch type for Germany
basic-5ess     AT&T 5ESS switch type for U.S.
basic-dmslOO   Northern DMS-100 switch type
basic-nets     NETS switch type for the UK and Europe
basic-nitl     National ISDN-1 switch type
basic-nwnetS   NETS switch type for Norway
basic-nznetS   NETS switch type for New Zealand
basic-tsOlS    TS013 switch type for Australia
ntt            switch type for Japan
vn2            VN2 switch type for France
vn3            VN3 and VN4 switch type for France
```

Для установки конфигурации коммутатора телефонной станции на ISDN-интерфейсе используется команда isdn switch-type в командном режиме глобальной конфигурации. Полный синтаксис команды:

isdn switch-type *тип*

Аргумент *тип* указывает тип коммутатора провайдера службы; по умолчанию это значение равно none, что означает отключение коммутатора на интерфейсе ISDN. Для отключения коммутатора на интерфейсе ISDN можно выполнить команду

```
isdn switch-type none
```

В следующем примере устанавливается тип коммутатора 5ESS:

```
isdn switch-type basic-5ess
```

Примечание

В версиях ОС Cisco до 11.2 тип коммутатора, заданный в конфигурации, является глобальной командой (отметим, что это также означает, что на одном шасси Cisco не могут быть одновременно использованы адаптеры BRI и PRI). В версии 11.3T и более поздних поддерживаются несколько типов коммутаторов на одном шасси.

Задание SPID

SPID позволяют нескольким устройствам ISDN, таким как звуковые устройства или устройства цифровых данных, совместно использовать локальное ответвление. Во многих случаях, например, при конфигурировании маршрутизатора для подсоединения к DMS-100, задание SPID является необходимым.

Инженерный журнал: коммутаторы DMS-100

Коммутаторы DMS-100 поддерживают только два SPID на каждом интерфейсе базовой скорости: по одному SPID на каждый B-канал. Если оба B-канала будут использоваться только для данных, то на маршрутизаторе необходимо установить конфигурацию для обоих SPID (на каждый B-канал). Нельзя передавать по одному и тому же B-каналу голос и данные одновременно. Наличие или отсутствие канального SPID в конфигурации маршрутизатора однозначно определяет, будет ли второй B-канал использоваться для данных или для голоса.

Следует помнить, что ISDN обычно используется для коммутируемых соединений. SPID обрабатываются при каждой операции установки вызова.

Команда **`isdn spid2`** в режиме конфигурирования интерфейса используется для остановки на маршрутизаторе номера SPID, который был назначен провайдером службы ISDN каналу B2. Полный синтаксис команды:

Lsdn spid2 номер-spid *[Idn]*

Команда `no isdn spid2` используется для отключения указанного SPID, в результате чего исключается доступ к коммутатору. Если в no-форму этой команды включитть LDN, то доступ к коммутатору остается разрешенным, однако другой B-канал, вероятно, не сможет принимать приходящие звонки. Полный синтаксис команды:

isdn spid2 номер-spid *[Idn]*

В качестве аргумента *номер-spid* задается число, указывающее службу, к которой подключен данный компьютер. Это число назначается провайдером службы ISDN и обычно представляет собой телефонный номер из 10 цифр с несколькими дополнительными цифрами. По умолчанию номер SPID не определен.

Инженерный журнал: аргумент Idn

Аргумент Idn является необязательным и означает номер локального каталога (LDN); он предоставляется провайдером во входном конфигурационном сообщении. Это семизначное число, назначаемое провайдером услуги.

Этот аргумент требуется только для коммутаторов DMS-100 в Национальной сети ISDN-1 (N1-1). LDN должен быть задан, если необходимо принимать все входящие звонки только на канал B1. Коммутатор ISDN проверяет LDN для определения того, могут ли оба канала использоваться для передачи и получения данных. Если LDN отсутствует, то для дуплексной коммуникации может быть использован только канал B2. Однако при этом второй канал по-прежнему может быть использован для выходных звон-

ков.
В приведенном ниже примере для канала B2 на маршрутизаторе задаются SPID и LDN:

```
isdn spid2 41555121202 5551214
```

Каждый SPID указывает на информацию об установке канала и о конфигурации. Когда некоторое устройство пытается подсоединиться к сети ISDN, оно запускает процесс инициализации D-канала 2-го уровня, что означает назначение устройству TEI. После этого устройство пытается инициализировать D-канал 3-го уровня. Если SPID являются необходимыми для устройства, но не сконфигурированы или сконфигурированы некорректно, то инициализации 3-го уровня не происходит и службами ISDN воспользоваться невозможно.
Для SPID не существует стандартного формата Вследствие этого номера SPID значительно варьируются в зависимости от производителя и носителя.
Типичная конфигурация SPID в операционной системе Cisco выглядит следующим образом:

```
Interface bri 0

isdn spidl 0835866201 8358662

isdn spid2 0835866401 8358664
```

Эти команды также задают LDN, представляющий собой семизначное число, назначаемое провайдером службы и используемое для маршрутизации вызова. Для установки ISDN-соединения LDN не является необходимым, однако оно должно быть указано, если требуется принимать входные звонки на канал B2. LDN является необходимым только в том случае, когда конфигурируются два SPID (например, если происходит подключение к коммутатору DMS или N1-1). Каждый SPID ассоциирован с LDN. Установка конфигурации LDN приводит к тому, что на входные звонки на канал B2 дается корректный ответ Если конфигурация LDN не установлена, то при приеме входных звонков на канале B2 возможны сбои.

Пример конфигурирования BRI

Материал этого раздела основан на тексте вывода, приведенном в листинге 11.3, который отображает конфигурацию BRI.

Листинг 11.3. Пример конфигурации BRI

```
! Установка типа коммутатора, статического маршрута и
! наборного устройства для ISDN на маршрутизаторе Cisco A
isdn switch-type basic-5ess
ip route 172.16.29.0 255.255.255.0 172.16.126.2
dialer list 1 protocol ip permit
i
! Настройка интерфейса BRI для PPP; установка адреса и маски
interface bri 0
ip address 172.16.126.1 255.255.255.0
i
! Обратитесь к списку протоколов в устройстве набора для
! идентификации интересующих пакетов
dialer-group 1
!
! Установить начало и конец вызова, а также другие параметры
! предоставленные провайдером ISDN
dialer wait-for-carrier time 15
dialer idle-timeout 300
isdn spidl 0145678912
```

```
! Настройка параметров вызова для маршрутизатора
dialer map ip 172.16.126.2 name cisco-b 445
```

Ниже приведено описание команд и параметров, имеющихся в тексте листинга 11.3.

Команда/параметр	Описание
isdn switch-type	Выбирает коммутатор AT&T в качестве типа коммутатора ISDN телефонной станции для данного маршрутизатора
dialer-list 1	Связывает разрешенный IP-поток данных с 1-й группой набора
protocol ip permit	Маршрутизатор будет вызывать ISDN только для пакетов 1-й группы набора
interface bri 0	Выбирает интерфейс с TA и другими функциями на маршрутизаторе
encapsulation ppp	Использование инкапсуляции PPP на выбранном интерфейсе
dialer group 1	Связывает интерфейс BRI 0 с первой группой набора
dialer wait-for-carrier time	Устанавливает максимальное время ожидания ответа провайдера: в течение 15 сек после инициализации вызова
Dialer idle timeout	Количество секунд бездействия до того, как маршрутизатор отключит вызов ISDN. Отметим, что для того, чтобы отложить прекращение вызова устанавливается большая длительность бездействия

Ниже приведено описание параметров команды dialer map из листинга 11.3.

Параметр dialer map	Описание
ip	Название протокола
172.16.126.2	Адрес получателя
name	Идентификация маршрутизатора удаленной стороны. Относится к вызываемому маршрутизатору
445	Номер ISDN-соединения, используемый для того, чтобы достичь пункта назначения данного DDR

Подтверждение операций BRI

Чтобы проверить работу BRI, следует использовать команду show isdn status, которая отображает статус интерфейса BRI. В листинге 11.4 были успешно согласованы TEI и 3-й (сквозной) уровень ISDN готов совершать или принимать вызовы.

Листинг 11.4. Вывод по команде show isdn status

```
kdt-1600# show isdn status
The current ISDN Switchtype = basic-nil
ISDN BRIO interface
   Layer 1 Status:
```

```
        ACTIVE
    Layer 2 Status:
        TEI=109, State=MULTIPLE_FRAME_ESTABLISHED
        TEI=110, State=MULTIPLE_FRAME_ESTABLISHED
    Spid Status:
        TEI 109, ces=l, state=8 (established)
            Spid1 configured, spidl sent, spidl valid
            Endpoint ID Info: epsf=0, usid=l, tid=l
        TEI 110, ces=2, state=8 (established)
            spid2 configured, spid2 sent, spid2 valid
            Endpoint ID Info: epsf=0, usid=l, tid=l
    Layer 3 Status:
        0 Active Layer 3 Call(s)
Activated dsl 0 CCBs=0
Total Allocated ISDN CCBs =0
```

Маршрутизация с подключением по запросу

При создании сетевых приложений необходимо определить, каким образом соединения ISDN будут инициироваться, устанавливаться и поддерживаться. DDR создает соединения между сайтами ISDN путем установки и отключения коммутируемых соединений в зависимости от требований сетевого потока. DDR может обеспечивать маршрутизацию и службы каталогов различными способами, что создает иллюзию постоянного соединения за счет использования коммутируемых соединений.

Для того, чтобы установить полный контроль над тем, когда устанавливаются DDR-соединения, необходимо тщательно рассмотреть следующие вопросы.

- Какие сайты могут инициировать соединение за счет анализа потока данных?
- Требуется ли установка соединения с сетями малого офиса? Требуется ли установка соединения для управления сетью или рабочей станцией? Какие сайты могут прекратить соединение по причине бездействия?
- Как поддерживаются службы каталогов и таблицы маршрутизации при бездействующем соединении?
- Какие приложения необходимо поддерживать для работы по соединениям DDR? Для какого количества пользователей их необходимо поддерживать?
- Какие неизвестные протоколы могут вызвать установку DDR-соединения? Можно ли их отфильтровать?

Проверка работы DDR

Для проверки работы DDR могут быть использованы следующие команды.

Команда	Описание
ping/telnet	При выполнении команд ping или telnet для удаленного сайта или в случае, когда поток данных вызывает установку соединения, маршрутизатор посылает сообщение об изменении статуса канала на консоль
show dialer	Используется для получения общей диагностической информации об интерфейсе, сконфигурированном для DDR, такой, например, как количество раз успешного соединения, значение таймера бездействия и быстрого таймера бездействия (fast idle

	timer) для каждого из B-каналов. Также предоставляется текущая информация о вызове, такая как длительность вызова, номер и имя устройства, с которым в настоящее время соединен интерфейс
show isdn active	Эту команду всегда следует выполнять при использовании ISDN. Она показывает, что происходит вызов и выводит информацию о пронумерованных вызовах
show isdn status	Используется для отображения статистики ISDN-соединения
show ip route	Отображает известные маршрутизатору пути, включая статические и динамические

Устранение ошибок при работе DDR

Для выявления ошибок при работе DDR могут быть использованы следующие команды.

Команда	Описание
debug isdn q921	Проверяет наличие соединения с коммутатором ISDN
debug dialer	Отображает набираемый интерфейсом номер
clear interface	Используется для снятия текущего вызова В ситуации наличия неисправностей иногда полезно очистить статистический журнал для того, чтобы сравнить количество успешных вызовов с количеством не состоявшихся. Эту команду следует использовать осторожно. Иногда требуется очистка как локального, так и удаленного маршрутизаторов

Для разрешения проблем, связанных с использованием SPID используется команда debug isdn q921. В листинге 11.5 показано, как команда isdn spidl была отвергнута маршрутизатором

Листинг 11.5. Разрешение проблем, связанных с использованием SPID

```
kdt-1600# debug isdn q921
ISDN Q921 packets debugging is on
kdt-1600# clear interface bri 0
kdt-1600#
*Mar 1 00:09:03.728: ISDN BRO: TX -> SABMEp sapi=0 tei=113
*Mar 1 00:09:04.014: ISDN BRO: RX <- IDREM ri=0 ai=127
*Mar 1 00:09:04.018: %ISDN-6-LAYER2DOWN:
       Layer 2 for Interface BRIO, TEI 113 changed to down
*Mar 1 00:09:04.022: %ISDN-6-LAYER2DOWN:
       Layer 2 for Interface BRO, TEI 113 changed to down
*Mar 1 00:09:04.046: ISDN BRO : TX -> IDREQ ri =44602 ai= 127
* Mar 1 00:09:04.049 :ISDN BRO : RX <- IDCKRQ ri = 0 ai = 113
* Mar 1 00:09:05.038 :ISDN BRO : RX <- IDCKRQ ri = 0 ai = 113
* Mar 1 00:09:06.030 :ISDN BRO : TX -> IDREQ ri = 37339 ai = 127
* Mar 1 00:09:06.149 :ISDN BRO : RX <- IDREM ri = 0 ai = 113
* Mar 1 00:09:06.156 :ISDN BRO : RX <- IDASSN ri = 37339 ai = 114
* Mar 1 00:09 :06.164 :ISDN BRO : TX -> SABMEp sapi = 44602 tei = 114
* Mar 1 00:09:06.188 :ISDN BRO : RX <- Uaf  sapi = 0 tei = 114
* Mar 1 00:09:06.188 : %ISDN-6-LAYER2UP:
       Layer 2 for Interface BRIO, TEI 114 changed to up
*Mar 1 00:09:06.200 : ISDN BRO : TX -> INFOc sapi=0 tei = 114
```

```
        ns = 0 nr = 0 i = 0x08007B3A6383932393833
* Mar 1 00:09:06.276 : ISDN BRO : RX <- INFOc sapi=0 tei = 114
        ns = 0 nr = 1 l = 0x08007B080382E43A
* Mar 1 00:09 :06.283 : ISDN BRO : TX -> RRr sapi = 0 tei=114 nr = 1
* Mar 1 00:09:06.287 : %ISDN-4- INVALID SPID: Interface BRO
        Spidl was rejected
```

Проверка состояния ISDN-линии Cisco 700 выполняется с помощью команды show status, как показано в листинге 11.6.

Листинг 11.6. Проверка состояния ISDN-линии Cisco 700

```
kdt-776># show status
Status 01/04/1995 18:15:15
Line Status
   Line Activated
   Terminal Identifier Assigned              SPID Accepted
   Terminal Identifier Assigned              SPID Accepted
Port Status     Interface Connection Link
   Ch: 1        Waiting for call
   Ch: 2        Waiting for call
```

Резюме

- ISDN обеспечивает интегрированные возможности передачи голоса/данных по общедоступной коммутируемой сети.
- Компонентами ISDN являются терминалы, TA, NT-устройства и коммутаторы ISDN.
- Соединительные точки ISDN определяют логические интерфейсы между функциональными группами, такими, например, как TA1 и NT1.
- SDN характеризуется набором стандартов ITU-T и использует физический, анальный и сетевой уровни эталонной модели OSI.
- Двумя основными типами инкапсуляции ISDN являются PPP и HDLC.
- ISDN имеет много применений, такие, например, как удаленный доступ, удаленные узлы и подключения малого офиса.
- Основными службами ISDN являются BRI и PRI.
- BRI делит общую полосу пропускания в 144 Кбит/с на три отдельных канала.
- Конфигурация BRI включает в себя конфигурацию BRI-интерфейса, тип коммутатора ISDN и SPID.
- DDR устанавливает и прекращает работу коммутируемых соединений по мере необходимости.

Задачи проекта Вашингтонского учебного округа: ISDN

В настоящей главе были рассмотрены принципы и процессы установки конфигурации, помогающие реализовать IGRP в качестве протокола маршрутизации в сети Вашингтонского учебного округа. В качестве составных частей конфигурирования и реализации ISDN необходимо решить следующие задачи.

1. Внести в документацию изменения конфигурации маршрутизации, связанные с реализацией на маршрутизаторах ISDN.

2. Занести в документацию информацию, относящуюся к использованию ISDN при проектировании распределенной сети, включая следующее:
   - схему сети, на которой отмечены все соединительные точки;
   - описание всей доступной полосы пропускания участка и описание соединений при передаче данных;
   - описание всего коммуникационного оборудования, необходимого для реализации всех поставленных задач.
3. Занести в документацию все команды маршрутизатора, необходимые для реализации на нем ISDN.

Контрольные вопросы

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

1. Какова максимальная скорость работы ISDN?
2. Сколько B-каналов используется в ISDN?
3. Сколько D-каналов используется в ISDN?
4. Провайдер услуги ISDN должен предоставить телефонный номер и идентификационный номер (ID). Каков тип этого ID?
5. Какой канал используется в ISDN для вызова?
6. Какое устройство может быть использовано в сетевом центре предприятия предоставления доступа пользователям по коммутируемым соединениям?
   A. Коммутатор.
   B. Маршрутизатор.
   C. Мост.
   D. Концентратор.
7. Для какой из перечисленных ниже ситуаций служба ISDN оказалась бы несоответствующей?
   A. Большая концентрация пользователей в сетевом центре.
   B. Малый офис.
   C. Сеть с одним пользователем.
   D. Ничто из вышеперечисленного.
8. Наличие буквы E в названии протокола указывает на...
   A. стандарты телефонной сети.
   B. коммутацию и сигнализацию.
   C. концепции ISDN.
   D. не используется с ISDN.
9. Если при использовании ISDN для аутентификации необходимо применить CHAP, то какой протокол следует избрать?
   A. HDLC.
   B. SLIP.
   C. PPP.
   D. PAP
10. Какие команды из ниже перечисленных следует использовать на маршрутизаторе для установки типа коммутатора ISDN?
    A. `Router>isdn switch-type`
    B. `Router# isdn switch type`
    C. `Router(config-if)# isdn switch–type`
    D. `Router(config)# isdn switch-type`

Основные термины

2B+D. В контексте службы BRI ISDN — два B-канала и один D-канал.

B-канал, канал-носитель (bearer channel, B channel). В ISDN-сетях дуплексный канал с пропускной способностью 64-Кбит/, используемый для передачи пользовательских данных.

D-канал, дополнительный канал, дельта-канал, канал управления скоростью передачи (delta channel, D channel). Дуплексный ISDN-канал с пропускной способностью 16-Кбит/с (для BRI) или 64-Кбит/с (для PRI).

Q.931. Протокол, который описывает сетевой уровень между оконечной точкой и локальным ISDN-коммутатором. Не накладывает ограничений на непосредственные соединения оконечных точек. Разные ISDN-провайдеры могут использовать различные реализации этого протокола.

Идентификатор профиля службы (service profile identifier, SPID). Число, используемое некоторыми провайдерами услуг для определения служб, к которым подключено абонентское ISDN-устройство. SPID используется ISDN-устройством во время доступа к коммутатору, который инициализирует соединение с провайдером услуг.

Интерфейс базовой скорости (Basic Rate Interface, BRI). ISDN-интерфейс, состоящий из двух B-каналов и одного D-канала для канально-коммутируемой передачи голоса, видео и других данных.

Интерфейс первичной скорости (основного уровня) (Primary Rate Interface, PRI). ISDN-интерфейс для основного доступа. Состоит из одного D-канала (64 Кбит/с) и двадцати трех (для T1) или 30 (для E1) B-каналов для голоса или данных.

Интерфейс типа "пользователь-сеть" (User-Network Interface, UNI). Спецификация, определяющая стандарты взаимодействия для интерфейса между устройствами (маршрутизаторами или коммутаторами), расположенными в частной сети, и коммутаторами общедоступных сетей. Также используется для описания сходных соединений в сетях Frame Relay.

Малый офис/домашний офис (small office/home office, SOHO). Такой офис объединяет несколько пользователей, нуждающихся в соединении, которое обеспечивало бы более быструю и надежную связь, чем аналоговое коммутированное соединение.

Оборудование заказчика (customer premises equipment, CPE) Оконечное оборудование, такое как терминалы, телефоны и модемы, поддерживаемые телефонной компанией, установленные на территории клиента этой компании и подключенное к ее сети.

Процедура доступа к D-каналу (Link Access Procedure, LAPD). В сетях ISDN протокол канального уровня для D-канала. LAPD получен из LAPB и разработан, в основном, для удовлетворения требований сигнализации базового доступа ISDN. Определяется в соответствии *с* рекомендациями ITU-T (International Telecommunications Union, Международный телекоммуникационный союз) Q.920 и Q.921.

Сбалансированный протокол доступа к каналу связи (Link Access **Procedure, Balanced, LAPB).** Протокол канального уровня в наборе протоколов X.25. LAPB — бит-ориентированный протокол, являющийся частью протокола HDLC.

Сетевая нагрузка 1-го типа (network termination type 1, NT1). Устройство, соединяющее четырех проводного абонента и стандартное двухпроводное устройство местной линии.

Сетевая нагрузка 2-го типа (network termination type 2, **NT2).** Устройство, направляющее поток данных между разными абонентскими устройствами и NT1. NT2 является интеллектуальным устройством, которое осуществляет коммутацию и концентрацию.

Сигнализация (signaling). В контексте ISDN — процесс установки соединения (инициализации вызова). Используется для обозначения установки соединения, разрыва соединения, передаваемой информации и различных сообщений, включающих в себя установку, подключение, освобождение линии, пользовательскую информацию, отмену соединения, состояние соединения и отключение.

Соединительная точка (reference point). Спецификация, которая определяет соединения между специфическими устройствами в зависимости от их функций в непосредственном соединении.

Телефонная станция (Central Office, CO). Офис местной телефонной компании, к которо-

му подсоединены все местные линии и в котором происходит коммутация каналов абонентских линий.

Терминальное оборудование 1-го типа (terminal equipment type 1, TE1). Устройство, совместимое с ISDN-сетью. TE1 подключается к сетевой нагрузке 1-го, либо 2-го типа.

Терминальное оборудование 2-го типа (terminal equipment type 2, **TE2).** Устройство, не совместимое с ISDN-сетью и требующее использования терминального адаптера.

Терминальный адаптер (terminal adapter, TA). Устройство, используемое для подсоединения основных интерфейсов ISDN к существующим интерфейсам, таким как EIA/TIA-232. Как правило, представляет собой ISDN-модем.

Учрежденческая АТС (private branch exchange, PBX). Цифровой или аналоговый коммутационный узел, находящийся на территории абонента и соединяющий частную телефонную сеть абонента с общедоступными сетями.

Цифровая сеть интегрированных служб (Integrated Services Digital Network, ISDN). Коммуникационный протокол, предложенный телефонными компаниями, который позволяет передавать информацию по телефонным сетям, в том числе голосовые данные, а также данные, полученные из других источников.

Ключевые темы этой главы

- Описана работа протокола Frame Relay
- Описаны функции идентификаторов (DLCI) протокола Frame Relay
- Описана Cisco-версия протокола Frame Relay
- Описан процесс конфигурирования и проверки работы протокола Frame Relay
- Описаны подынтерфейсьг протокола Frame Relay
- Описано использование протоколом Frame Relay подынтерфейсов для решения проблемы расщепления горизонта

Глава 12

Протокол Frame Relay

Введение

В главе 10, "Протокол PPP", был рассмотрен протокол типа "точка-точка", а в главе 11, "ISDN - цифровая сеть интегрированных служб", была описана цифровая сеть интегрированных служб Было показано, что PPP и ISDN представляют собой два типа технологий распределенных сетей, которые используются с целью решения вопросов установки связи для пользователей, которым требуется получить доступ к другим географически удаленным сетевым устройствам В настоящей главе описываются службы, стандарты, компоненты и функционирование протокола ретрансляции фреймов (Frame Relay) Кроме того, в этой главе описаны методы конфигурирования служб протокола Frame Relay и команды, используемые для тестирования и поддержки установленных соединений

Вашингтонский проект: реализация протокола ретрансляции фреймов

В настоящей главе будут описаны основные понятия и процедуры конфигурации, позволяющие включить протокол ретрансляции фреймов в проект сети Вашингтонского учебного округа Кроме того, будут описаны действия, необходимые для обеспечения взаимодействия протокола Frame Relay с Internet в соответствии со спецификациями в документах, описывающих технические требования Этот этап будет последним в проектировании и реализации сети учебного округа

Обзор протокола ретрансляции фреймов

Протокол ретрансляции фреймов (Frame Relay) представляет собой стандарт Консультативного комитета по международной телефонии и телеграфии (Consultative Committee for International Telegraph and Telephone, CCITT, в настоящее время — отдел стандартизации при международном телекоммуникационном союзе, ITU-T) и Американского национального института стандартов (Amencan National Standards Institute, ANSI), описывающий процесс передачи данных по **открытым сетям данных (public data network, PDN).** Эта сетевая технология канального уровня была создана для обеспечения высокопроизводительной и эффективной связи. Протокол ретрансляции фреймов действует на физическом и канальном уровнях эталонной модели OSI, но для коррекции ошибок использует протоколы верхних уровней, такие как TCP.

Протокол ретрансляции фреймов первоначально планировалось использовать на интерфейсах ISDN. В настоящее время этот протокол является стандартным промышленным коммутируемым протоколом канального уровня, используемым для работы с различными виртуальными каналами с использованием инкапсуляции протокола канального управления высокого

уровня (High-Level Data Link Control, HDLC) для обмена данными между соединенными устройствами. Протокол ретрансляции фреймов использует виртуальные каналы для установки соединений через ориентированную на соединение службу.

Сетью, обеспечивающей интерфейс протокола ретрансляции фреймов, может быть как общедоступная сеть одного из национальных операторов связи или сеть, обслуживающая отдельное предприятие, оборудование которой принадлежит частному владельцу. Протокол ретрансляции фреймов обеспечивает пакетно-коммутируемый обмен данными, который происходит по интерфейсу между устройствами пользователя (такими как маршрутизаторы, мосты и хосты) и сетевым оборудованием (таким как коммутирующие узлы). Как было сказано ранее, устройства пользователя часто называются оборудованием терминала данных (data terminal equipment, DTE), а сетевое оборудование, взаимодействующее с DTE, называется оконечным оборудованием канала данных (data circuit-terminating equipment, DCE) (рис. 12.1).

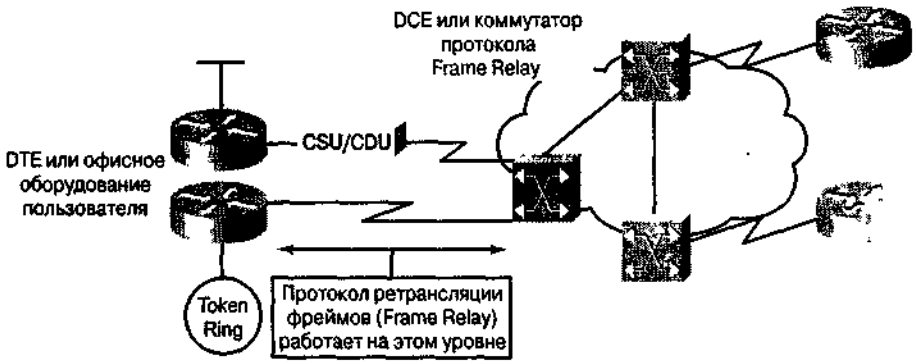


Рис 12.1. Протокол ретрансляции фреймов (Frame Relay) определяет процесс установки соединения между маршрутизатором и коммутирующим оборудованием локального доступа, используемым провайдером услуг

Терминология протокола Frame Relay

Ниже объясняются некоторые термины, используемые в настоящей главе при обсуждении протокола Frame Relay.

- Скорость локального доступа (local access rate) (скорость порта) — скорость установки соединения локального ответвления со средой протокола Frame Relay. Она характеризует скорость поступления данных в сеть и получения данных из нее.
- **Идентификатор канального соединения (data-link connection identifier, DLCI). Как** показано на рис. 12.2, DLCI представляет собой номер, идентифицируюший логический канал между устройствами источника и получателя. Коммутатор протокола ретрансляции фреймов назначает DLCI каждой паре маршрутизаторов для создания постоянных виртуальных каналов.
- **Интерфейс локального управления (local management interface, LMI) —** стандарт сигналов, передаваемых между офисным оборудованием пользователя (CPE) и коммутатором протокола Frame Relay, ответственным за установку связи и поддержку статуса этих устройств. Интерфейсы локального управления могут поддерживать:
    - механизм анализа активности, проверяющий наличие передачи данных по линии;
    - механизм многоадресной передачи (multicast), предоставляющий сетевому серверу свои локальные DLCI;
    - групповую адресацию, предлагая несколько DLCI в качестве адресов для много-

адресной передачи (передачи в несколько пунктов назначения);

- изменение сферы действия DLCI путем придания своим локальным DLCI (используемым только локальным коммутатором) глобального статуса (вся сеть на базе протокола ретрансляции фреймов);
- статусного механизма, придающего выходной статус идентификаторам локального управления, известным только данному коммутатору. Существует несколько типов LMI и поэтому маршрутизаторы должны быть проинформированы об используемом типе LMI. Поддерживаются три типа LMI: `Cisco`, `ansi` и `q933a`.

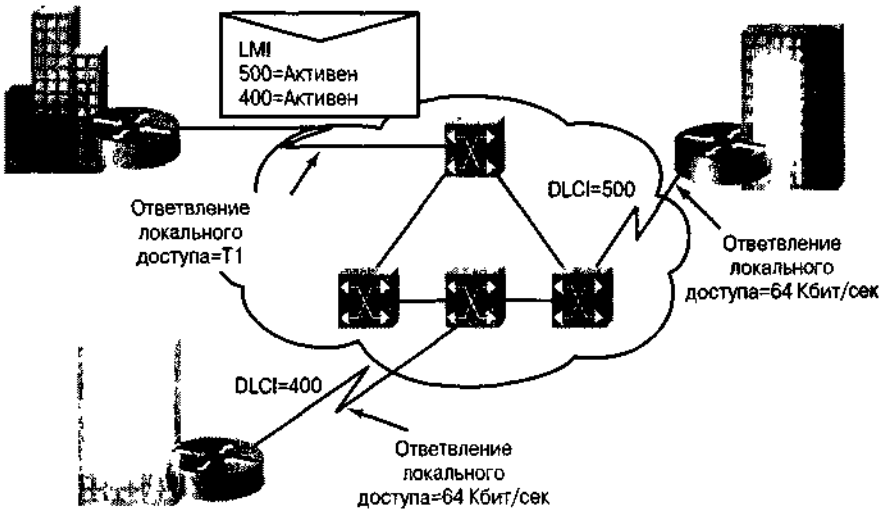


Рис 12 2. Значение DLCI идентифицирует логическое соединение, которое мультиплексируется в физический канал

- Согласованная скорость передачи информации (committed information rate, CIR) представляет собой гарантируемую провайдером услуг скорость передачи в бит/с.
- Согласованный объем — максимальное количество битов, которое коммутатор должен передать за установленный интервал времени с согласованной скоростью.
- Избыточный объем — максимальное количество превышающих CIR битов, которое коммутатор протокола ретрансляции фреймов пытается передать. Это количество зависит от возможностей службы, заложенных производителем оборудования, но обычно ограничено скоростью порта локального ответвления.
- **Прямое явное уведомление о перегрузке (Forward Explicit Congestion Notification, FECN).** В случае, когда коммутатор протокола ретрансляции фреймов обнаруживает в сети затор, он посылает пакет FECN устройству получателя, информируя его о заторе.
- **Обратное явное уведомление о перегрузке (Backward Explicit Congestion Notification, 1**
- **BECN).** Как показано на рис. 12 3, когда коммутатор протокола ретрансляции фреймов обнаруживает в сети затор, он посылает BECN-пакет маршрутизатору сети отправителя с инструкцией уменьшить скорость передачи пакетов. Если маршрутизатор получает такой пакет в текущем временном интервале, то он уменьшает скорость передачи на 25%
- Индикатор разрешения на отбрасывание пакетов (discard eligibility indicator, DE). Когда маршрутизатор обнаруживает в сети затор, коммутатор Frame Relay первыми отбрасывает пакеты с установленным DE-битом. Бит DE устанавливается на пакетах

избыточного потока данных (т.е. превышающего согласованную скорость передачи).

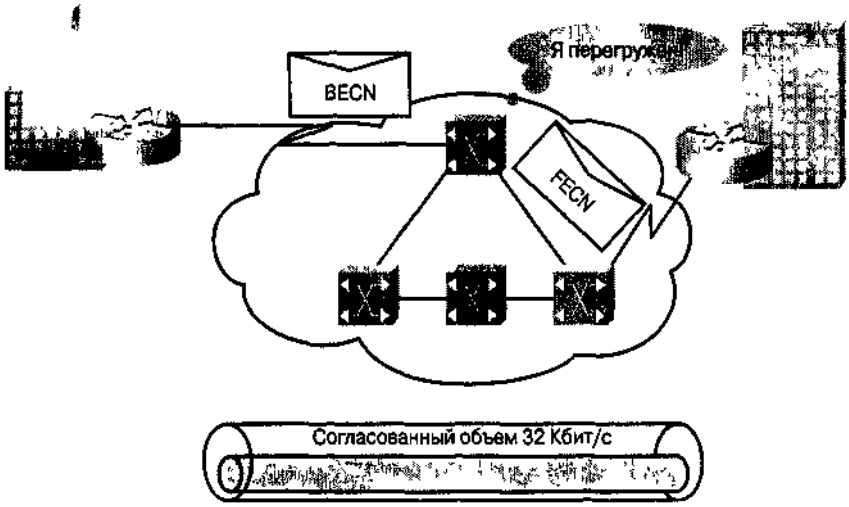


Рис. 12.3 Коммутатор протокола ретрансляции фреймов посылает BECN-пакеты маршрутизатору отправителя с целью снижения или ликвидации перегрузки в сети

Функционирование протокола Frame Relay

Протокол Frame Relay может быть использован в качестве интерфейса к службе, предоставляемой поставщиком услуг, или к сети, оборудование которой принадлежит частному владельцу. Для создания общедоступной службы на основе протокола ретрансляции фреймов коммутирующее оборудование этого протокола размещается на промплощадке (в центральном офисе, телефонной станции) поставщика услуг. В этом случае пользователи получают экономические преимущества за счет использования регулируемой потоком данных скорости передачи, и им не приходится тратить время и усилия на администрирование и поддержку службы и оборудования сети.

Для сетей, использующих протокол Frame Relay, не существует стандарта на оборудование, осуществляющее внутренние коммуникации. Поэтому поддержка интерфейсов протокола Frame Relay не требует обязательного использования этого протокола между сетевыми устройствами Таким образом, как показано на рис 12.4, могут быть использованы традиционная коммутация каналов, пакетная коммутация или комбинированный подход, объединяющий обе эти технологии.

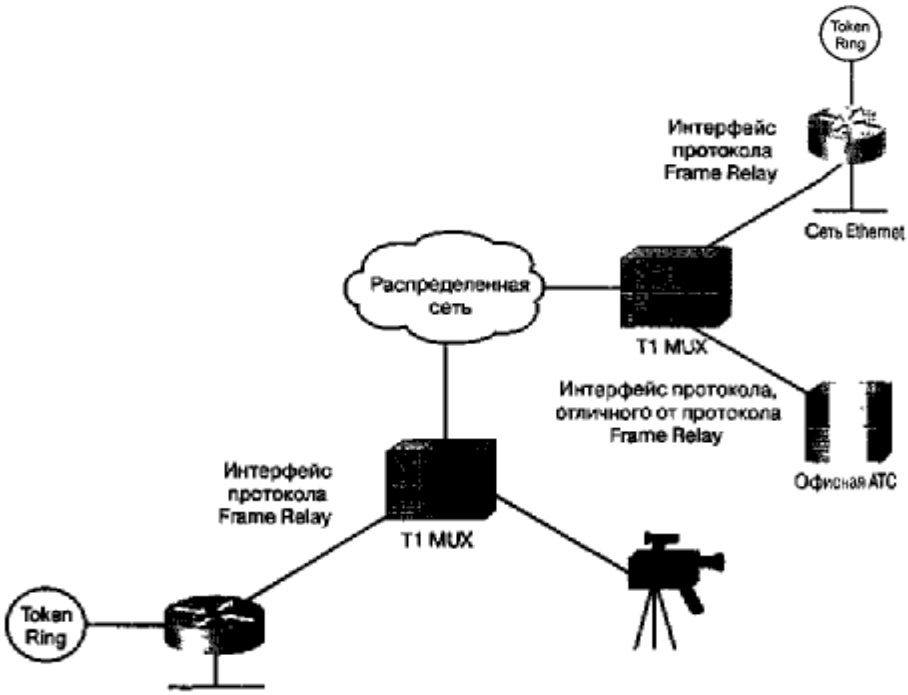


Рис. 12 4 Протокол Frame Relay может использоваться в качестве интерфейса к сети за счет соединения между собой таких устройств, как коммутаторы этого протокола и маршрутизаторы

Линии, соединяющие устройства пользователя с сетевым оборудованием, могут работать со скоростями, выбираемыми из широкого диапазона. Типичными являются скорости от 56 Кбит/с до 2 Мбит/с, хотя протокол ретрансляции фреймов может поддерживать как более высокие, так и более низкие скорости.

DLCI протокола Frame Relay

В качестве интерфейса между оборудованием пользователя и сетевым оборудованием (рис 12.5), протокол Frame Relay предоставляет средства мультиплексирования при обмене данными (называемые *виртуальными каналами, virtual circuits)* через совместно используемую **физическую среду (medium)** путем назначения DLCI каждой паре устройств ОСЕ.

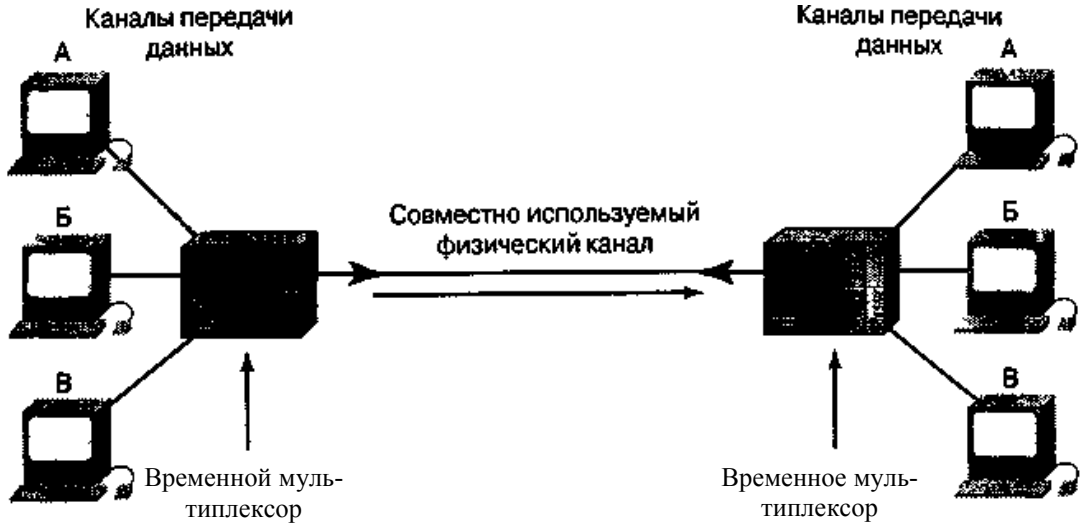


Рис. 125. Одно физическое соединение обеспечивает непосредственную связь со всеми устройствами сети

Мультиплексирование, осуществляемое в соответствии с протоколом Frame Relay, предоставляет более гибкий и эффективный способ использования доступной полосы пропускания. Этот протокол позволяет пользователям совместно использовать одну полосу пропускания, сокращая их финансовые расходы. Например, представим себе, что имеется распределенная сеть, использующая протокол Frame Relay. Этот протокол можно представить как группу дорог, владельцем которых являются телефонные компании, они же занимаются их ремонтом и поддержкой. Можно арендовать дорогу (полосу) исключительно для своей компании (выделенную) или, заплатив меньше, арендовать полосу на совместно используемой дороге. Конечно, протокол Frame Relay может быть полностью реализован и в частных сетях, однако там он редко используется.

Стандарты протокола Frame Relay оговаривают параметры адресации **постоянных виртуальных каналов (permanent virtual circuit, PVC),** которые в сети протокола Frame Relay конфигурируются и управляются администратором. Постоянные виртуальные каналы характеризуются своими идентификаторами DLCI (рис. 12.6). DLCI протокола Frame Relay имеют локальный характер. Это означает, что их значения в распределенной сети протокола ретрансляции фреймов не являются уникальными и могут совпадать. Два устройства DTE, соединенные одним виртуальным каналом, могут использовать различные DLCI для обращения к одному и тому же соединению, как показано на рис. 12.6.

В ситуации, когда протокол Frame Relay предоставляет средства мультиплексирования логического обмена данными, коммутирующее оборудование провайдера службы сначала создает таблицу, задающую значение DLCI выходным портам. При получении фрейма коммутирующее устройство анализирует идентификатор соединения и доставляет фрейм на соответствующий выходной порт. В конечном итоге еще до отправки первого фрейма устанавливается полный путь к пункту назначения.

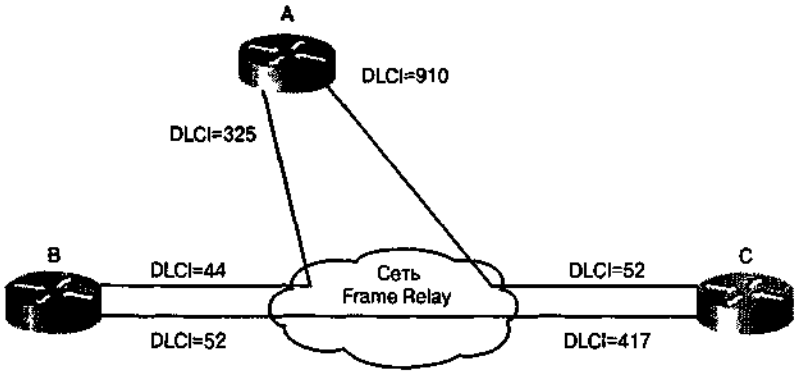


Рис. 12 6. Два конечных устройства на разных концах соединения могут использовать различные номера DLCI для обращения к одному и тому же соединению

Формат фрейма протокола Frame Relay

Формат фрейма протокола Frame Relay показан на рис. 12.7. Поля флагов указывают на начало и конец фрейма. За первым полем флага следуют два байта адресной информации; 10 битов из этих двух байтов представляют собой текущий ID канала (т е. DLCI).

Ниже описаны поля фрейма.

- Флаг — указывает на начало и конец фрейма.
- Адрес — указывает длину адресного поля. Хотя в настоящее время адреса протокола ретрансляции фреймов имеют длину 2 байта, адресные биты позволяют в будущем увеличить длину адреса. Восьмой бит каждого байта адресного поля используется для указания адреса. Адрес содержит следующую информацию
  - Значение DLCI — отображает значение DLCI и состоит из 10 битов адресного поля.
  - Контроль перегрузки — последние 3 бита адресного поля, управляющие механизмами уведомления о перегрузке в сети. Такими механизмами являются FECN, BECN и DE (биты допустимости отбрасывания).
- Данные — поле переменной длины, содержащее инкапсулированные данные и протоколов верхних уровней.
- FCS — последовательность проверки фрейма (frame check sequence, FCS), используемая для обеспечения целостности передаваемых данных.

Длина поля в байтах	1	2	Поле переменной длины	2	1
	Флаг	Адрес, включая DLCI, FECN, BECN и биты DE	Данные	FCS	Флаг

Рис 12 7 Поля флагов задают начало и конец фрейма

Адресация протокола Frame Relay

На рис 12.8 изображены два воображаемых PVC, один между Атлантой и Лос-Анджелесом, другой — между Сан-Хосе и Питтсбургом Для ссылки на свой PVC с Атлантой Лос-Анджелес использует DLCI 22, в то время как Атланта использует для этой же цели DLCI 82. Аналогичным образом, Сан-Хосе использует DLCI 22 для ссылки на свой PVC с Питтсбургом. Сеть использует свои внутренние механизмы для того, чтобы эти два локальных идентификатора PVC имели разные значения.

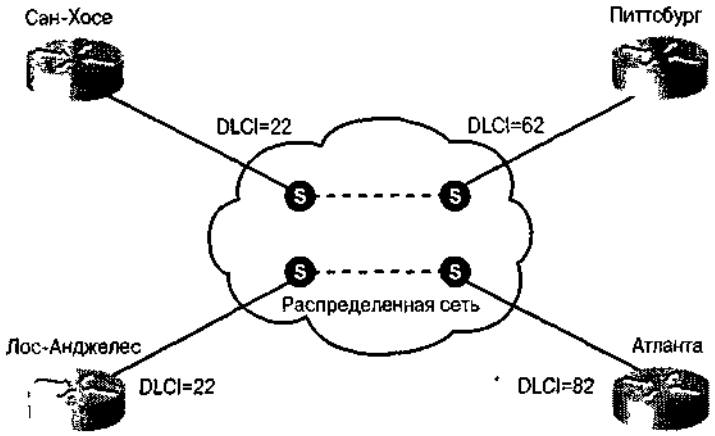


Рис 12.8. Пример использования DLCI в сети протокола Frame Relay

Реализация протокола Frame Relay в маршрутизаторах Cisco — LMI

В истории протокола ретрансляции фреймов важное значение имеет 1990 год, когда компании Cisco Systems, StrataCom, Northern Telecom и Digital Equipment Corporation создали группу с целью концентрации средств и усилий на развитии технологии протокола ретрансляции фреймов и на ускорении внедрения взаимосвязанных программных продуктов этого протокола. Эта группа создала спецификацию, соответствующую базисной версии протокола, но дополнила ее новыми возможностями для сложных сред совместного использования. Эти усовершенствования стали называть *интерфейсом локального управления (Local Management Interface, LMI).*

Функционирование LMI

Главными целями применения LMI являются:

- определение оперативного состояния различных PVC, известных маршрутизатору;
- передача пакетов об активности устройств, с целью удостовериться в том, что PVC продолжает функционировать, а не отключился в связи с простоем (рис. 12.9);
- информирование маршрутизатора о доступных PVC;
- три типа LMI могут быть активизированы следующими командами маршрутизатора ansi, Cisco и q933a.

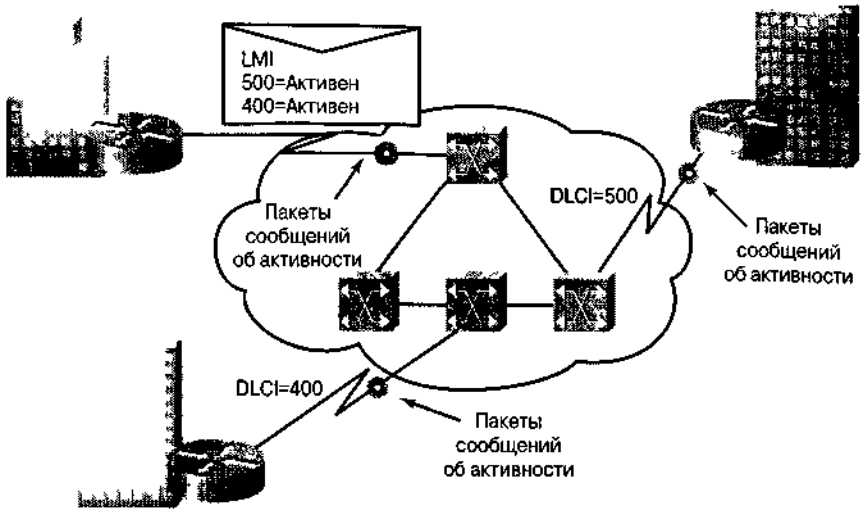


Рис. 12.9. LMI обеспечивают управление соединениями в сети

Дополнительные возможности интерфейса локального управления (LMI)

В дополнение к основным функциям протокола ретрансляции фреймов по передаче данных LMI-спецификация этого протокола включает в себя дополнительные возможности, которые облегчают поддержку больших и сложных сетей совместного использования. Некоторые из этих дополнительных возможностей называются *общими (common)* и могут быть использованы любым устройством, удовлетворяющим требованиям спецификации. Другие функции LMI рассматриваются как *необязательные (optional)*. Приведем полный список дополнительных возможностей, предоставляемых LMI.

- Сообщения о состоянии виртуального канала — они обеспечивают связь и синхронизацию между сетевыми устройствами и устройствами пользователя, периодически сообщая о появлении новых PVC и удалении существовавших, а также информируя о работе сети в целом. Эти сообщения избавляют от ненужной рассылки данных по уже несуществующим каналам.
- Рассылка данных одновременно нескольким получателям (многоадресная рассылка, multicast). Такая рассылка позволяет отправить один фрейм, а сеть обеспечивает его доставку сразу нескольким адресатам. Она является эффективным средством передачи сообщений протокола маршрутизации и протоколов преобразования адресов, которые обычно требуется рассылать одновременно в несколько пунктов назначения.
- Глобальная адресация (необязательная) придает локальному идентификатору соединения глобальный характер, после чего он может быть использован для идентификации конкретного интерфейса во всей сети протокола Frame Relay. Глобальная адресация делает сеть протокола Frame Relay в вопросе адресации похожей на локальную сеть; протоколы преобразования адресов работают в этих двух типах сетей одинаково.
- Простой контроль потока (необязательный) — предоставляет механизм управления потоком типа XON/XOFF, который применяется ко всему интерфейсу. Предназначен для устройств, верхние уровни которых не могут использовать биты уведомления о переполнении и требуют определенного уровня контроля потока данных.

Формат LMI-фрейма

Спецификация протокола Frame Relay также включает в себя процедуры рассылки LMI. Сообщения LMI рассылаются во фреймах, отличающихся друг от друга индивидуальными LMI-идентификаторами (DLCI), определенными в спецификации консорциума как DLCI=1023. Формат фрейма протокола ретрансляции фреймов показан на рис. 12.10.

Длина поля в байтах

1	2	1	1	1	1	Переменное	2	1
Флаг	Идентификатор LMI	Индикатор ненумерованной информации	Дискриминатор протокола	Ссылка на вызов	Тип сообщения	Информационные элементы	FCS	Флаг

Рис. 12.10. В LMI-фреймах базовый протокольный заголовок такой же, как и у обычного фрейма протокола ***Frame*** *Relay*

После поля флага и поля LMI фрейм содержит 4 обязательных байта. Первый из этих обязательных байтов *(индикатор ненумерованный информации, unnumbered information indicator)* имеет такой же формат, как и LAPB-индикатор фрейма *ненумерованной информации (unnumbered information, UI),* в котором последний (poll/final) бит установлен в ноль. Следующий байт, называемый *дискриминатором протокола (protocol discriminator),* содержит значение, определяющее LMI. Третий обязательный байт *(ссылка на вызов, call reference)* всегда заполнен нулями.

Последний обязательный байт представляет собой поле *типа сообщения (message type).* Определены два типа сообщений: сообщения запросов о состоянии и сообщения о текущем состоянии. Сообщения о текущем статусе являются ответами на сообщения-запросы. *Сообщения об активности (keepalive)* (сообщения, посылаемые в оба конца соединения для подтверждения того, что обе стороны продолжают рассматривать соединение как активное) и сообщения о статусе PVC представляют собой примеры таких сообщений. Они являются типичными для LMI, и, как правило, присутствуют в любой реализации сети, соответствующей спецификации протокола Frame Relay.

Вместе взятые, запросы о статусе и ответы на них (сообщения о статусе) помогают проверить целостность логического и физического каналов. Эта информация имеет критически важное значение для маршрутизации, поскольку протоколы маршрутизации принимают решения, основанные на предположении о целостности сети.

Далее следует поле информационного элемента (information element, IE), содержащее переменное количество байтов. За полем типа сообщения находится некоторое количество IE. Каждый информационный элемент состоит из однобайтного *идентификатора IE,* поля длины IE и одного или более байтов, содержащих конкретные данные.

Глобальная адресация

Кроме общих возможностей LMI имеется несколько необязательных, которые, однако, оказываются исключительно полезными при совместном использовании среды. Первой такой возможностью является опция *глобальной адресации (global addressing).* При ее использовании значения, вводимые в DLCI-поле фрейма становятся глобально значимыми адресами индивидуальных устройств конечного пользователя (например, маршрутизаторов). Пример такой адресации приведен на рис. 12.8.

Как уже отмечалось ранее, базовая (нерасширенная) спецификация протокола Frame Relay поддерживает только такие значения поля DLCI, которые имеют локальный характер. В этом случае отсутствуют адреса, идентифицирующие сетевые интерфейсы или узлы, подсоединенные

к этим интерфейсам. Ввиду отсутствия таких адресов они не могут быть найдены обычными методами обнаружения и преобразования адресов. Это означает, что при обычной адресации протокола ретрансляции фреймов необходимо создавать карты статической разметки, которые будут указывать маршрутизаторам, какие DLCI следует использовать для нахождения удаленных устройств и ассоциированных с ними адресов.

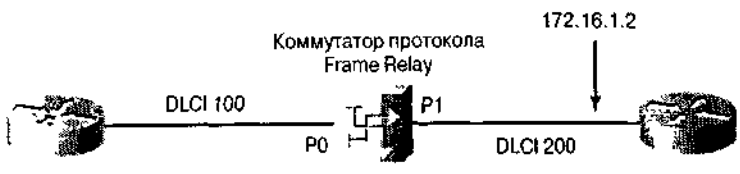
Следует обратить внимание на то, что каждый интерфейс на рис. 12.8 имеет собственный идентификатор. Предположим, что Питтсбург должен отправить фрейм в Сан-Хосе. Идентификатором Сан-Хосе является 22, поэтому Питтсбург помещает значение 22 в поле DLCI и посылает фрейм в сеть протокола Frame Relay. В точке выхода сеть меняет содержимое поля DLCI на 62 для указания на узел, являющийся источником фрейма. Каждому интерфейсу маршрутизатора в качестве идентификатора узла присвоено уникальное значение, поэтому отдельные устройства без труда различаются. Это позволяет выполнять маршрутизацию в сложных средах. В больших разветвленных средах глобальная адресация предоставляет значительные преимущества. В результате сеть протокола Frame Relay выглядит для периферийного маршрутизатора как обычная локальная сеть.

Многоадресная передача

Еще одной ценной особенностью LMI является одновременная передача одного и того же пакета данных нескольким пользователям. Группы многоадресной рассылки задаются последовательностью из четырех зарезервированных значений DLCI (от 1019 до 1022). Фреймы, отправленные устройством, использующим один из этих четырех DLCI, дублируются сетью и рассылаются по всем выходным точкам, указанным в наборе. В многоадресном расширении определены также сообщения LMI, которые уведомляют устройства пользователя о добавлении, удалении и наличии многоадресных групп. В сетях, использующих динамическую маршрутизацию, многие маршрутизаторы должны обмениваться между собой информацией о маршрутах. Сообщения о состоянии сети могут эффективно рассылаться путем использования многоадресных идентификаторов DLCI. Это также позволяет рассылать сообщения отдельным группам пользователей.

Инверсный протокол ARP

Механизм инверсного протокола ARP позволяет маршрутизатору автоматически строить карту отображения протокола Frame Relay, как показано на рис. 12.11. Маршрутизатор узнает используемые DLCI от коммутатора при первоначальном обмене LMI. После этого маршрутизатор посылает запрос инверсного ARP каждому DLCI оля каждого протокола, сконфигурированного и поддерживаемого этим интерфейсом. Возвращаемая инверсным ARP информация используется для построения карты отображения протокола ретрансляции фреймов.



Карта отображения протокола Frame Relay

Адрес следующего маршрутизатора	DLCI
172.16.1.2	100

Коммутационная таблица P0

IN_Port	IN_DLCI	OUT_Port	OUT_DLCI
P0	100	P1	200

Рис. 12.11. Маршрутизатор узнает используемые DLCI от коммутатора протокола ретрансляции фреймов и посылает запрос инверсного ARP каждому DLCI

Отображение в протоколе ретрансляции фреймов

Адрес маршрутизатора следующего перехода, найденный в таблице маршрутизации, должен быть преобразован в DLCI протокола ретрансляции фреймов, как показано на рис. 12.12. Это преобразование осуществляется через структуру данных, называемую *картой отображения протокола Frame Relay (Frame Relay map).* После этого таблица маршрутизации используется для определения адреса следующего перехода или DLCI для выходного потока данных. Эта структура данных может быть статически сконфигурирована на маршрутизаторе или автоматически установлена путем использования возможностей инверсного протокола ARP.

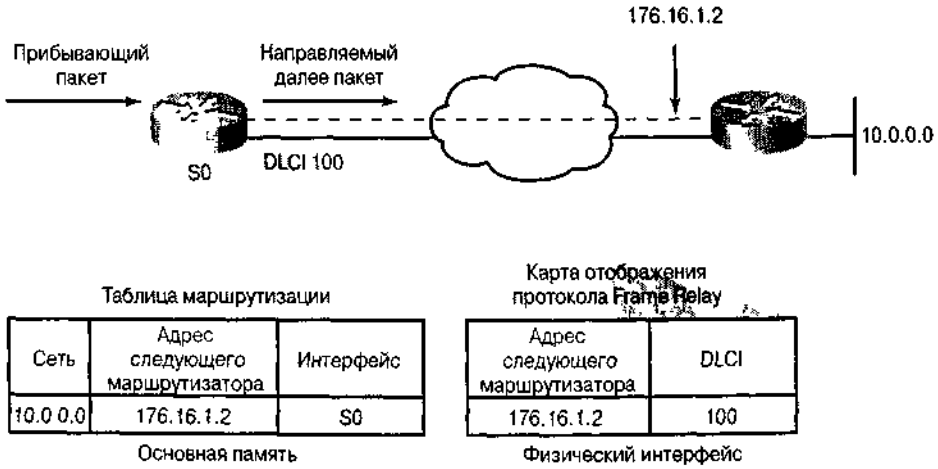


Рис. 12.12. Ответы на запросы инверсного ARP заносятся в таблицу отображения ("адрес–DLCI") маршрутизатора или сервера доступа

Таблицы коммутации протокола Frame Relay

Таблица коммутации протокола Frame Relay состоит из четырех элементов: два — для входного порта и входного DLCI и два — для выходного порта и выходного DLCI, как показано на рис. 12.13. Таким образом, при прохождении каждого коммутатора значение DLCI может быть отображено заново. Поскольку" ссылка на порт может измениться, значения DLCI остаются постоянными.

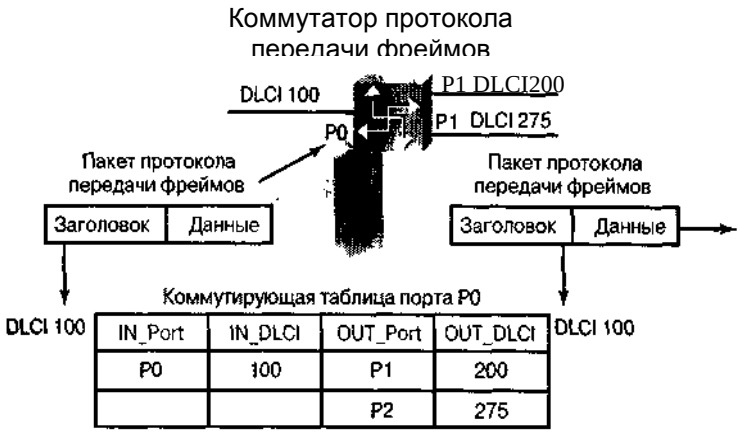


Рис. 12.13. Маршрутизаторы используют инверсный протокол АКР для нахождения удаленных IP-адресов и создания карты отображения локальных DLCI и ассоциированных с ними IP-адресов

Инженерный журнал: общее описание функционирования протокола Frame Relay

После изучения описанных выше операций протокола ретрансляции фреймов можно выполнить следующие действия по реализации этого протокола в сети:

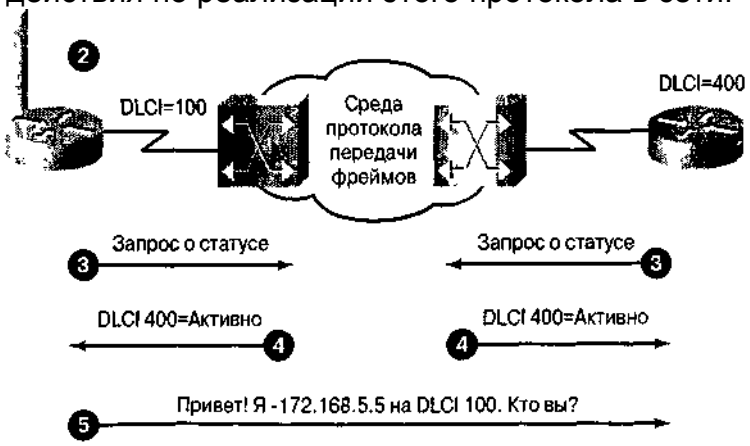


Рис. 12.14. Если инверсный ARP не работает или удаленный маршрутизатор не поддерживает этот протокол, то необходимо сконфигурировать маршруты (т.е. DLCI и IP-адреса) удаленных маршрутизаторов

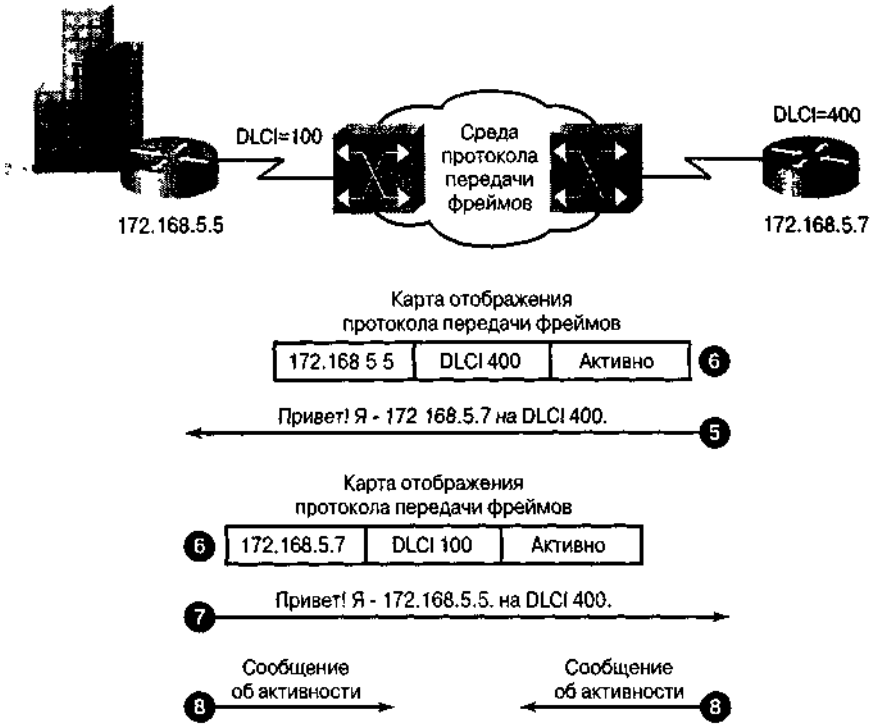


Рис. 12.15. Маршрутизатор изменяет статус каждого DLCI, основываясь на ответе коммутатора протокола ретрансляции фреймов

Этап 1. Следует заказать службу протокола Frame Relay у провайдера или создать собственную среду действия этого протокола.

Этап 2. Подсоединить каждый маршрутизатор, непосредственно или посредством CSU/DSU (модуль канальной службы/модуль цифровой службы) к коммутатору протокола Frame Relay.

Этап 3. Когда маршрутизатор CPE начинает функционировать, он посылает сообщение-запрос о статусе коммутатору протокола Frame Relay. Это сообщение уведомляет коммутатор о статусе этого маршрутизатора и запрашивает у коммутатора информацию о статусе связи других удаленных маршрутизаторов.

Этап 4. После получения коммутатором этого запроса он отвечает сообщением о состоянии, содержащим DLCI всех удаленных маршрутизаторов, которым данный локальный маршрутизатор может посылать данные.

Этап 5. Каждый маршрутизатор рассылает каждому DLCI пакет запроса инверсного ARP, представляя себя и предлагая каждому удаленному маршрутизатору сделать то же, сообщив свой адрес сетевого уровня.

Этап 6. Для каждого DLCI, о котором маршрутизатор получает сообщение инверсного ARP, создается элемент в таблице отображения протокола ретрансляции фреймов, содержащий локальный DLCI и адрес сетевого уровня удаленного маршрутизатора, а также информацию о состоянии канала связи. Отметим, что этот DLCI является локально сконфигурированным, а не тем, который используется удаленным маршрутизатором. В таблице отображения протокола ретрансляции фреймов могут быть зафиксированы три вида состояния канала связи.

- Активное состояние — указывает на то, что канал активен и маршрутизаторы могут обмениваться данными.
- Неактивное состояние — указывает на то, что локальная связь с коммутатором протокола ретрансляции фреймов существует, а связь удаленного маршрутизатора с эти коммутатором отсутствует;

- Отключенное состояние — указывает на то, что от коммутатора не поступило LMI или отсутствует служба между маршрутизатором CPE и коммутатором протокола Frame Relay.

Этап 7. Каждые 60 секунд маршрутизаторы обмениваются сообщениями инверсного протокола ARP.

Этап 8. Каждые 10 секунд (этот интервал устанавливается в параметрах конфигурации) маршрутизатор CPE посылает коммутатору Frame Relay сообщение об активности. Цель рассылки таких сообщений состоит в проверке работоспособности этого коммутатора.

Подынтерфейсы протокола Frame Relay

Для того, чтобы привести в действие механизм рассылки полных сообщений об изменениях маршрутизации в сети протокола Frame Relay необходимо сконфигурировать на маршрутизаторе логически назначаемые интерфейсы, называемые подынтерфейсами (субинтерфейсами). Подынтерфейсы являются логическими разделами одного физического интерфейса. В конфигурации, использующей Подынтерфейсы, каждый постоянный виртуальный канал может быть сконфигурирован как соединение "точка-точка". Это позволяет подынтерфейсу функционировать аналогично выделенной линии, как показано на рис. 12.16.

Рис. 12.16. Сообщения об изменениях маршрутной информации могут рассылаться через Подынтерфейсы так, как если бы они исходили от различных физических интерфейсов

Прежние реализации протокола ретрансляции фреймов требовали, чтобы маршрутизатор (т.е. устройство DTE) имел последовательный интерфейс в распределенной сети для каждого PVC, как показано на рис. 12.17.

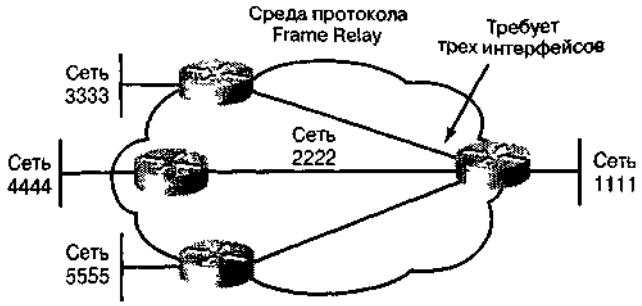


Рис. 12.П. Увеличение количества интерфейсов центрального маршрутизатора эффективно, но значительно увеличивает стоимость сети

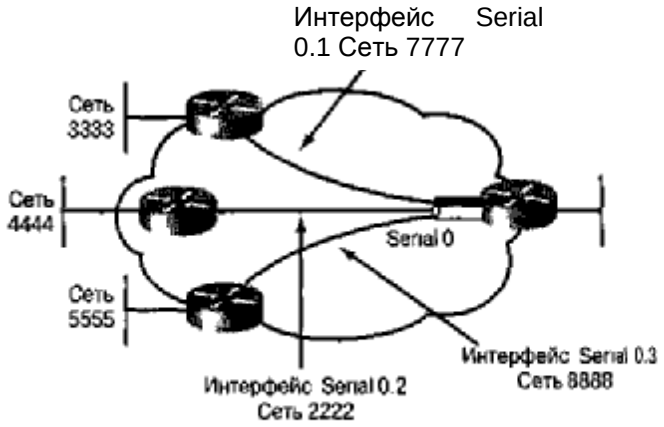


Рис. 12.18. Каждый подынтерфейс рассматривается как отдельная сеть и имеет уникальный номер DLCI

Логическое разделение одного физического последовательного интерфейса распределенной сети на несколько виртуальных подынтерфейсов позволяет существенно уменьшить общую стоимость сети протокола Frame Relay, как показано на рис. 12.18.

Среды с расщеплением горизонта

В средах маршрутизации с расщеплением горизонта маршруты, найденные на одном подынтерфейсе, могут быть сообщены другому подынтерфейсу. Вследствие этого маршрутизация с расщеплением горизонта уменьшает количество петель маршрутизации, не позволяя сообщениям об изменениях в сети, полученных на одном физическом интерфейсе, передаваться через тот же самый физический интерфейс (рис. 12.19). Благодаря этому в ситуации когда удаленный маршрутизатор посылает сообщение об изменении на центральный маршрутизатор, который соединяет несколько виртуальных каналов (PVC) в один физический интерфейс, последний не может передавать этот маршрут другим удаленным маршрутизаторам через тот же физический интерфейс (рис. 12.20).

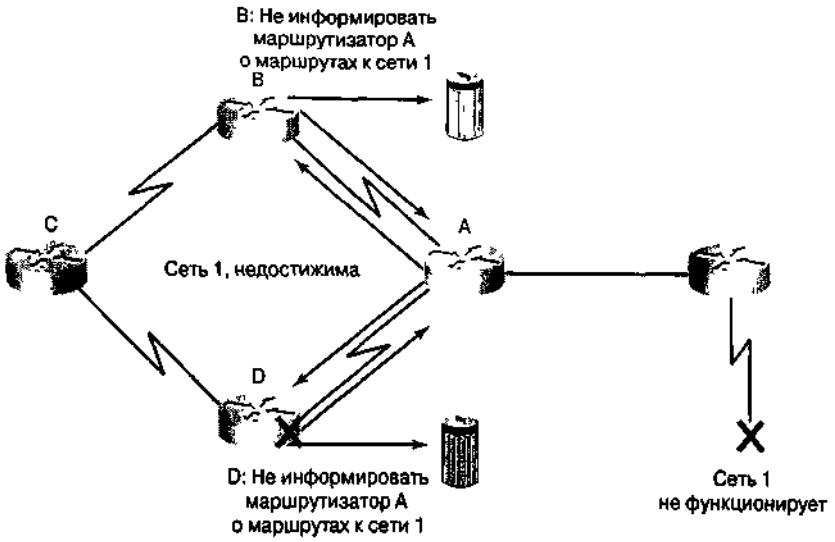


Рис. 12.19. В ситуации, когда используется расщепление горизонта, маршрутизатор, который получил маршрутную информацию через некоторый интерфейс, не посылает вновь информацию об этом маршруте на этот интерфейс

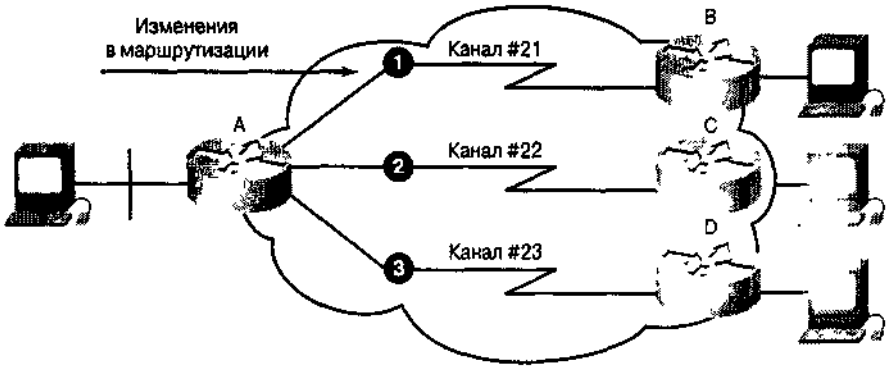


Рис. 12.20. При использовании расщепления горизонта сообщения об изменениях, полученные на центральном маршрутизаторе, не могут передаваться другим маршрутизаторам через тот же самый физический интерфейс

Разрешение проблем достижимости посредством использования подынтерфейсов

Подынтерфейс может быть сконфигурирован для обеспечения поддержки соединений перечисленных ниже типов.

- *Соединение типа "точка-точка"*. При этом отдельный подынтерфейс используется для установки соединения PVC с другим физическим интерфейсом или подынтерфейсом на удаленном маршрутизаторе. В этом случае подынтерфейсы оказываются в одной подсети и каждый из них имеет отдельный DLCI. Каждое соединение типа "точка-точка" является отдельной подсетью. В такой ситуации проблемы широковещательной передачи отсутствуют, поскольку маршрутизаторы непосредственно соединены друг с другом и функционируют как выделенная линия
- *Многоточечное соединение* Один подынтерфейс используется для установки нескольких PVC-соединений с несколькими физическими интерфейсами или подынтерфейсами удаленных маршрутизаторов В этом случае все участвующие интерфейсы будут находиться в одной и той же подсети и каждый интерфейс будет иметь собственный локальный DLCI Поскольку подынтерфейс в такой среде действует как

обычная сеть протокола Frame Relay, сообщения об изменениях подвергаются расщеплению горизонта

Базовая конфигурация протокола Frame Relay

В базовом варианте предполагается, что настройка параметров протокола Frame Relay устанавливается на одном или нескольких физических интерфейсах (рис. 12.21), а LMI и инверсный ARP поддерживаются удаленным маршрутизатором (маршрутизаторами). В такой среде LM1 сообщает маршрутизатору о доступных DLCI. Инверсный ARP включен по умолчанию, поэтому данные о нем не появляются при выводе информации о конфигурации сети. Для установки базовой конфигурации протокола Frame Relay необходимо выполнить следующие действия:

Этап 1. Выбрать интерфейс и перейти в режим установки конфигурации:

Router(config)# interface serial 0

Этап 2. Сконфигурировать адрес сетевого уровня, например, IP-адрес:

```
Router(config-if)# ip address 192.168.38.40 255.255.255.0
```

Этап 3. Выбрать тип инкапсуляции для потока данных, передаваемого от одного конца сети к другому.

```
Router(config)# encapsulation frame relay [ Cisco | letf ]
```

где-

- **cisco** — значение, принимаемое по умолчанию, которое используется при соединении с другим маршрутизатором Cisco;
- **ietf** — используется для подсоединения всех отличных от Cisco маршрутизаторов

Этап 4. Если используется версия ОС Cisco 11.1 или более ранняя, то необходимо указать тип LMI, используемый коммутатором протокола Frame Relay:

```
Router(config-if)I frame-relay Imi-type { ansi I cisco | q933I }
```

где значение cisco принимается по умолчанию
При использовании версии 112 или более поздней тип LMI распознается автоматически, поэтому при установке конфигурации его задавать не требуется

Этап 5. Задать ширину полосы пропускания данного канала'

```
Router (config-if)# bandwidth полоса
```

Эта команда воздействует на процесс маршрутизации таких протоколов, как IGRP, поскольку она определяет метрику канала

Этап 6. Если инверсный протокол ARP был на маршрутизаторе отключен, то его следует снова включить (он является включенным по умолчанию):

Router(config-if)# **frame-relay inverse-arp** [протокол] *[dlci]*

где

- *протокол* — название одного из поддерживаемых протоколов, таких как IP, IPX, Apple Talk, DECNet, VINES или XNS
- *dlci* — DLCI локального интерфейса, с которым предполагается обмениваться сообщениями инверсного ARP.

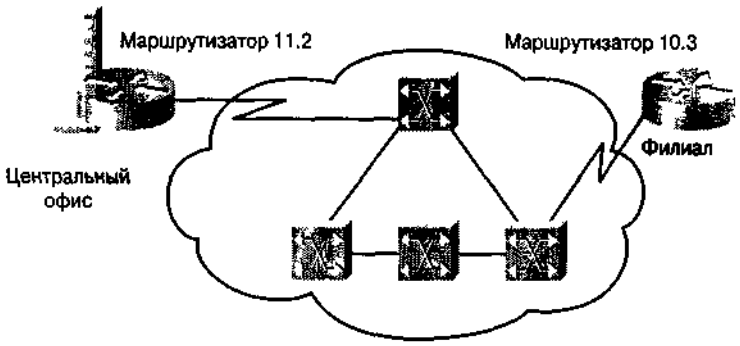


Рис 12 21 После установки надежного соединения с коммутатором протокола Frame Relay на обоих концах РУС следует начать процесс конфигурации протокола Frame Relay

---

Инженерный журнал : обеспечение безопасности сети при ее конфигурировании

Для предотвращения несанкционированного доступа к сети рекомендуется при установке конфигурации сети предпринять некоторые действия по обеспечению безопасности, такие, например, как задание имени хоста и пароля

Этап 1. Задать на маршрутизаторе имя хоста, которое будет использоваться в приглашениях и именах файлов конфигурации При использовании аутентификации протокола PPP имя, введенное этой командой, должно соответствовать имени пользователя, указанного на маршрутизаторе центрального сайта

```
Router(config) # hostname 1600
```

Этап 2. Указать пароль для предотвращения несанкционированного доступа к маршрутизатору:

```
1600(config)# enable password 1600user
```

Тестирование протокола Frame Relay

После установки конфигурации протокола Frame Relay можно убедиться в том, что все соединения активны, выполнив одну из команд show.

Команда	Описание
show interfaces serial	Отображает информацию о DLCI, используемых при групповой передаче, о DLCI, используемых на последовательных интерфейсах, сконфигурированных под протокол ретрансляции фреймов, а также о DLCI интерфейса локального управления (LMI), используемого для LMI
show frame-relay pvc	Отображает статус каждого сконфигурированного соединения и статистику потока данных. Эта команда также полезна для того, чтобы узнать количество BECN- и FECN-пакетов, полученных маршрутизатором
show frame-relay map	Отображает адрес сетевого уровня и ассоциированный с ним DLCI для каждого удаленного устройства, с которым со-

единен локальный маршрутизатор

show frame-relay lmi	Отображает статистику потока данных LMI. Например, выводится количество сообщений о статусе, которыми обменялись локальный маршрутизатор и коммутатор протокола ретрансляции фреймов

Проверка работоспособности канала

Для проверки работоспособности канала следует выполнить перечисленные ниже действия.

Этап 1. В привилегированном командном режиме (EXEC) необходимо ввести команду **show interface serial 0.**

В результате ее выполнения будет получена следующая информация:

```
1600# show interface serial 0
Serial0 is up, line protocol is up
Hardware is QUICC Serial
MTU 1500 bytes, BW 1544 Kbit,
     DLY 2000 usec, rely 255/255, load 1/255
Encapsulation FRAME-RELAY
     loopback not set, keepalive set (10 sec)
LMI enq sent 163, LMI stat recvd 136,
     LMI upd recvd 0, DTE LMI up
LMI enq recvd 39, LMI stat sent 0, LMI upd sent 0
LMI DLCI 1023 LMI type is CISCO frame relay DTE
Broadcast queue 0/64, broadcasts sent/dropped 27/0,
     interface broadcast 28
Last input 00:00:01, output 00:00:05, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0 (size/max/drops);
     Total output drops: 0
Queuing strategy: weighted fair
Output queue: 0/64/0 (size/threshold/drops)
Conversations 0/1 (active/max active)
Reserved Conversations 0/0 (allocated/max allocated)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
1813 packets input, 109641 bytes, 0 no buffer
Received 1576 broadcasts, 0 runts, 0 giants
13 input errors, 0 CRC, 13 frame, 0 overrun,
     0 ignored, 0 abort
1848 packets output, 117260, 0 underruns
0 output errors, 0 collisions, 32 interface resets
0 output buffer failures, 0 output buffers swapped out
29 carrier transitions
DCD=up DSR=up DTR=up RTS=up CTS=up
```

Этап 2. Следует удостовериться, что в вышеприведенном выводе имеются следующие (выделенные) строки:

- SerialO is up, line protocol is up — означает, что соединение протокола Frame Relay является активным;
- LMI enq sent 163, LMI stat recvd 136 — означает, что соединение отправляет и получает данные. Количество принятых и переданных данных, естественно, будет отличаться от приведенного в данном примере;
- LMI type is Cisco — означает, что тип LMI для данного маршрутизатора сконфигурирован правильно.

Этап 3. Если последнее сообщение при выводе отсутствует, то следует удостовериться в

том, что:

- установка LMI провайдером службы протокола Frame Relay соответствует данному каналу;
- происходит рассылка сообщений об активности и маршрутизатор получает сообщения об изменениях LMI.

Этап 4. Для того, чтобы продолжить установку конфигурации, следует вновь войти в глобальный режим

Проверка наличия карты отображения

Для того, чтобы убедиться в наличии таблицы отображения протокола ретрансляции фреймов, необходимо выполнить следующие действия.

Этап 1. Находясь в привилегированном командном режиме (EXEC), ввести команду show frame-relay map. Проверить, что сообщение status defined, active (в примере выделено) появляется для каждого последовательного интерфейса.

```
16001 show frame-relay map

Serial0.1 (up): point-to-point dlci, dlci 17(0x11,0x410),
broadcast, status defined, active
```

Этап 2. Если такое сообщение не появляется, то необходимо:

- удостовериться в том, что маршрутизатор центрального сайта подсоединен и сконфигурирован;
- проверить вместе с провайдером протокола Frame Relay, что канал функционирует правильно.

Этап 3. Для того, чтобы продолжить конфигурирование, следует вновь перейти в глобальный режим установки конфигурации

Проверка связи с маршрутизатором центрального сайта

Для того, чтобы убедиться в наличии связи с маршрутизатором центрального сайта, необходимо выполнить следующие действия.

Этап 1. Находясь в привилегированном режиме (EXEC), ввести команду ping, после которой должен быть указан IP-адрес маршрутизатора центрального сайта.

Этап 2. Обратите внимание на строку Success rate... (в примере она выделена).

```
1600# ping  192.168.38.40
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.38.40,
       timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5),
 round-trip min/avg/max =32/32/32 ms
1600#
```

Если доля успешного обмена равна 10% или больше, то этот этап тестирования можно считать успешно выполненным.

Этап 3. Для продолжения установки конфигурации следует вновь перейти в глобальный режим.

Инженерный журнал: конфигурирование Ethernet-интерфейса

Для установки конфигурации Ethernet-интерфейса (соединяющего маршрутизатор с локальной сетью), использующего IP- и IPX-маршрутизацию и сетевые адреса, следует выполнить следующие действия.

Этап 1. Войти в режим установки конфигурации интерфейса сети Ethernet:

1600 (config)# **interface ethernet** 0

Этап 2. Задать для этого интерфейса IP-адрес и маску подсети:

1600(config-if)# **ip address** 172.16.25.1 255.255.255.0

Этап 3. Включить на данном интерфейсе IPX-маршрутизацию:

```
1600 (config-if)# ipx network номер
```

Этап 4. Активизировать интерфейс, чтобы учесть только что внесенные изменения в параметры его конфигурации:

```
1600 (config-if)# no shutdown
```

Этап 5. Выйти из режима установки конфигурации данного интерфейса:

1600(config-if)# **exit**

Конфигурирование последовательного интерфейса для подключения по протоколу Frame Relay

Для установки на последовательном интерфейсе типа инкапсуляции пакетов, используемого протоколом Frame Relay, необходимо выполнить следующие действия.

Этап 1. Войти в режим установки конфигурации последовательного интерфейса: 1600(config)# **interface serial** 0

Этап 2. Установить на этом интерфейсе метод инкапсуляции протокола ретрансляции фреймов:

1600(config-if)# **encapsulation frame-relay**

Этап 3. Разрешить изменение конфигурации этого интерфейса:

```
1600(config-if)# no shutdown
```

Проверка конфигурации протокола Frame Relay

Для проверки правильности установленной на данный момент конфигурации можно удостовериться, что тестируемый PVC является активным для канала протокола Frame Relay. Для этого выполните следующие действия.

Этап 1. Ввести команду **encapsulation frame-relay** и подождать 60 секунд.

Этап 2 В привилегированном EXEC-режиме ввести команду

show frame-relay pvc

Этап 3. Проверить, что в выводе упомянутой выше команды имеется сообщение (в примере выделенное жирным шрифтом) PVC STATUS=ACTIVE:

```
1600# show frame relay pvc
PVC Statistics for interface Serial0 (Frame Relay DTE)
DLCI=17, DLCI USAGE=LOCAL, PVC STATUS =ACTIVE, INTERFACE =Serial0.1
input pkts 45 output pkts 52 in bytes 7764
out bytes 9958 dropped pkts 0 in FECN pkts 0
in BECN pkts 0 out FECN pkts 0 out BECN pkts 0
```

```
in DE pkts 0 out DE pkts 0
pvc create time 00:30:59, last time pvc status changed
00:19:21
```

Этап 4. Рекомендуется запомнить номер, указанный в сообщении DLCI= ... (в данном примере этот номер равен 17). Он будет использован при завершении конфигурирования интерфейса протокола ретрансляции фреймов.

Этап 5. Если после ввода команды ничего не произойдет, то следует выполнить команду **show interfaces serial 0** для выяснения активности данного последовательного интерфейса. Пример такой команды приведен в следующем разделе. Первая строка вывода должна выглядеть следующим образом:

SerialO is up, line protocol is up

Если первой строкой вывода является `SerialO is up, line protocol is down`, то необходимо проверить на коммутаторе протокола ретрансляции фреймов правильность установки типа LMI. Это можно выяснить из строки вывода `LMI type is CISCO`, содержащейся в том же тексте вывода.

Этап 6. Для продолжения установки конфигурации следует вновь перейти в глобальный режим.

Инженерный журнал : конфигурирование доступа к консоли маршрутизатора

Для задания параметров, управляющих доступом к маршрутизатору, таких как используемый маршрутизатором тип терминальной линии, длительность ожидания маршрутизатором регистрации пользователя и пароль, используемый для начала сеанса работы с маршрутизатором, необходимо выполнить следующие действия.

Этап 1. Указать номер линии консольного терминала:

1600(config)# line console 0

Этап 2. Установить интервал, в течение которого командный интерпретатор EXEC ожидает появления ввода пользователя:

1600 (config-line)# **exec-timeout 5**

Этап 3. Указать виртуальный терминал для доступа к удаленной консоли:

1600(config-line)# **line vty** 0 4

Этап 4. Указать пароль:

1600(config-line)# **password** *lineaccess*

Этап 5. Включить проверку пароля в начале терминального сеанса:

1600 (config-line)# **login**

Этап 6 Выйти из режима установки конфигурации:

1600 (config-line)# **end**

Конфигурирование подынтерфейсов

Для установки конфигурации подынтерфейсов на одном физическом интерфейсе, как показано на рис. 12.22, необходимо выполнить следующие действия.

Этап 1 Выбрать интерфейс, на котором будут созданы подынтерфейсы и войти в режим установки конфигурации.

Этап 2. Удалить все адреса сетевого уровня, назначенные данному физическому интер-

фейсу. Если физический интерфейс имеет адрес, то локальные интерфейсы не будут получать фреймы.

Этап 3. Сконфигурировать инкапсуляцию протокола ретрансляции фреймов, как это было описано выше в разделе "Базовая конфигурация протокола Frame Relay".

Этап 4. Выбрать подынтерфейс, который требуется сконфигурировать:

Router(config-if)# **interface serial** номер.*номер-подынтерфейса* { **multipoint | point-to-point** }

где:

- *номер.номер-подынтерфейса* — представляет собой номер подынтерфейса, лежащий в диапазоне от 1 до 4 294 967 293. *Номер* интерфейса, предшествующий точке, должен соответствовать номеру интерфейса, которому принадлежит подынтерфейс.
- multipoint — используется, если требуется, чтобы маршрутизатор направлял далее принимаемые им широковещательные сообщения и сообщения об изменениях маршрутной информации. Это значение следует выбрать если используется IP-маршрутизация и желательно объединить все маршрутизаторы в одну и ту же подсеть (рис. 12.23).
- point-to-point — используется в том случае, когда не требуется, чтобы маршрутизатор направлял далее принимаемые им широковещательные сообщения и сообщения об изменениях маршрутов в сети, а также в случае, когда требуется чтобы каждая пара маршрутизаторов, образующая соединение "точка-точка" имела собственную подсеть (рис. 12.24).

Выбор одного из двух значений: point-to-point или multipoint является обязательным; значения по умолчанию не предусмотрено.

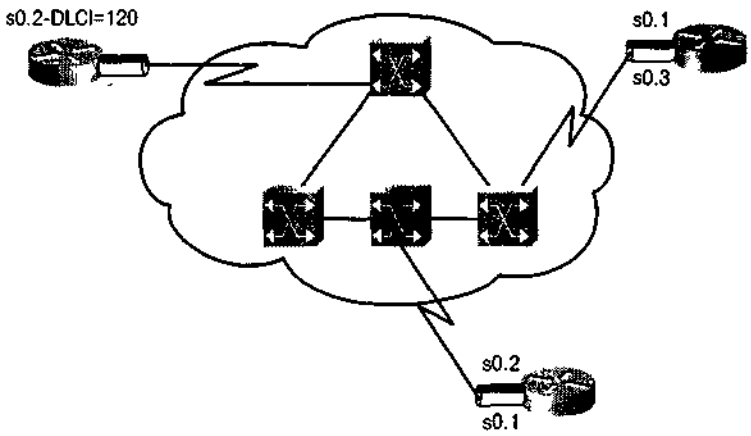


Рис. 12.22. В подынтерфейсе "точка-точка" для каждого соединения назначается отдельная подсеть

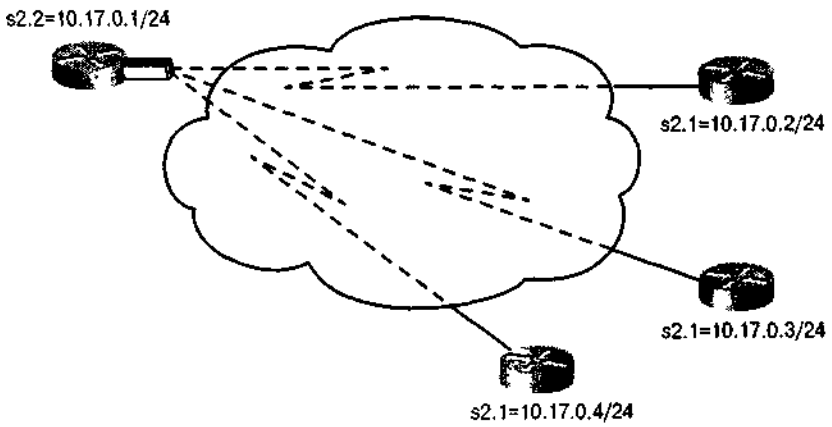


Рис. 12.23. При использовании многоточечной конфигурации требуется только одна сеть или подсеть

Этап 5. Сконфигурировать на подынтерфейсе адрес сетевого уровня. Если подынтерфейс имеет тип point-to-point и используется протокол IP, то можно использовать команду **ip unnumbered:**

```
Router(config-if)# ip unnumbered интерфейс
```

Если требуется использовать эту команду, то желательно, чтобы рассматриваемый интерфейс был интерфейсом обратной петли. Это связано с тем, что канал протокола ретрансляции фреймов не будет работать, если в данной команде указан интерфейс, работающий со сбоями, а интерфейсы обратной петли обладают весьма высокой надежностью.

Этап 6 Если была установлена конфигурация **multipoint** или **point-to-point**, то необходимо изменить локальный DLCI для подынтерфейса, для того, чтобы его можно было отличить от физического интерфейса:

Router(config-if)# **frame-relay interface-dlci** *номер-did*

где:

- *номер-did* — определяет локальный номер DLCI, связанный в настоящий момент с данным подынтерфейсом. Это единственный способ связать определяемый LMI постоянный виртуальный канал с подынтерфейсом, поскольку LMI не знает о существовании подынтерфейсов.

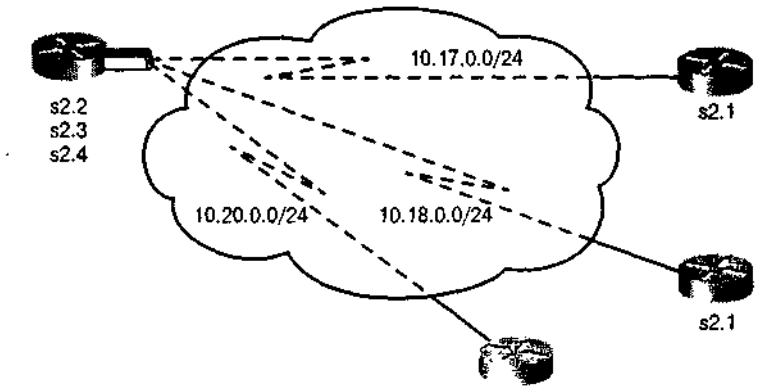


Рис. 12.24. В конфигурации подынтерфейса типа point-to-point *по-дынтерфейс функционирует как выделенная линия*

Эту команду необходимо выполнить для всех подынтерфейсов типа point-to-point. Она также необходима для всех многоточечных подынтерфейсов, для которых включен инверсный протокол ARP. Однако она не требуется для многоточечных подынтерфейсов, на которых установлена статическая разметка маршрутов.

Эта команда не используется для физических интерфейсов.

Примечание

Если подынтерфейс определен как point-to-point, его нельзя переназначить на multipoint с тем же номером без предварительной перезагрузки маршрутизатора. Однако такой перезагрузки можно избежать, задав этому подынтерфейсу другой номер.

Необязательные команды конфигурирования

При необходимости на маршрутизаторе можно указать дополнительные параметры соедине-

ния посредством использования следующей команды:

router(config-if)# **frame-relay map** *протокол протокольный-адрес dlci* **[broadcast] [ietf | cisco | payload-compress | packet-by-packet]**

В приведенной ниже таблице описаны различные параметры этой команды.

Параметр	Описание
протокол	Задает тип поддерживаемого протокола, способ использованиямоста или управления логическим каналом
протокольный-адрес	Определяет адрес интерфейса сетевого уровня маршрутизатора
dlci	Определяет локальный DLCI, используемый для соединения судаленным протокольным адресом
broadcast	(Необязательный параметр) Направляет широковещательные сообщения на этот адрес в случае, когда не включен режим групповой рассылки Используется в случае, когда требуется, чтобы маршрутизатор направлял дальше сообщения об изменении маршрутной информации
ietf I cisco	(Необязательный параметр) Выбирает тип инкапсуляции протокола ретрансляции фреймов. Если удаленный маршрутизатор является маршрутизатором Cisco, то следует использовать значение cisco, в противном случае — значение ietf
payload-compress и packet-by-packet	(Необязательный параметр) Задает использование режима сжатия пакетов при загрузке методом Стеккера (Stacker)

Обычно инверсный протокол ARP используется при запросе протокольного адреса следующего перехода для некоторого соединения. Ответы на эти запросы помещаются в таблицу отображения (т.е. составляется карта отображения протокола ретрансляции фреймов, как показано на рис. 12.25). После этого карта используется для маршрутизации выходного потока данных. Если удаленный маршрутизатор не поддерживает инверсный ARP, то при установке протокола OSPF поверх протокола ретрансляции фреймов или в случае когда желательно контролировать широковещательные сообщения при маршрутизации, необходимо определить таблицу отображения статически. Элементы такой таблицы называют *статическими картами (static map).*

При использовании протокола ретрансляции фреймов можно увеличить или уменьшить интервал отправки сообщений об активности, т.е. период времени, по истечении которого интерфейс маршрутизатора посылает сообщение об активности коммутатору протокола ретрансляции фреймов. По умолчанию он равен 10 секундам, а изменить его можно выполнив команду:

```
router(config-if)# keepalive число
```

Параметр *число* задает значение интервала в секундах. Обычно это значение устанавливается на 2—3 секунды меньшим, чем установленное на коммутаторе протокола ретрансляции фреймов. Это делается для обеспечения синхронизации работы этих устройств.

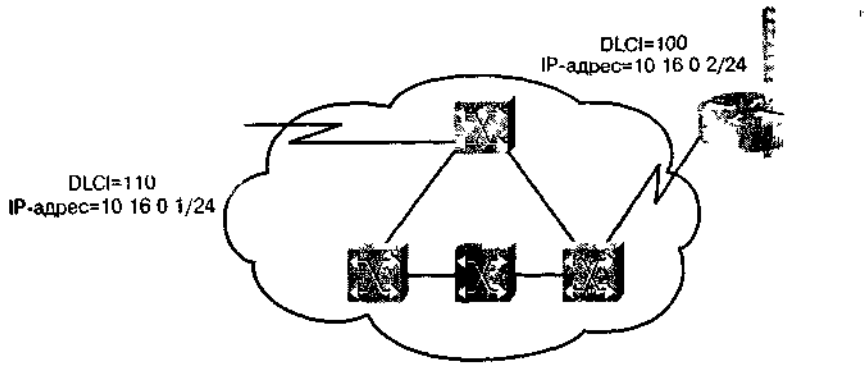


Рис 12 25 Ответы на запросы инверсного ARP об адресе следующего перехода заносятся в таблицу отображения инверсного протокола ARP

Если в сети не используется LMI или осуществляется взаимное тестирование маршрутизаторов, то каждому из локальных интерфейсов следует назначить DLCI посредством следующей команды

```
router(config-if)# frame-relay local-dlci число
```

Здесь параметр *число* представляет собой DLCI используемого локального интерфейса.

Резюме

- Технология распределенных сетей, использующая протокол ретрансляции фреймов, представляет собой гибкий метод установки связи между локальными сетями через каналы распределенных сетей.
- Протокол ретрансляции фреймов обеспечивает возможность пакетно-коммутируемой передачи данных через интерфейс между устройствами пользователя (такими, как маршрутизаторы, мосты и хосты) и сетевым оборудованием (таким, как коммутирующие узлы).
- Для установки соединения через каналы распределенных сетей протокол ретрансляции фреймов использует виртуальные каналы.
- Главными целями применения LMI являются:
- определение оперативного состояния различных PVC, известных маршрутизатору;
- передача пакетов об активности устройств, с целью удостовериться в том, что PVC продолжает функционировать, а не отключился в связи с бездействием;
- информирование маршрутизатора о доступных PVC;
- возможность автоматического построения карты отображения протокола ретрансляции фреймов с использованием механизма инверсного ARP,
- преобразование определенного по таблице маршрутизации адреса следующего перехода в DLCI протокола ретрансляции фреймов
- Протокол ретрансляции фреймов может разделить один физический интерфейс распределенной сети на несколько подынтерфейсов
- В среде маршрутизации с расщеплением горизонта маршруты, полученные с одного интерфейса могут быть сообщены другому интерфейсу.

Задачи проекта Вашингтонского учебного округа: протокол ретрансляции фреймов

В настоящей главе были описаны основные понятия и процесс конфигурирования, которые помогают реализовать канал протокола ретрансляции фреймов в сети Вашингтонского учебного округа. Настройка параметров конфигурации и реализация протокола включает в себя, в частности, решение перечисленных ниже задач.

1. Документирование процесса установки протокола ретрансляции фреймов в распределенную сеть, которое должно включать в себя:

- запись номеров DLCI;
- значение CIR;
- Описание всех устройств передачи данных, необходимых для установки протокола ретрансляции фреймов на маршрутизаторе.

2. Документирование всех команд маршрутизатора, с помощью которых осуществляется процесс развертывания протокола Frame Relay на маршрутизаторе.

Контрольные вопросы

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

1. Каким образом протокол ретрансляции фреймов обрабатывает несколько потоков обмена данными по одному физическому соединению?
   A. Они передаются в дуплексном режиме;
   B. Он мультиплексирует каналы;
   C. Он конвертирует их в ячейки ATM;
   D. Этот протокол допускает передачу нескольких потоков данных одновременно.

2. Какие из перечисленных ниже протоколов используются протоколом ретрансляции фреймов для коррекции ошибок?
   A. Протоколы физического и канального уровней.
   B. Протоколы верхнего уровня.
   C. Протоколы нижнего уровня.
   D. Протокол ретрансляции фреймов не выполняет коррекции ошибок.

3. Что из перечисленного ниже позволяет протоколу ретрансляции фреймов сделать свои DLCI глобальными?
   A. Он передает их широковещательном режиме.
   B. Он высылает несколько сообщений отдельным получателям.
   C. Он рассылает сообщения сразу нескольким получателям.
   D. DLCI не могут стать глобальными.

4. Какая из перечисленных ниже скоростей является той скоростью, на которой коммутатор протокола ретрансляции фреймов будет передавать данные?
   A. Согласованная скорость передачи информации (CIR).
   B. Скорость передачи данных.
   C. Скорость синхронизации.
   D. Скорость в бодах (бит/сек).

5. Кто из перечисленных ниже назначает номера DLCI?
   A. Конечный пользователь.
   B. Корневое устройство сети.
   C. Сервер DLC1.
   D. Провайдер службы.

6. В какое из перечисленных ниже полей заголовка протокола ретрансляции фреймов

включается информация DLCI?

A. В поле флага.
B. В поле адреса.
C. В поле данных.
D. В поле контрольной суммы.

7. Что из перечисленного ниже позволяет протоколу ретрансляции фреймов поддерживать PVC в активном состоянии?

A. Соединение типа "точка-точка",
B. Интерфейс сокетов Windows.
C. Сообщения об активности.
D. Переход PVC в неактивное состояние.

8. Как протокол ретрансляции фреймов использует запросы инверсного ARP?

A. Он конвертирует IP-адреса в MAC-адреса.
B. Он конвертирует MAC-адреса в IP-адреса.
C. Он конвертирует MAC-адреса в сетевые адреса.
D. Он использует таблицу отображения IP-адресов в DLCI.

9. Что из перечисленного ниже используется в протоколе ретрансляции фреймов для определения адреса следующего перехода?

A. Таблица ARP.
B. Таблица маршрутизации протокола RIP.
C. Таблица отображения протокола ретрансляции фреймов.
D. Таблица маршрутизации протокола IGRP.

10. Для какой цели из перечисленных ниже протокол ретрансляции фреймов использует расщепление горизонта?

A. Для увеличения числа сообщений об обновлении маршрутной информации.
B. Для предотвращения маршрутных петель.
C. Для увеличения времени конвергенции.
D. Протокол ретрансляции фреймов не использует расщепление горизонта.

Основные термины

Идентификатор канального соединения (data-link connection identifier, DLCI). Значение, которое определяет PVC или SVC в сети Frame Relay. В базовой спецификации Frame Relay DLCI-идентификаторы являются локальными (для указания одного и того же соединения подключенные устройства могут использовать разные значения), а в расширенной спецификации LMI — глобальными (указывают на отдельные оконечные устройства).

Интерфейс локального управления (local management interface, LMI). Набор усовершенствований основной спецификации Frame Relay. Он включает в себя:

- механизм многоадресной передачи (multicast), предоставляющий сетевому серверу свои локальные и многоадресные DLCI;
- механизм глобальной адресации, который назначает DLCI-интерфейсам глобальное, а не локальное значение в сетях Frame Relay
- механизм извещений об активности, который проверяет состояние канала передачи данных;
- механизм определения статуса, который предоставляет отчет о текущем состоянии известных коммутатору DLCI-интерфейсов. В терминологии ANSI LMI называется LMT.

Обратное явное уведомление о перегрузке (backward explicit congestion notification, BECN). Бит, устанавливаемый во фреймах протокола Frame Relay, которые передаются в направлении, обратном тому, в котором передаются кадры, столкнувшиеся с перегруженным маршрутом. DTE-устройства, получающие фреймы с установленным BECN-битом могут потребовать, чтобы протоколы высшего уровня предприняли соответствующие действия по управлению потоком данных.

Открытая сеть передачи данных (public data network, PDN). Принадлежащие государству (как в Европе) или частным концернам (как в США) сети, обеспечивающие общедоступную компьютерную связь, обычно платную. PDN позволяют небольшим организациям создавать распределенные сети без затрат на прокладку каналов связи на дальние расстояния.

Постоянный виртуальный канал (соединение) (permanent virtual circuit, PVC). Постоянно действующий виртуальный канал. Если виртуальный канал должен существовать постоянно, то использование PVC уменьшают загрузку полосы пропускания, необходимую на установку и разрыв соединения.

Протокол ретрансляции фреймов (Frame Relay). Стандартный промышленный протокол передачи данных с коммутацией каналов, который управляет несколькими виртуальными каналами между подключенными устройствами с помощью HDLC-инкапсуляции. Он более эффективен, чем X.25, и обычно рассматривается как его замена.

Прямое явное уведомление о перегрузке (Forward Explicit Congestion Notification, FECN). Бит, устанавливаемый во фреймах протокола Frame Relay для уведомления DTE-устройств, получающих фреймы, о перегрузке участка сети между источником и получателем. DTE-устройства, получающие фреймы с установленным FECN-битом могут потребовать, чтобы протоколы высшего уровня предприняли соответствующие действия по управлению потоком данных.

Скорость локального доступа (скорость порта) (local access rate). Скорость установки соединения (локального ответвления) со средой протокола ретрансляции фреймов. Она характеризует скорость поступления данных в сеть и получения данных из нее.

Физическая передающая среда (physical media, media). Употребляется как в единственном (medium), так и во множественном числе (media). Типичными сетевыми передающими средами являются: витая пара, коаксиальный или волоконно-оптический кабель, электромагнитные волны (для СВЧ, лазерной и инфракрасной передачи данных).

Приложене A

Ответы на контрольные вопросы

В этом приложении приведены ответы на контрольные вопросы, которые находятся в конце каждой главы

Глава 1

1. C Физический уровень
2. A. Он посылает данные, используя управление потоком
3. B Определение пути и коммутация
4. C Дистанционно-векторная и канальная
5. A Конвергированная
6. Каждый уровень зависит от предоставляемых услуг лежащего ниже уровня Эталонной модели. При осуществлении такой услуги нижний уровень использует инкапсуляцию, размещая PDU верхнего уровня в своем поле данных, после этого он может добавить заголовки или трейлеры, необходимые ему для выполнения своих функций
7. Услуги транспортного уровня обеспечивают надежную доставку данных от хостов к пунктам назначения Для достижения надежной транспортировки используется ориентированная на соединение связь между взаимодействующими системами
8. ICMP используется всеми хостами TCP/IP Сообщения ICMP передаются в IP-дейтаграммах и используются для отправки управляющих сообщений и сообщений об ошибках В качестве примеров ICMP-сообщений можно привести *ping и destination unreachable.*
9. Окна применяются для управления количеством информации передаваемой из одного конца сети в другой Они представляют собой результат договоренности о количестве передаваемой между подтверждениями информации
10. Сетевой уровень обеспечивает негарантированную доставку пакетов из одного конца в другой Сетевой уровень пересылает пакеты от источника к адресату, опираясь на данные таблицы маршрутизации

Глава 2

1. B. Фрейм данных
2. B. 800 наносекунд.
3. D. Первый и второй варианты: выделенные пути между хостами отправителя и получателя и несколько путей передачи данных внутри коммутатора.
4. D. Мосты с несколькими портами, работающие на 2-м уровне.
5. A. Для потока данных сети в случае, когда "быстрый" порт коммутатора подсоединен к серверу.
6. B. Сквозной; с промежуточным хранением.
7. D. Использовать дополнительные пути, без отрицательных эффектов от образования петель.

8. При коммутации с промежуточным хранением происходит прием всего фрейма, прежде чем начнется его передача, в то время, как при сквозной коммутации коммутатор считывает адрес получателя до полного приема фрейма. При этом отправка фрейма начинается до его полного получения.
9. В полудуплексном Ethernet линии передачи (TX) и приема (RX) конкурируют за право использования совместно используемой среды. В полнодуплексном Ethernet TX и RX являются разными линиями и, следовательно, конкуренция за право передачи данных по среде отсутствует.
10. Основной функцией протокола распределенного связующего дерева состоит в том, чтобы сделать возможным использование нескольких коммутируемых путей без появления в сети маршрутных петель.

Глава 3

1. Среди преимуществ виртуальных локальных сетей можно отметить большую безопасность за счет создания безопасных групп пользователей, лучшую управляемость и управление широковещательной активностью, микросегментацию сети и размещение рабочих серверов в более безопасных централизованных помещениях.
2. Широковещание в одной виртуальной локальной сети не выходит за ее пределы. С другой стороны, прилегающие порты не принимают широковещательных сообщений, сгенерированных другими VLAN.
3. VLAN с центральным портом, статические и динамические.
4. При использовании фреймовых тегов в виртуальных локальных сетях некоторый уникальный идентификатор сети помещается в заголовок каждого фрейма при его перемещении по сетевой магистрали.
5. A. Возможность расширения сети без создания коллизионных доменов.
6. D. Все перечисленное.
7. C. Концентратора; коммутатора.
8. D. Автоматическое обновление конфигурации портов при добавлении новых станций.
9. D. Все вышеперечисленные понятия являются характерными признаками виртуальной сети.
10. A. Отсутствует необходимость конфигурирования коммутаторов.

Глава 4

1. Основными четырьмя целями любого сетевого проекта являются функциональность, расширяемость, адаптируемость и управляемость.
2. Задачами сетевых устройств 2-го уровня являются: обеспечение управления потоком, обнаружение ошибок, исправление ошибок и уменьшение числа заторов в сети.
3. Устройства 3-го уровня, такие как маршрутизаторы, позволяют осуществить микросегментацию локальной сети на логическую сеть и физическую сеть. Маршрутизаторы также позволяют выполнить подключение к распределенной сети, такой как Internet.
4. В сетевом проектировании различают два основных типа серверов: промышленные и серверы рабочих групп. Промышленные серверы обслуживают всех пользователей сети, в то время как серверы рабочих групп обслуживают отдельные группы пользователей.
5. Любая документация по сети должна включать в себя карту физической сети, карту логической сети и карту адресации. Их наличие значительно уменьшает время, требуемое для разрешения возникающих в сети проблем.
6. D. Все перечисленное.
7. D. Слишком много сетевых сегментов.
8. C. 2-го уровня; 1-го уровня.

9. Максимальная длина — 400 метров.
10. D. Все перечисленное.

Глава 5

1. Определение пути происходит на сетевом уровне (3-й уровень Эталонной модели OSI).Функция определения пути позволяет маршрутизатору оценить доступные пути к пункту назначения и выбрать из них наиболее предпочтительный для отправки пакета по сети.
2. Маршрутизатор анализирует заголовок пакета для определения сети-получателя и после этого находит соответствующий выходной интерфейс используя данные таблицы маршрутизации.
3. При маршрутизации с использованием нескольких протоколов маршрутизаторы могут одновременно поддерживать несколько независимых протоколов и несколько таблиц маршрутизации. Это позволяет маршрутизатору пересылать пакеты, принадлежащие нескольким маршрутным протоколам, таким, например, как IP и IPX, по одним и тем же каналам передачи данных.
4. Успех динамической маршрутизации зависит от двух основных функций маршрутизатора:
   - поддержка таблицы маршрутизации;
   - своевременное оповещение других маршрутизаторов о топологии сети путем рассылки сообщений об изменениях;
5. В случае, когда все маршрутизаторы обладают одной и той же информацией о топологии сети, сеть называют конвергированной.
6. D. Коммутация пакета.
7. D. B (поддержка таблицы маршрутизации) и C (периодическая рассылка обновлений).
8. A. Дистанционно-векторные; канального уровня.
9. D. Протокол IGRP использует все перечисленные величины.
10. D. router igrp.

Глава 6

1. Списки управления доступом предоставляют еще один эффективный инструмент для управления пакетами данных в сети. Списки управления доступом фильтруют входной и выходной потоки на интерфейсах маршрутизатора.
2. Стандартные списки управления доступом проверяют адрес источника маршрутизируемых пакетов. В результате анализа сети, подсети или адреса хоста пакету разрешается или запрещается отправка.
3. Расширенные списки управления доступом разрешают отправку или запрещают ее на основе более точного анализа свойств пакета. Расширенные списки управления доступом анализируют как адрес источника, так и адрес получателя. Дополнительно могут проверяться конкретные протоколы, номера портов и другие параметры.
4. Директивы списков управления доступом выполняются последовательно сверху вниз. Проверка следующего условия происходит только в том случае, если не выполнено предыдущее.
5. Стандартные списки управления доступом имеют номера от 1 до 99. Расширенные списки управления доступом имеют номера от 100 до 199.
6. C. **`show ip interface.`**
7. A. Биты шаблона.
8. C. "Разрешить доступ только к моей сети."
9. A. Истинно.
10. B. Просмотреть директивы списка управления доступом.

Глава 7

1. MAC-адрес.
2. `ipx maximum paths.`
3. Режим установки глобальной конфигурации.
4. **`show ipx interface.`**
5. **`debug ipx sap.`**
6. C. Номер сети; номер узла.
7. D. Всегда A (серверы Novell) и B (маршрутизаторы Cisco).
8. B. RIP; SAP.
9. `A. ipx routing [узел].`
10. `B. show ipx interface; show ipx route; show ipx servers.`

Глава 8

1. B. Один.
2. C. На физическом уровне.
3. D. DCE.
4. D. Ничто из перечисленного.
5. A. Frame Relay.
6. C. Стационарное оборудование пользователя.
7. D. Все перечисленное.
8. D. Все перечисленное.
9. B. Frame Relay.
10. B. LCP.

Глава 9

1. D. Все перечисленное.
2. A. Во время наибольшей загруженности сети.
3. B. В непосредственной близости от пользователя.
4. C. Простая топология.
5. A. Эффективное использование полосы пропускания.
6. B. Маршрутизаторы.
7. C. Уровень доступа.
8. D. Уровень доступа.
9. A. Сервера.
10. B. Маршрутизатор.

Глава 10

1. SLIP.

2. Асинхронный последовательный, ISDN или синхронный последовательный./
3. D. Все перечисленные.
4. B. Мультипротокольная инкапсуляция.
5. C. Поле протокола.
6. A. Установка, поддержание и прекращение связи типа "точка-точка".
7. C. Три.
8. B. Двустороннее.
9. C. Router# show interfaces.
10. C. Когда рабочей станции требуется доступ в Internet по коммутируемому каналу связи.

Глава 11

1. 128 Кбит/с.
2. Два B-канала.
3. Один D-канал.
4. SPID.
5. D-канал.
6. B. Маршрутизатор.
7. A. Большая концентрация пользователей в сетевом центре.
8. A. Стандарты телефонной сети.
9. C. PPP.
10. D. `Router(config)# isdn switch-type`

Глава 12

1. B. Он мультиплексирует каналы.
2. B. Протоколы верхнего уровня.
3. C. Он рассылает сообщения сразу нескольким получателям.
4. A. Согласованная скорость передачи информации (CIR).
5. D. Провайдер службы.
6. B. В поле адреса.
7. C. Сообщения об активности.
8. D. Он использует таблицу отображения IP-адресов в DLCI.
9. C. Таблица отображения протокола ретрансляции фреймов.
10. B. Для предотвращения маршрутных петель.

Приложение Б

Список команд

Настоящее приложение содержит список команд, которые использовались в книге и призвано служить кратким справочником Для каждой команды приведено краткое описание Кроме того, в таблице содержатся перекрестные ссылки на главу, в которой данная |р команда была впервые использована и описана Это приложение должно помочь в понимании команд используемых для конфигурирования маршрутизаторов Cisco

Команда	Описание	Глава
access-group	Применяет к интерфейсу список управления доступом (ACL)	6
access-list	Определяет стандартный IP-список управления доступом	6
clear interface	Выполняет сброс логических устройств интерфейса	11
debug dialer	Отображает различную информацию, например, номер, который набирает интерфейс	11
debug ipx routing activity	Отображает информацию о пакетах обновления маршрутов протокола RIP	7
debug ipx sap	Отображает информацию о пакетах обновлений протокола служб оповещения (SAP)	7
debug isdn q921	Отображает процедуры доступа к канальному уровню (уровню 2), исполняемые в настоящий момент на D-канале (LAPD) интерфейса ISDN маршрутизатора	11
debug ppp	Отображает информацию о потоках данных и обменах данными в объединенной сети, работающей по протоколу PPP	8
deny	Устанавливает условия в именованном списке управления доступом	6
dialer-group	Управляет доступом путем установки в конфигурации интерфейса принадлежности его к какой-либо конкретной группе набора	11
dialer idle-timeout	Устанавливает время простоя до отключения соединения	11
dialer-list protocol	Определяет список DDR-набора для управления набором по протоколу или комбинацией протокола и списка управления доступом	11
dialer map	Конфигурирование последовательного интерфейса для вызова одного или нескольких сайтов	11
dialer wait-for-carrier-time	Устанавливает время ожидания несущей	11
enable password	Устанавливает пароль для предотвращения несанкционированного доступа к маршрутизатору	12
encapsulation frame-relay	Разрешает инкапсуляцию протокола Frame Relay	12
encapsulation novell-ether	Указывает на то, что в сегменте сети используется только формат фрейма фирмы Novell	7
encapsulation ppp	Устанавливает PPP в качестве метода инкапсуляции на последовательном интерфейсе или интерфейсе ISDN	8, 10, 11

Команда	Описание	Глава
encapsulation sap	Указывает на то, что в сегменте сети используется формат фрейма Ethernet 802.3. Ключевым словом в ОС IOS является sap	7
end	Выход из режима установки конфигурации	12
exec-timeout	Устанавливает интервал, в течение которого командный интерпретатор EXEC ожидает ввода данных пользователем	12
exit	Осуществляет выход из любого режима установки конфигурации или закрывает текущий сеанс и заканчивает работу интерпретатора EXEC	12
frame-relay local-dlci	Включает механизм интерфейса локального управления (Local Management Interface, LMI) для последовательных линий с использованием инкапсуляции типа Frame Relay	12
hostname	Устанавливает в конфигурации маршрутизатора имя хоста, которое будет использоваться по умолчанию или выводиться в качестве приглашения	12
interface	Устанавливает тип интерфейса и переводит маршрутизатор в режим конфигурирования интерфейса	6, 7, 8, 11
interface serial	Осуществляет выбор интерфейса и переводит маршрутизатор в режим конфигурирования интерфейса	12
ip access-group	Управление доступом к интерфейсу	6
ip address	Устанавливает логический сетевой адрес интерфейса	1,6,12
ip unnumbered	Активизирует IP-протокол на последовательном интерфейсе без назначения интерфейсу явного IP-адреса	12
ipx delay	Устанавливает количество тактов	7
ipx ipxwan	Активизирует протокол IPXWAN на последовательном интерфейсе	7
ipx maximum-paths	Устанавливает количество равноценных путей, которое ОС Cisco использует при отправке пакетов	7
ipx network	Включает маршрутизацию протокола обмена пакетами (Internetwork Packet Exchange, IPE) на конкретном интерфейсе и, при необходимости, задает тип инкапсуляции фреймов	7,12
ipx router	Задает используемый протокол маршрутизации	7
ipx routing	Активизирует маршрутизацию IPX	7
ipx sap-interval	Устанавливает меньшую частоту SAP-сообщений об изменениях на медленных линиях	7
ipx type-20-input-checks	Ограничивает прием широковещательных сообщений типа IPX 20	7
isdn spidl	Задает на маршрутизаторе номер профильного идентификатора услуги (service profile identifier number), назначенный провайдером услуги ISDN каналу B1	11
isdn spid2	Задает на маршрутизаторе номер профильного идентификатора услуги (service profile identifier number), назначенный провайдером услуги ISDN каналу B2	11
isdn switch type	Задает тип коммутатора центрального офиса на интерфейсе ISDN	11
keepalive	Активизирует механизм LMI для последовательных линий с использованием инкапсуляции типа Frame Relay	12
line console	Задание конфигурации линии консольного порта	12

Команда	Описание	Глава
line vty	Задает виртуальный терминал для получения доступа к удаленной консоли	12
login	Задает проверку пароля в начале терминального сеанса	12
metric holddown	В течение некоторого времени не разрешает использовать информацию о маршрутизации IGRP	5
network	Назначает NIC-адрес сети, к которой непосредственно подключен маршрутизатор. Активизирует в сети процесс IGRP-маршрутизации. Активизирует в сети расширенный протокол IGRP; при этом на маршрутизаторе должен быть установлен режим конфигурации протокола IPX	1, 5, 7
network-number	Указывает непосредственно подсоединенную сеть	1
permit	Задает условия для именованного списка управления доступом	6
ping	Посылает ICMP-пакеты эхо-запросов на другой узел сети. Проверяет достижимость хоста и возможность установки сетевого соединения. Диагностирует возможность установки связи в сети	1, 7, 11 ,12
ppp authentication	Активизирует протокол аутентификации с предварительным согласованием вызова (Challenge Handshake Authentication Protocol, CHAP), протокол аутентификации паролем (Password Authentication Protocol, PAP) или оба, а также указывает в каком порядке эти два типа аутентификации устанавливаются на интерфейсе	10
ppp chap hostname	Создает группу маршрутизаторов удаленного доступа к сети, которые будут рассматриваться в качестве одного хоста при аутентификации протоколом CHAP	10
ppp chap password	Создает пароль, который будет разослан хостам, которым требуется выполнить проверку подлинности данного маршрутизатора. Эта команда ограничивает количество элементов пользователь/пароль на маршрутизаторе	10
ppp pap sent-username	Задает поддержку на интерфейсе удаленного PAP и использует команды sent-username И password В запросе на аутентификацию, направляемом соответствующему устройству	10
protocol	Задает протокол IP-маршрутизации, в качестве которого могут выступать RIP, IGRP, OSPF или EIGRP	1
router igrp	Активизирует процесс маршрутизации IGRP	5
router rip	Выбирает RIP в качестве протокола маршрутизации	1
show access-list	Отображает содержимое всех текущих списков управления доступом	6
show dialer	Отображает общую диагностическую информацию для последовательных интерфейсов сконфигурированных для DDR	11
show frame-relay Lmi	Отображает LMI-статистику	12
show frame-relay map	Отображает текущие элементы таблицы отображения и информацию об установленных соединениях	12
show frame-relay pvc	Отображает статистику PVC для интерфейсов типа Frame Relay	12
show interfaces	Отображает статистику для всех интерфейсов, сконфигурированных на маршрутизаторе или сервере доступа	8, 10,11
show interfaces serial	Отображает информацию о последовательном интерфейсе	12
show ip interface	Выводит информацию об IP-интерфейсе и о его состоянии	6

Команда	Описание	Глава
`show ip route`	Выводит текущее состояние таблицы маршрутизации	11
`show ipx interface`	Отображает состояние IPX-интерфейсов, сконфигурированных в ОС Cisco и параметры каждого интерфейса	7
`show ipx route`	Отображает содержимое таблицы IPX-маршрутизации	7
`show ipx servers`	Отображает список IPX-серверов	7
`show ipx traffic`	Отображает число и тип пакетов	7
`show isdn active`	Отображает информацию текущего вызова, включая вызываемый номер, время, оставшееся до отключения, количество денежных единиц, использованных за время вызова, а также предоставляется ли такая информация во время вызова или после его окончания	11
`show isdn status`	Отображает состояние всех ISDN интерфейсов. При необходимости можно указать конкретный цифровой сигнальный канал (digital signal link, DSL) или конкретный ISDN-интерфейс	11
`show protocols`	Отображает типы сконфигурированных `протоколов`	7
`show spantree`	Отображает информацию протокола распределенного связующего дерева для виртуальной локальной сети (VLAN)	2
`show status`	Отображает текущее состояние ISDN-линии и обоих B-каналов	11
`term ip netmask-format`	Задает формат, в котором отображается маска сети при выводе по команде show	1
`timers basic`	Задает частоту рассылки протоколом IGRP сообщений об изменениях в сети	5
`username password`	Задает пароль, который будет использоваться при аутентификации CHAP и PAP.	10

Словарь терминов

В предлагаемом глоссарии определены многие термины и аббревиатуры, связанные с работой в сетях. Глоссарий включает в себя все ключевые термины, использованные в настоящей книге, а также многие другие термины, используемые при описании сетевых технологий. Как и в любой другой развивающейся области, некоторые термины постепенно меняют свой смысл и приобретают новые значения. В предлагаемом глоссарии для некоторых терминов приводятся несколько определений и аббревиатур. Термины, состоящие из нескольких слов, упорядочены так, как если бы между отдельными словами не было пробелов, а слова в кавычках так, как если бы кавычки отсутствовали.

Как правило, описание терминов дается при их аббревиатурах. При этом для каждой аббревиатуры отдельно дается ее полное словосочетание с перекрестной ссылкой на саму аббревиатуру. Кроме того, для многих определений даются перекрестные ссылки на сопутствующие термины.

Авторы надеются, что этот глоссарий облегчит читателю понимание вопросов, связанных с сетевыми технологиями.

Числовые аббревиатуры

2B+D. В контексте службы BRI ISDN — два B-канала и один D-канал.

4B/5B local fiber. 4/5-байтовый локальный волоконно-оптический кабель, используемый для FDDI и ATM. Многорежимная модификация обеспечивает передачу данных со скоростью до 100 Мбит/с.

4-byte/5 byte local fiber См. *4B/5B local fiber.*

8B/10B local fiber. 8/10-байтовый локальный волоконно-оптический кабель. Многорежимная модификация обеспечивает передачу данных со скоростью до 149,76 Мбит/с.

8-byte/10-byte local fiber. См. *8B/10B local fiber.*

lOBasel. Разновидность спецификации Ethernet для передачи данных со скоростью 10 Мбит/с по тонкому коаксиальному кабелю с сопротивлением 50 Ом. 10Base2 является частью спецификации IEEE 802 3. Максимальная длина сегмента 10Base2 ограничена расстоянием 185 метров. См. также *Ethernet* и *IEEE 802.3.*

lOBaseS. Разновидность спецификации Ethernet для передачи данных со скоростью 10 Мбит/с по стандартному (толстому) коаксиальному кабелю с сопротивлением 50 Ом. 10Base5 является частью спецификации IEEE 802.3. Максимальная длина сегмента 10Base5 ограничена расстоянием 500 метров. См. также *Ethernet* и *IEEE 802.3.*

lOBaseF. Спецификация Ethernet для передачи данных со скоростью 10 Мбит/с **по** волоконно-оптическому кабелю, относящаяся к Ethernet-стандартам **lOBaseFB, lOBaseFL** и lOBaseFP. См. также *lOBaseFB, lOBaseFL, lOBaseFP* и *Ethernet.*

lOBaseFB. Спецификация Ethernet для передачи данных со скоростью 10 Мбит/с по волоконно-оптическому кабелю. Представляет собой часть спецификации IEEE *lOBaseF.* Эта спецификация не используется для непосредственной связи между рабочими станциями, а обеспечивает

синхронную сигнальную магистраль, позволяющую подсоединять к сети новые сегменты и повторители.

lOBaseFL. Разновидность спецификации Ethernet для передачи данных со скоростью 10 Мбит/с по волоконно-оптическому кабелю. Является частью спецификации IEEE lOBaseF, совместима со спецификацией FO1RL, однако, как правило, используется для последующей замены последней. Сегменты lOBaseFL могут достигать длины 1000 метров при использовании вместе с FOIRL и 2000 метров без нее. См. также *lOBaseF* и *Ethernet.*

lOBaseFP. Разновидность спецификации Ethernet для передачи данных со скоростью 10 Мбит/с по пассивному волоконно-оптическому кабелю. Является частью спецификации IEEE lOBaseF и используется для создания топологии типа "звезда" без использования повторителей. Сегменты lOBaseFP могут достигать длины 500 метров. См. также *lOBaseF и Ethernet.*

lOBaseT. Разновидность спецификации Ethernet для передачи данных со скоростью 10 Мбит/с по двойной витой паре (категории 3, 4 или 5). Одна пара используется для передачи данных, а другая для их получения. Является частью спецификации IEEE 802.3. Применение lOBaseT ограничено расстоянием 100 метров на один сегмент. См. также *Ethernet* и *IEEE 802.3.*

10Broad36. Разновидность спецификации Ethernet для широкополосной передачи данных со скоростью 10 Мбит/с по широкополосному коаксиальному кабелю. Является частью спецификации IEEE 802.3. Применение 10Broad36 ограничено расстоянием 3600 метров на один сегмент. См. также *Ethernet* и *IEEE 802.3.*

100BaseFX. 100-Мбит/с стандарт Fast Ethernet, использующий два многожильных, многомодовых оптоволоконных кабеля на каждое соединение. Чтобы гарантировать соответствующую синхронизацию сигнала, lOOBaseFX-соединение не должно превышать 400 метров в длину. Базируется на стандарте IEEE 802.3. См. также *lOOBaseX, Ethernet* и *IEEE 802.3.*

100BaseT. Разновидность спецификации Fast Ethernet для передачи данных со скоростью 100 Мбит/с на основе UTP. Основана на технологии lOBaseT и аналогична ей, в спецификации 100BaseT предусмотрена передача импульсов связывания в сетевом сегменте, в котором отсутствует сетевой поток данных. Однако, эти импульсы содержат более подробную информацию, чем в технологии lOBaseT. Основана на стандарте IEEE 802.3. См. также *lOBaseT, Fast Ethernet* и *IEEE 802.3.*

100BaseT4. Разновидность спецификации Fast Ethernet для передачи данных со скоростью 100 Мбит/с на основе четырех пар UTP-кабеля категории 3, 4 или 5. Необходимость синхронизации ограничивает применение 100BaseT4 сегментом не более 100 метров. Основан на стандарте IEEE 802.3. См. также *Fast Ethernet* и *IEEE 802.3.*

100BaseTX. Стандарт Fast Ethernet для передачи данных со скоростью 100-Мбит/с, использующий две пары UTP или STP. Первая пара используется для получения данных, вторая — для передачи. Для обеспечения соответствующей синхронизации длина сегмента не должна превышать 100 метров. Основан на стандарте IEEE 802.3.

lOOBaseX. Разновидность спецификации Fast Ethernet для передачи данных со скоростью 100 Мбит/с по волоконно-оптическому кабелю, относящаяся к 100BaseFX и 100BaseTX. Основана на стандарте IEEE 802.3. См. также *100BaseFX, 100BaseTX, Fast Ethernet* и *IEEE 8G2.3.*

lOOVG-AnyLAN. Разновидность спецификаций Fast Ethernet и Token Ring для передачи данных со скоростью 100 Мбит/с на основе четырех пар UTP-кабеля категории 3, 4 или 5. Эта высокоскоростная технология фирмы Hewlett-Packard может функционировать в уже существующих сетях lOBaseT Ethernet. Основана на стандарте IEEE 802.12. См. также *IEEE 802.12.*

A

A&B bit signaling. Процедура, используемая в устройствах передачи данных T1, где для каждого из 24 подканалов T1 выделяется по 1 биту каждого шестого кадра для передачи координирующей сигнальной информации.

ABM. 1. Asynchronous Balanced Mode, Асинхронный сбалансированный режим. Режим обмена данными по протоколу HDLC (и его производным протоколам), равноправный или "точка-точка", где инициатором передачи данных может быть любая из станций. 2. Accunet Bandwidth Manager.

Access method. 1. Метод доступа. Любой способ обращения устройств к сети. 2. Программное обеспечение SNA-процессора, которое управляет потоком информации в сети.

АСК. См. *подтверждение (acknowledgment)*

Adapter. *См. сетевая плата (NIC).*

Address Resolution Protocol. См. *преобразование адресов.*

Advanced Research Projects Agency. См. *агентство перспективного планирования научно-исследовательских работ*

AppleTalk. Набор коммуникационных протоколов Apple Computer, который состоит из двух фаз. Более ранняя версия, Phase 1, поддерживает простую физическую сеть, которая может иметь только один сетевой номер и находиться в одной зоне. Phase 2 поддерживает несколько логических сетей в одной физической сети и позволяет сетям находится в нескольких зонах. См. также *зона (zone).*

ARPA (Advanced Research Projects Agency). Агентство перспективного планирования научно-исследовательских работ. Научно-исследовательская организация при Министерстве обороны США. Именно ей мы обязаны значительными технологическими достижениями в области телекоммуникаций и сетевых технологий. Позднее она стала называться DARPA, а с 1994 г. — снова ARPA.

ARPANET (Advanced Research Projects Agency Network). Знаменитая сеть на основе коммутации пакетов, созданная в 1969 г. В 70-х гг. XX века развитием ARPANET занималась BBN, а финансированием — ARPA (позднее DARPA). ARPANET стала прообразом сети Internet. Официально термин ARPANET был отменен в 1990 г.

Asynchronous Balanced Mode. См. *ABM*.

Asynchronous Transfer Mode. См. *режим асинхронной передачи.*

B

Banyan VINES. См. *виртуальная интегрированная сетевая служба.*

Basic Rate Interface. См. *BRI*

Bootstrap Protocol. См. *протокол начальной загрузки.*

B-канал, канал носителя (bearer channel, B channel). Дуплексный, канал ISDN-типа ра-

ботающий со скоростью 64 Кбит/с, используемый для передачи данных пользователя.

C

Challenge Handshake Authentication Protocol. См. *CHAP*.

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

Concentrator. См. *концентратор.*

Connectionless. Передача данных без установки соединения. Режим передачи данных при отсутствии виртуального канала. Ср. с *connection-oriented.* См. также *виртуальный канал.*

Connection-oriented. Обмен данными, ориентированный на соединение и требующий установления виртуального канала. См. также *connectionless* и *виртуальный канал.*

D

D channel, delta channel. Дуплексный ISDN-канал со скоростью передачи 16 Кбит/с (BRI) или 64 Кбит/с (PRI). См. также *B-канал.*

DAS (dual attachment station). 1. Станция с двойным подключением. Устройство, подключаемое к первичному и вторичному кольцам FDDI. Двойное подключение обеспечивает избыточность для кольца FDDI: в случае сбоя первичного кольца станция может перейти к работе на вторичном кольце, изолируя этот сбой и обеспечивая целостность кольца. Станции DAS также называют станциями класса A. Ср. с *SAS. 2.* **Dynamically Assigned Socket,** или динамически назначаемый сокет. Сокет, назначаемый при DDP-обработке динамически, по запросу клиента. В сетях AppleTalk такие сокеты, пронумерованные от 128 до 254, выделяются динамически.

DECNet. Группа коммуникационных продуктов (в том числе набор протоколов), созданная и поддерживаемая корпорацией Digital Equipment Corporation. Ее последней версией является DECNet/OSI (или DECNet Phase V). DECNet/OSI поддерживает протоколы OSI и собственные протоколы Digital Equipment Corporation. Phase IV Prime поддерживает MAC-адреса, которые позволяют узлам DECNet сосуществовать с системами на основе других протоколов, которые имеют некоторые ограничения на MAC-адреса. См. также *DNA.*

Destination service access point. См. *точка доступа к службе получателя.* **Dial-on-demand routing. См.** *маршрутизация с коммутацией по запросу.* **Dual attachment station. См.** *DAS.*

D-канал, дополнительный канал, дельта-канал, канал управления скоростью передачи (delta channel, D channel). Дуплексный ISDN-канал с пропускной способностью 16 Кбит/с (для BRI) или 64-Кбит/с (для PRI).

E

E1. Цифровая сеть передачи данных с полосой 2,048 Мбит/с. Используется в Европе. Каналы E1 могут арендоваться для закрытого использования. Ср. с 77.

E3. Цифровая сеть передачи данных с полосой пропускания 34,368 Мбит/с. Используется в Европе. Каналы E3 могут арендоваться для закрытого использования.

EEPROM (electrically erasable programmable read-only memory, электрически стираемое программируемое ПЗУ). Микросхема постоянного запоминающего устройства, которую можно перепрограммировать с помощью электрических сигналов, приложенных к определенным выводам.

EIA/TIA-568. Стандарт, описывающий характеристики и приложения для различных категорий UTP кабеля.

ES-IS (End System-to-Intermediate System). Протокол OSI, определяющий способ, каким оконечная система (хост) объявляет о себе промежуточной системе (маршрутизатору).

Ethernet. Спецификация локальных сетей, изобретенная корпорацией Xerox и разработанная совместно Xerox, Intel и Digital Equipment Corporation. Сети Ethernet используют CS MA/CD и работают на различных типах кабелей со скоростью 10 Мбит/с. Стандарт Ethernet подобен серии стандартов IEEE 802.3.

F

FDDI II. Усовершенствованная версия ANSI-стандарта FDDI-интерфейса. FDDI II обеспечивает изохронную передачу данных для соединений, не требующих предварительной установки связи с получателем, а также речевых и видеоданных, ориентированных на установку соединения с конечным получателем. Ср. с *распределенный интерфейс передачи данных по волоконно-оптическим каналам (FDDI).*

Fiber Distributed Data Interface. см. FDDI

File Transfer Protocol. См. *протокол передачи файлов.*

G

Gbps. Гбит/с, гигабитов в секунду.

Get Nearest Server. См. *запрос ближайшего сервера.*

H

Horizontal cross-connect. См. *горизонтальное кросс-соединение,* Hypertext Markup Language. См. *язык гипертекстовой разметки.* Hypertext Transfer Protocol. См. *протокол передачи гипертекста.*

IEEE 802.2. Стандарт IEEE протокола локальной сети, который описывает реализацию LLC-подуровня канального уровня. IEEE 802.2 обрабатывает ошибки, управляет фреймами и потоками, а также интерфейсом сетевого уровня (уровень 3). Используется в локальных сетях IEEE

802.3 и **IEEE 802.5**, См. также *IEEE 802.3* и *IEEE 802.5.*

IEEE 802.3. Стандарт IEEE протокола локальной сети, который описывает физический уровень и MAC-подуровень канального уровня. В нем используется доступ CSMA/CD на разных скоростях и для разных физических носителей. Существуют расширения этого стандарта для Fast Ethernet. Среди физических разновидностей IEEE 802.3 следует отметить 10Base2, lOBaseS, lOBaseF, lOBaseT и 10Broad36. Для Fast Ethernet существуют такие варианты, как 100BaseT, 100BaseT4 и lOOBaseX.

IEEE 802.5. Стандарт IEEE протокола локальной сети, определяющий физический уровень и MAC-подуровень канального уровня. IEEE 802.5 использует доступ с передачей маркеров со скоростями от 4 до 16 Мбит/с по кабелям STP и UTP; функционально и в операционном отношении эквивалентен Token Ring. См. также *Token Ring.*

Institute of Electrical and Electronic Engineers. См. *Институт инженеров по электротехнике и электронике.*

Integrated Services Digital Network. См. *цифровая сеть интегрированных служб.* Intermediate distribution facility. См. *промежуточная распределительная станция.*

International Organization for Standardization. См. *международная организация по стандартизации.*

Internet Protocol. См. *протокол IP.*

Internetwork Packet Exchange. См. *протокол межсетевого обмена пакетами.*

Internet Control Message Protocol. См. *протокол межсетевых управляющих сообщений.*

Internet. 1. Крупнейшая глобальная межсетевая структура, соединяющая десятки тысяч сетей во всем мире. Обладает "культурой", где основное внимание уделяется исследованиям и стандартизации на основе практических требований. В сообществе Internet созданы многие передовые сетевые технологии. Отчасти Internet появилась в результате эволюции ARPANET и прежде называлась DARPA Internet. Этот термин не следует путать с более общим термином *internet.* См. также *ARPANET. 2.* Сокращение от internetwork — "объединенная сеть". Этот термин не следует путать с названием глобальной сети Internet. См. *объединенная сеть.*

internet. Сокращение для "объединенной сети".

Intranet. Внутренняя сеть организации, к которой имеют доступ пользователи.

IOS (Internetwork Operating System). См. *Cisco IOS.*

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

IP-дейтаграмма (IP-datagram). Блок информации, передаваемый по объединенной сети; наряду с данными содержит адреса отправителя и получателя, а также поля, определяющие длину дейтаграммы, контрольную сумму заголовка и флаги, говорящие о возможности (или невозможности) фрагментации дейтаграммы.

L

Link Access Procedure on the D channel. См. *протокол доступа к d-каналу*.

Link Control Protocol. См. *протокол управления каналом*.

Local Management Interface. См. *интерфейс локального управления.*

Local-area network. См. *локальная сеть.*

Logical link control. См. *протокол логического канала*.

M

MAC-layer address. См. *MAC-address.*

MAC-адрес (адрес управления доступом к передающей среде) (Media Access Control Address, MAC address). Стандартизованный адрес данных канального уровня, который требуется любому порту или устройству, подсоединенному к локальной сети. Другие устройства сети используют эти адреса для нахождения конкретных портов в сети, создания и обновления таблиц маршрутизации и структур данных. MAC-адреса имеют длину 6 байтов и контролируются IEEE. Их также называют адресами устройств, адресами MAC-уровня или физическими адресами.

Management Information Base. См. *база управляющей информации*.

Media Access Control. См. *управление доступом к передающей среде.*

Media access unit. См. *устройство подсоединения к передающей среде.*

Media attachment unit. См. См. *устройство подсоединения к передающей среде.*

Multistation access unit. См. *модуль множественного доступа.*

N

NetWare Link Services Protocol. См. *протокол служб канального уровня NetWare.*

NetWare Loadable Module. См. *загружаемый модуль NetWare.*

Network address translation. См. *трансляция сетевых адресов.*

Network Basic Input/Output System. См. *сетевая базовая система ввода-вывода*.

Network Control Program. См. *программа управления сетью.*

Network File System. См. *сетевая файловая система.*

Network interface card. См. *сетевая плата*.

Network management system. См. *система управления сетью*.

Network operating system. См. *сетевая операционная система.*

Networking. Процесс взаимодействия между собой рабочих станций и периферийных устройств, таких как принтеры, жесткие диски, сканеры, дисководы компакт-дисков и т.д.

Novell IPX. См. *протокол межсетевого обмена пакетами.*

O-P

Open Shortest Path First. См. *протокол выбора первого кратчайшего пути.*

Packet internet groper. См. *проверка доступности адресата.*

Password Authentication Protocol. См. *протокол аутентификации паролем.*

Permanent virtual circuit. См. *постоянный виртуальный канал.*

Physical address. См. *MAC-address.*

PHY. 1. ***Physical sublayer,*** физический подуровень. Один из двух подуровней физического уровня **FDDI.** ***2. Physical layer,*** физический уровень. В ATM физический уровень обеспечивает передачу ячеек по физической среде, которая связывает два устройства ATM. PHY содержит два подуровня: *PMD* и *TC*.

Point-to-Point Protocol. См. *протокол "точка-точка".* Protocol address. См. *сетевой адрес.* Protocol analyzer. См. *сетевой анализатор.* Proxy Address Resolution Protocol. См. *агент ARP.*

Q-R

Q.931. Протокол, который описывает сетевой уровень между оконечной точкой и локальным ISDN-коммутатором. Не накладывает ограничений на непосредственные соединения оконечных точек. Разные ISDN-провайдеры могут использовать различные реализации этого протокола.

Random-access memory. См. *оперативное запоминающее устройство.*

Request for Comment. См. *запрос на комментарий.*

Routing Table Maintenance Protocol. См. *протокол обслуживания таблиц маршрутизации.*

S

Sequenced Packet Exchange. См. *протокол последовательного обмена пакетами.*

Serial Line Internet Protocol (протокол Internet для последовательного канала, SLIP).Стандартный протокол последовательных соединений типа "точка-точка" с использованием различных вариантов протоколов TCP/IP. Предшественник PPP.

Service Advertising Protocol. См. *протокол объявления служб.*

Small office/home office. См. *малый офис/домашний офис.*

Subnet. См. *подсеть*.

Synchronous Data Link Control. См. *управление синхронным каналом данных*.

T

T1. Цифровой канал передачи данных по глобальной сети. T1 передает данные формата DS-1 со скоростью 1,544 Мбит/с по коммутируемой телефонной сети, используя кодировку AMI или B8ZS.

T3. Цифровой канал передачи данных по глобальной сети. T3 передает данные формата DS-3 со скоростью 44,736 Мбит/с по коммутируемой телефонной сети.

Telnet. Стандартный протокол виртуального терминала из набора TCP/IP. Протокол Telnet используется для удаленного терминального соединения, что дает возможность пользователям подключаться к удаленным системам и использовать их ресурсы, как если бы они работали через обычный терминал. Telnet описан в RFC 854.

Time To Live. См. *время жизни*.

Token Ring. Локальная сеть с передачей маркера, разработанная и поддерживаемая компанией IBM. Сеть Token Ring имеет кольцевую топологию и работает со скоростью 4 или 16 Мбит/с. Подобна IEEE 802.5.

Token Talk. Продукт канального уровня, разработанный Apple Computers и позволяющий соединять сеть AppleTalk кабелями Token Ring.

Traceroute). Программа, установленная на многих системах, которая отслеживает путь пакета к месту назначения. Обычно используется для устранения проблем с маршрутизацией между хостами. Существует также протокол трассировки, определенный в RFC 1393.

V

Vertical cross-connect. См. *вертикальное кросс-соединение*.

A

Автономная система (autonomous system, AS). Набор сетей, работающих под одним административным управлением и использующих общую стратегию маршрутизации. Также называется *доменом маршрутизации.* Департамент назначения номеров Internet (Internet Assigned Numbers Authority) присваивает автономным системам 16-битный номер.

Агент (agent). 1. Обычно программное обеспечение, обрабатывающее очереди и возвращающее ответ с ведома приложения. 2. В NMS — процесс, расположенный на всех управляемых устройствах и сообщающий станциям управления о значениях заданных переменных.

Агент ARP, агент протокола преобразования адресов (proxy Address Resolution Protocol, proxy ARP). Вариант протокола ARP, в котором промежуточное устройство (например, мар-

шрутизатор) посылает ответ ARP от имени конечного узла запрашивающему хосту. На низкоскоростных каналах связи использование агентов ARP может существенно уменьшить полосу пропускания. См. также протокол *преобразование адресов.*

Агентство по выделению имен и уникальных параметров протоколов Internet (Internet Assigned **Numbers Authority, IANA).** Организация, уполномоченная ISOC, являющаяся частью IAB. IANA делегирует полномочия для выделения IP-адресного пространства и присвоения доменных имен InterNIC и другим организациям. IANA также поддерживает базу данных присвоенных идентификаторов протоколов, используемых в стеке TCP/IP, включая номера автономных систем.

Адрес (address). Структура данных или логическое соглашение для идентификации уникального объекта, например, процесса или сетевого устройства.

Адрес отправителя (source address). Адрес сетевого устройства, посылающего данные. См. также *адрес получателя.*

Адрес подсети (subnet address). Часть IP-адреса, обозначенная как подсеть маской подсети.

Адрес получателя (destination address). Адрес сетевого устройства, получающего данные. См. также *адрес отправителя.*

Адрес представления в модели OSI (OSI presentation address). Адрес, который используется для локализации объекта уровня приложений в модели OSI. Состоит из сетевого адреса OSI и не более трех селекторов, каждый из которых используется объектами транспортного, сеансового уровня и уровня представлений.

Адрес следующего перехода (next-hop address). IP-адрес, вычисляемый протоколом маршрутизации IP и программным обеспечением.

Адрес хоста (host address). См. *номер хоста.*

Адресная маска (address mask). Комбинация битов для описания той части адреса, которая относится к сети, подсети или к узлу. Иногда называется просто маской. См. также *маска подсети.*

Активный монитор (active monitor). Управляет сетью **Token** Ring. Для этой роли выбирается сетевой узел с самым большим MAC-адресом в данной сети. Активный монитор следит за тем, чтобы не терялись маркеры, и кадры не циркулировали бы бесконечно.

Алгоритм построения распределенного связующего дерева (spanning-tree algorithm). Алгоритм, используемый протоколом распределенного связующего дерева для построения связующего дерева. Иногда используется аббревиатура STA. См. также *распределенное связующее дерево.*

Американский стандартный код обмена информацией (American Standard Code for Information Interchange, ASCII). Восьмиразрядный код для представления символов (7 бит плюс один контрольный бит).

Анонсирование (advertising). Процесс, выполняемый на маршрутизаторе, при котором обновленная маршрутная и служебная информация передаются через заданные интервалы времени таким образом, чтобы другие маршрутизаторы сети могли обновить списки используемых маршрутов.

Аппаратный (физический) адрес (hardware address). См. *MAC-адрес.*

Асимметричная коммутация (asymmetric switching). Тип коммутации, обеспечивающий коммутируемые соединения портов с разной шириной полосы пропускания. Например, порты на 10 Мбит/с и 100 Мбит/с.

Асинхронный канал (asynchronous circuit). Сигнал, передаваемый без точной синхронизации. Такие сигналы обычно имеют разные несущие частоты и фазы. При асинхронной передаче отдельные символы обычно инкапсулируются в управляющие биты (называемые битами начала и остановки), указывающими на начало и конец каждого символа. См. также *синхронный канал*.

Ассоциация телекоммуникационной индустрии (Telecommunications Industries Association, TIA). Организация, разрабатывающая стандарты для телекоммуникационных технологий. TIA и EIA совместно формализовали стандарты, такие как EIA/TIA-232, определяющие электрические характеристики процесса передачи данных.

Ассоциация электронной индустрии (Electronic Industries Association, EIA). Группа, устанавливающая стандарты передачи данных. EIA и TIA совместно разработали большое количество стандартов коммуникации, включая стандарты EIA/TIA-232 и EIA/TIA-449.

Аутентификация (authentication). В контексте обеспечения безопасности — проверка идентичности пользователя или процесса.

Б

База управляющей информации (Management Information Base, MIB). База данных, где хранится информация для управления сетью, которая используется и поддерживается такими протоколами сетевого управления, как SNMP и CMIP. Значение M1B-объекта может быть изменено или извлечено с помощью команд SNMP или CMIP и (обычно) сетевой системы управления с GUI-интерфейсом. MIB-объекты образуют древовидную структуру с открытыми (стандартными) и закрытыми (частными) ветвями.

Байт (byte). Ряд последовательных двоичных чисел, составляющих единое целое (например, 8 бит = 1 байт).

Без буферизации пакетов (cut-through). Коммутация пакетов, при которой данные просолят через коммутатор следующим образом: начало пакета появляется на исходящем торту до того, как пакет закончит прохождение входящего порта. Устройство, исполь-syioLuee этот вид коммутации, читает, обрабатывает и отправляет пакеты сразу, как только узнает адрес и порт пункта назначения. Коммутация без буферизации пакетов известна также под названием *непрерывная коммутация (on-the-fly packet switching)* или *коммутация на лету*.

Бесклассовая междоменная маршрутизация (classless interdomain routing, CIDR). Технопогия, поддерживаемая BGP4 и основанная на агрегации маршрута. Позволяет маршрутизаторам группировать маршруты для сокращения объема маршрутной информации, передаваемой основными маршрутизаторами. С ее помощью несколько IP-сетей выглядят для внешних сетей как одна сеть. Благодаря этому IP-адреса и их маски подсети записываются в виде 4 байтов, разделенных точками, за которыми следует косая черта и 2-х значное число — маска подсети.

Бесконечное возрастание счетчика (count to infinity). Проблема, возникающая в алго-эитмах маршрутизации со слабой сходимостью. Заключается в том, что маршрутизаторы постоянно увеличивают счетчик узлов для отдельных сетей. Обычно во избежание этой проблемы вводится некоторое предельное значение счетчика.

Бит (bit). Число в двоичной системе счисления. Равно нулю или единице.

Битовая корзина (bit bucket). Место, в которое направляются отвергнутые маршрутизатором пакеты.

Ближайший соседний активный узел против направления основного трафика (nearest active upstream neighbor, NAUN). В сетях Token Ring или IEEE 802.5 — ближайшее активное соседнее устройство, расположенное в направлении, противоположном основному трафику.

Блок канального интерфейса/блок цифровой службы (channel service unit/digital service unit, CSU/DSU). Устройство цифровой связи, соединяющее оборудование конечного пользователя и ответвление локальной телефонной станции.

Брандмауэр (firewall). Один или несколько маршрутизаторов или серверов доступа, выполняющих роль буфера между частной и общей сетью. Использует список контроля доступа (ACL) и другие методы для обеспечения безопасности частной сети.

Буфер памяти (memory buffer). Область памяти, в которой коммутатор хранит передаваемые данные и их адреса.

Быстрый Ethernet (Fast Ethernet). Спецификации Ethernet для скоростей передачи данных до 100 Мбит/с. В Fast Ethernet скорость передачи данных увеличена в 10 раз, по сравнению с lOBaseT; при этом сохранены такие характеристики, как формат фрейма, механизмы MAC и MTU. Подобное сходство позволяет использовать существующие lOBaseT приложения и сетевые управляющие механизмы в сетях на основе Fast Ethernet. Базируется на расширении спецификации IEEE 802.3.

Быстрый транспортный протокол (Rapid Transport Protocol, RTF). Обеспечивает пошаговою обработку и исправление ошибок для данных APPN, когда они проходят по сети APPN. Благодаря RTP исправление и контроль ошибок выполняются на всем маршруте, а не на каждом узле. RTP предотвращает перегрузку, а не является средством ее устранения.

В

Вертикальное кросс-соединение (vertical cross-connect, VCC). Соединение, которое используется для подключения разных ПРС к центральной ГРС.

Взаимодействие открытых систем (Open System Interconnection, OSI). Международная программа стандартизации, созданная ISO и ITU-T для разработки стандартов межсетевого обмена данными, способствующих функциональной совместимости оборудования различных производителей.

Виртуальная интегрированная сетевая служба (Virtual Integrated Network Service, VINES). Сетевая операционная система, разработанная и выпущенная на рынок компанией Banyan Systems.

Виртуальная локальная сеть (virtual LAN, VLAN). Группа устройств в локальной сети, которые сконфигурированы (с использованием управляющего программного обеспечения) таким образом, что они могут обмениваться информацией, как если бы они были соединены одним кабелем. В действительности они располагаются в разных сегментах локальной сети. Поскольку виртуальные сети основываются на логическом, а не физическом соединении, они являются чрезвычайно гибкими.

Виртуальная сеть с центральным портом (port-centric VLAN). Виртуальная сеть, все узлы которой присоединены к одному порту коммутатора.

Виртуальный канал или виртуальная цепь (virtual circuit). Логический канал, создаваемый для обеспечения надежной связи между двумя сетевыми устройствами. Виртуальный канал определяется парой VPI/VCI и может быть постоянным (PVC) или коммутируемым (SVC). В виртуальных каналах используются протоколы ретрансляции фреймов и X.25. Иногда используется аббревиатура VC.

Внешний протокол (exterior protocol). Протокол, используемый для обмена маршрутной информацией между сетями, находящимся под различным административным управлением.

Внутренний протокол (interior protocol). Протокол, используемый в сетях, находящихся под единым административным управлением.

Волоконно-оптический кабель (fiber-optic cable). Физическая среда, способная передавать модулированные световые сигналы. Волоконно-оптический кабель дороже, по сравнению с другими видами передающих сред, однако он не восприимчив к электромагнитным помехам и способен передавать данные с более высокой скоростью. Иногда его называют оптоволоконный кабель или просто *оптоволокно (optical fiber).*

Временное мультиплексирование (time-division multiplexing, TDM). Сигнал коммутации канала, используемый для определения маршрута вызова, который является выделенным путем от отправителя к получателю.

Время жизни (Time To Live, TTL). Поле в заголовке IP-дейтаграммы, указывающее время, в течение которого пакет считается действительным.

Время распространения (propagation delay). Время, которое требуется данным, чтобы пройти сеть от источника до конечного адресата. Также называется *задержкой (latency).*

Время установки вызова (call setup time). Время, необходимое для установки коммутируемого

вызова между DTE-устройствами.

Встроенные программно-аппаратные средства (firmware). Программы, встроенные в ПЗУ, которые управляют каким-либо устройством.

Вторичная станция (secondary station). В протоколах канального уровня с битовой синхронизацией, таких как HDLC, — станция, отвечающая на команды первичной станции.

Выделенная линия (Leased line). Линия передачи, зарезервированная поставщиком коммуникационных услуг для частного использования заказчиком. Является подтипом выделенного канала.

Выделенный канал (dedicated link). Коммуникационный канал, неопределенно зарезервированный для передачи данных. Такой канал качественно отличается от канала, коммутируемого при появлении необходимости в передаче данных.

Выделенный маршрутизатор (designated router). OSPF-маршрутизатор, который генерирует LSA-пакеты для сети с множественным доступом и другими специальными обязанностями при использовании алгоритма OSPF. Каждая OSPF-сеть с множественным доступом, где есть по крайней мере два присоединенных маршрутизатора, имеет выделенный маршрутизатор, выбранный протоколом приветствия OSPF. Выделенный маршрутизатор позволяет сократить количество смежных элементов в сети с множественным доступом, что, в свою очередь, сокращает объем маршрутизируемого трафика и размер топологической базы данных.

Высокоскоростной канал (high-speed channel, H channel). Дуплексный первичный канал ISDN со скоростью передачи 384 Кбит/с. Ср. с *B-канал*.

Высокоуровневый протокол управления каналом (High-level Data Link Control, HDLC).

Бит-ориентированный синхронный протокол канального уровня ISO. Основан на протоколе SDLC и определяет метод инкапсуляции данных в синхронных последовательных каналах с помощью символов кадрирования и контрольных сумм. См. также *синхронное управление каналом данных*.

Г

Гарантированная скорость передачи (insured rate). Долговременная скорость передачи данных (в битах или ячейках в секунду), обеспечиваемая сетью ATM в нормальных условиях. Ее суммарное значение выводится на основе суммарной полосы пропускания канала. Ср. с *максимальная скорость передачи*.

ГБит, гигабит (Gb). Равен 1024 Мбит, или 1 073 741 824 бит.

Гибридная сеть (hybrid network). Комбинация разных сетей, включая LAN и WAN.

Главная распределительная станция ГРС (main distribution facility, MDF). Первичный коммуникационный зал здания. Центральная точка звездообразной сетевой топологии, где расположены коммуникационные панели, концентраторы и маршрутизаторы.

Горизонтальное кросс-соединение (horizontal cross-connect, HCC). Монтажный шкаф, где горизонтальные кабели подсоединяются к коммуникационной панели, которая, в свою очередь, соединена магистральным кабелем с ГРС.

Графический пользовательский интерфейс (graphical user interface, GUI). Пользовательская

среда, в которой для ввода и вывода данных приложения используются рисунки и текст. В графическом пользовательском интерфейсе используется иерархическая и другие структуры для хранения данных. GUI обычно состоит из стандартных кнопок, пиктограмм и окон, а многие действия выполняются с помощью указательного устройства (например, мыши). Яркими примерами платформ, построенных на основе GUI, являются Microsoft Windows и Apple Macintosh.

Групповая или многоадресная передача (multicast). Способ передачи одиночных пакетов, при котором их копии рассылаются по нескольким адресам, определяемым *групповым адресом.*

Групповой адрес (multicast address). Общий адрес, который относится к некоторой группе сетевых устройств.

Групповой адрес зоны (zone multicast address). Зависящий от канала групповой адрес, по которому узел получает широковещательные сообщения NBP, посланные в его зону.

Д

Данные (data). Информация, передаваемая протоколами верхних уровней.

Двоичная система счисления (binary). Система счисления на основе единиц и нулей (1 — бит установлен, 0 — сброшен).

Двойное подключение (dual homing). Сетевая топология, в которой устройство подсоединяется к сети в двух точках доступа (называемых точками прикрепления). Одна точка доступа является первичным соединением, а вторая находится в пассивном состоянии и активизируется в случае обрыва первичного соединения.

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

Демаркация (demarcation). Точка, в которой заканчивается CPE и начинается местное ответвление службы. Часто находится в точке присутствия здания.

Демультиплексирование (demultiplexing). Разделение нескольких входящих потоков, уплотненных (мультиплексированных) в общем физическом сигнале, обратно на несколько внешних потоков. См. также *мультиплексирование.*

Диаграмма (без использования масштаба) (cut sheet). Указана прокладка кабелей и номера помещений, в которые они ведут.

Динамическая виртуальная сеть (dynamic VLAN). Виртуальная сеть, базирующаяся на MAC-адресах, логических адресах или типе протокола пакетов данных.

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

Дистанционно-векторный протокол маршрутизации (distance-vector routing protocol). Изучает все переходы в маршруте для построения дерева кратчайшего пути. Протокол заставляет все маршрутизаторы при каждом обновлении рассылать внутренние таблицы только своим со-

седям. Дистанционно-векторный протокол маршрутизации полностью не устраняет маршрутные петли, однако в вычислительном отношении, он проще, чем протокол состояния канала связи. Также называется алгоритмом маршрутизации Беллмана-Форда (Bellman-Ford routing algorithm).

Древовидная топология (tree topology). Топология локальной сети, подобная шинной топологии, но с тем отличием, что древовидные сети могут содержать ответвления с несколькими узлами. Сообщение от одной станции распространяется по всей линии передачи и получается всеми остальными станциями.

Дренажная область (catchment area). Зона, входящая в область, которую обслуживает устройство сетевого взаимодействия (например, концентратор).

Дуплексная передача (full duplex). Одновременная передача данных между станцией-отправителем и станцией-получателем. Ср. с *полудуплексной и симплексной переданей.*

Дуплексная сеть Ethernet (full-duplex Ethernet). Возможность одновременной передачи данных между передающей и принимающей станцией.

З

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

Загружаемый модуль NetWare (NetWare Loadable Module, NLM). Отдельная программа, которая может быть загружена в память и функционировать как часть сетевой операционной системы NetWare.

Задержка (delay). Время, между началом передачи пакета данных от отправителя к адресату и началом получения ответа отправителем. Также время, которое требуется пакету для того, чтобы дойти от отправителя к получателю по заданному пути.

Задержка очереди (s). Время ожидания данных перед тем, как они могут быть переданы в статистически мультиплексируемый физический канал.

Задержка передачи (backoff). Задержка передачи, вызванная коллизией.

Запрос ближайшего сервера (Get Nearest Server, GNS). Пакет запроса, посланный клиентом по IPX-сети с целью нахождения ближайшего активного сервера требуемого типа. Клиент сети IPX делает GNS-запрос для получения непосредственного ответа от подсоединенного сервера или ответа от маршрутизатора, который сообщает, в каком месте сети можно получить требуемую услугу. GNS является частью IPX SAP.

Запрос на комментарий (Request for Comment, RFC). Серия документов IETF с описаниями набора протоколов Internet и дополнительной информацией. Некоторые документы RFC приняты IAB как Internet-стандарты. Большинство документов RFC определяют такие протоколы, как Telnet и FTP, но некоторые носят юмористический или исторический характер. Документы RFC доступны на многих Web-узлах.

Затухание (attenuation). Величина потерь коммуникационного сигнала при передаче.

Зона (area). Логический набор сетевых сегментов (на основе CLNS, DECNet или OSPF) и присоединенных к ним устройств. Обычно зоны соединены с другими зонами с помощью маршрутизаторов и образуют единую автономную систему. См. также *автономная система.*

Зона (zone). 1. Совокупность всех терминалов, шлюзов и модулей многоточечного управления (multipoint control units, MCU), управляемых одним драйвером шлюза. В зону входит по крайней мере один терминал. Кроме того, в нее могут входить шлюзы и MCU. Зона имеет только один драйвер шлюза. Зона может не зависеть от топологии LAN или состоять из нескольких сегментов LAN, соединенных маршрутизаторами или другими устройствами. 2. В сетях AppleTalk — логическая группа сетевых устройств.

И

Идентификатор канального соединения (data-link connection identifier, DLCI). Величина, используемая для указания на наличие PVC или SVC в сети передачи фреймов. В базовой спецификации протокола передачи фреймов DLCI имеют локальное значение (т.е. подсоединенные устройства могут использовать различные значения для одного и того же соединения). В расширенной спецификации LMI идентификаторы канального уровня являются глобальными (т.е. указывают на индивидуальные оконечные устройства).

Идентификатор профиля службы (service profile identifier, SPID). Число, используемое некоторыми провайдерами услуг для определения служб, к которым подключено абонентское ISDN-устройство. SPID используется ISDN-устройством во время доступа к коммутатору, который инициализирует соединение с провайдером услуг.

Избыточность (redundancy). 1. При межсетевом обмене — дублирование устройств, служб и соединений. В случае неисправности позволяет избыточным устройствам, службам и соединениям выполнять функции неисправных. *2.* В телефонии — часть общей информации, содержащейся в сообщении, которая может быть изъята без потери смысла.

Инженерная группа по решению конкретной задачи в Internet (Internet Engineering task Force, IETF). Организация, состоящая более чем из 80 рабочих групп, и отвечающая за развитие стандартов Internet. IFTF работает под руководством ISOC.

Инкапсуляция (encapsulation). В сетевом контексте — помещение данных в пакет (фрейм) некоторого протокола. Например, данные перед передачей по сети Ethernet помещаются в фрейм Ethernet. Кроме того, при соединении разнородных сетей весь фрейм из одной сети целиком помещается во фрейм, используемый протоколом канального уровня другой сети. См. также *туннелирование.*

Институт инженеров по электротехнике и электронике (Institute of Electrical and Electronic Engineers, IEEE). Профессиональная организация, чья деятельность включает в себя разработку коммуникационных и сетевых стандартов. Сетевые стандарты IEEE для локальных сетей в настоящее время являются общепринятыми.

Интервал активности (keepalive interval). Период времени между сообщениями об активности (keepalive messages), посланными сетевым устройством.

Интерфейс (interface). 1. Соединение между двумя системами или устройствами. 2. В системах маршрутизации — соединение с сетью. 3. В телефонии — воображаемая граница раздела между характеристиками общей физической среды передачи данных, характеристиками сигналов и назначением передаваемых сигналов. 4. Граница раздела между соседними уровнями Эталонной модели OSI.

Интерфейс базовой скорости передачи (Basic Rate Interface, BRI). ISDN-интерфейс, состоящий из двух B-каналов и одного D-канала для канально-коммутируемой передачи голоса видео и других данных.

Интерфейс локального управления (Local Management Interface, LMI). Набор усовершенствований основной спецификации Frame Relay. Он включает в себя механизм извещений об активности, который проверяет состояние передачи данных, механизм широковещательных рассылок, который предоставляет сетевой сервер с локальным и широковещательным DLCI-интерфейсами, механизм глобальной адресации, который дает DLCI-интерфейсам глобальное, а не локальное значение в сетях Frame Relay, а также механизм определения статуса, который предоставляет отчет о текущем состоянии известных коммутатору DLCI-интерфейсов. В терминологии ANSI LMI называется LMT.

Интерфейс первичной скорости (основного уровня) (Primary Rate Interface, PRI). ISDN-интерфейс для основного доступа. Состоит из одного D-канала (64 Кбит/с) и двадцати трех (для T1) или 30 (для E1) B-каналов для голоса или данных.

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

Интерфейс прикладного программирования (Application programming interface, API). Спецификация вызовов функций, образующих интерфейс некоторой службы.

Интерфейс типа "пользователь-сеть" (User-Network Interface, UNI). Спецификация, определяющая стандарты взаимодействия для интерфейса между устройствами (маршрутизаторами или коммутаторами), расположенными в частной сети, и коммутаторами общедоступных сетей. Также используется для описания сходных соединений в сетях Frame Relay.

Информационный центр Internet (InterNIC). Организация, занимающаяся формированием, регистрацией и стратегическим развитием Internet, включая регистрацию доменных имен. Ранее назывался NIC.

Исключение перегрузки (congestion avoidance). Механизм регулирования трафика в сети ATM с целью сведения возможных задержек к минимуму. Для более эффективного использования ресурсов трафик с низким приоритетом приостанавливается на границе системы в случае, если он не может быть передан в данных условиях.

Исследование MAC-адресов (MAC address learning). Служба самообучающегося моста, в которой хранятся MAC-адреса отправителей для каждого полученного пакета. Эти адреса используются для передачи проходящих пакетов только через те мостовые интерфейсы, где расположены эти адреса. Пакеты с нераспознанным адресом передаются через все мостовые интерфейсы. Эта схема позволяет уменьшить трафик через присоединенные локальные сети. Служба исследования MAC-адресов определена в стандарте IEEE 802.1.

Источник бесперебойного питания (uninterruptable power supply, UPS). Резервное устройство, предназначенное для обеспечения питания в случае отсутствия электропитания. Обычно такие устройства устанавливаются на файловых серверах и на кабельных концентраторах.

Исходный маршрутизатор (seed router). Маршрутизатор в сети AppleTalk, в дескриптор порта которого встроен сетевой номер или кабельный диапазон. Исходный маршрутизатор определяет сетевой номер или кабельный диапазон для других маршрутизаторов данного сетевого сегмента и отвечает на запросы конфигурации от неисходных маршрутизаторов подключенной к нему сети AppleTalk, благодаря чему эти маршрутизаторы могут подтвердить свою конфигурацию или изменить ее соответствующим образом. В каждой сети AppleTalk должен быть хотя бы один исходный маршрутизатор См. также *неисходный маршрутизатор.*

К

Кабель категории 1 (category I cabling). Один из пяти уровней UTP-кабеля, описанный в стандарте EIA/TIA-586. Кабель категории 1 применяется для телефонных коммуникаций и не подходит для передачи данных. См. также *EIA/TIA-586* и *неэкранированна^ витая пара (UTP).*

Кабель категории 2 (category 2 cabling). Один из пяти уровней UTP-кабеля, описанный в стандарте EIA/TIA-586. Кабель категории 2 обеспечивает передачу данных со скоростью до 4 Мбит/с. См. также *EIA/TIA-586* и *неэкранированная витая пара (UTP).*

Кабель категории 3 (category 3 cabling). Один из пяти уровней UTP-кабеля, описанный в стандарте EIA/TIA-586. Кабель категории 3 применяется в сетях lOBaseT и обеспечивает передачу данных со скоростью до 10 Мбит/с. См. также *EIA/TIA-586* и *неэкранированная витая пара (UTP).*

Кабель категории 4 (category 4 cabling). Один из пяти уровней UTP-кабеля, описанный в стандарте EIA/TIA-586. Кабель категории 4 применяется в сетях Token Ring и обеспечивает передачу данных со скоростью до 16 Мбит/с. См. также *EIA/TIA-586* и *неэкранированная витая пара (UTP).*

Кабель категории 5 (Category 5 cabling). Один из пяти уровней UTP-кабеля, описанный і стандарте EIA/TIA-586. Кабель категории 5 обеспечивает передачу данных со скоростью дс 100 Мбит/с. См. также *EIA/TIA-586* и *неэкранированная витая пара (UTP).*

Кабельный диапазон (cable range). Диапазон сетевых номеров, доступных для использования узлами расширенной сети AppleTalk. Может иметь одно или несколько значений. Адреса присваиваются узлам в пределах кабельного диапазона.

Канал (circuit). Коммуникационный путь между двумя, или более точками.

Канал (link). Сетевой канал связи, состоящий из линии или пути передачи данных от отправителя к получателю и соответствующего оборудования. Этот термин наиболее часто употребляется в контексте соединения распределенной сети. Иногда называете? линией или каналом передачи данных.

Канал "точка-точка" (point-to-point link). Канал, обеспечивающий единый, заранее установленный путь коммуникации от стационарного оборудования потребителя до удаленной сети через сеть-носитель, такую как телефонная компания. Также называется выделенной или арендованной линией.

Канал распределенной сети (WAN **link).** Коммуникационный канал распределенной сети, состоящий из линии или пути передачи данных от отправителя к получателю и соответствующего оборудования.

Канальная группа (circuit group). Группа собранных вместе последовательных каналов, связывающих два моста. Если один из каналов группы находится в связующем дереве сети, то любой из последовательных каналов группы может использоваться для распределения нагрузки. Такая стратегия распределения нагрузки позволяет избежать проблем упорядочения данных путем назначения для каждого адреса приемника отдельного последовательного канала.

Канальный уровень (data link layer). Второй уровень эталонной модели OSI. Обеспечивает точную передачу данных по физическому каналу. Занимается физической адресацией, сетевой топологией, дисциплиной линий связи, сообщениями об ошибках, порядком доставки фреймов и управлением потоками данных. Разделен IEEE на два подуровня: MAC и LLC. Канальный

уровень примерно соответствует уровню управления каналом связи (data link control layer) в модели SNA.

Карта маршрута (route map). Метод контроля перераспределения маршрутов между доменами маршрутизации.

Качество обслуживания (quality of service, QoS). Показатель эффективности системы передачи данных, который отражает качество передачи и обслуживания.

Кбайт, килобайт (kilobyte, kB). Равен 1024 байт.

Кбайт/с, килобайт в секунду (kilobytes per second, kBps). Скорость передачи данных, выраженная в количестве байт, посланных за одну секунду.

Кбит, килобит (kilobit, kb). Равен 1024 бит.

Кбит/с, килобит в секунду (kilobits per second, kbps). Скорость передачи данных в канале связи, выраженная в количестве бит, посланных за одну секунду.

Квитирование (handshake). Последовательность сообщений, которыми обмениваются два и более сетевых устройства для гарантированной синхронизации

Клиент (client). Узел сети или набор программного обеспечения (от начального до оконечного устройства), обращающийся за услугами к *серверу*.

Клиент/сервер (client/server). Архитектура соединения в сети рабочей станции и сервера.

Клиент/серверная модель (client/server model). Распространенный способ описания сетевых служб и пользовательских процессов (программ) для этих служб. В качестве примера можно привести систему доменных имен (DNS), взаимодействие между файловым сервером и клиентскими приложениями, а также бездисковые рабочие станции.

Клиент/серверные вычисления (client/server computing). Способ распределенной обработки данных в сетевых системах, при котором обработка транзакций делится на две части: клиентскую (front end) и серверную (back end). Оба термина (клиент и сервер) могут применяться как для программного, так и для аппаратного обеспечения. Они также называются распределенными вычислениями или распределенной обработкой данных (distributed computing). Ср. с *одноранговые вычисления*. См. также *удаленный вызов процедур*.

Коаксиальный кабель (coaxial cable). Провод, имеющий соосное (коаксиальное) расположение центрального проводника, окруженного изолятором, и внешнего проводника, выполненного в виде проволочной оплетки. В локальных сетях используются два типа коаксиального кабеля: с сопротивлением 50 Ом для передачи цифровых сигналов и с сопротивлением 75 **Ом** для передачи аналоговых сигналов, а также для высокоскоростных цифровых сигналов.

Кодирование (coding). Технология передачи двоичных сигналов.

Кодирование (encoding). Процесс представления битов в виде **импульсов** напряжения.

Количество переходов (hop count). Метрика маршрутизации, используемая для измерения расстояния между отправителем и получателем. Эта метрика используется в качестве базовой в протоколе RIP.

Коллизионный домен (collision domain). В сети Ethernet — участок, в котором распространяются столкнувшиеся фреймы. Повторители и концентраторы позволяют распространяться коллизиям, в то время как коммутаторы, мосты и маршрутизаторы их останавли-

вают.

Коллизия (collision). В сети Ethernet коллизии происходит в результате одновременной передачи фреймов с двух узлов. При встрече в передающей среде, происходит столкновение фреймов, что приводит к искажению формы передаваемого сигнала и, как следствие, потере передаваемых данных.

Кольцевая топология (ring topology). Сетевая топология, которая состоит из набора повторителей, связанных однонаправленными каналами и образующих одну замкнутую петлю. Каждая сетевая станция подключается к сети через повторитель. Чаще всего кольцевая топология образует звезду в виде замкнутой петли.

Кольцо (ring). Соединение двух и более станций по логически кольцевой топологии. Информация передается последовательно между активными станциями. На этой топологии основаны протоколы Token Ring, FDDI и CDDI.

Коммутатор (switch). Сетевое устройство, которое фильтрует, перенаправляет и рассылает фреймы на основе адресов пункта назначения каждого из них. Коммутаторы выполняют операции на уровне канала связи эталонной модели OSI.

Коммутационная панель (patch panel). Сборка из гнезд портов, которая может быть установлена на стойке или на стенной скобе в монтажном шкафу. Эти панели действуют как платы переключателей, соединяющие кабели рабочих станций между собой и с внешними кабелями.

Коммутация (switching). Процесс принятия входящего фрейма на одном интерфейсе и отправки его через другой.

Коммутация без фрагментации (fragment-free switching). Методика коммутации, при которой до начала перенаправления отбрасываются фрагменты, подвергшиеся коллизиям. Большинство из них содержат ошибки.

Коммутация каналов (circuit switching). Система коммутации, при которой во время сеанса связи должен существовать физический канал между отправителем и получателем. Широко используется в сетях телефонных компаний. С технологической точки зрения, коммутацию каналов можно рассматривать, как противоположность коммутации пакетов и сообщений, а с точки зрения методов доступа — как противоположность конкуренции и передаче маркеров.

Коммутация пакетов (packet switching). Сетевая технология, при которой узлы обмени-заются друг с другом пакетами данных по одному каналу связи.

Коммутация с быстрой отправкой (fast-forward switching). Коммутация, с наименьшей задержкой. Пакет перенаправляется немедленно после получения адреса пункта назначения.

Коммутация с промежуточным хранением пакетов (store-and-forward). Методика коммутации пакетов, при которой фреймы полностью обрабатываются до отправки на порт передачи, Эгот процесс включает в себя вычисление CRC и проверку адреса пункта назначения. Кроме того, фреймы должны временно храниться до тех пор, пока не появятся сетевые ресурсы для отправки сообщения (например, неиспользуемые каналы).

Коммутируемая линия (dialup line). Канал связи, устанавливаемый с помощью коммутации каналов в телефонной сети.

Коммутируемый виртуальный канал (switched virtual circuit, SVC). Виртуальный канал, устанавливаемый динамически по требованию и ликвидируемый после окончания передачи. Коммутируемые виртуальные каналы используются в ситуациях спорадической передачи данных.

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

Конкуренция (contention). Метод доступа, при котором сетевые устройства конкурируют друг с другом за право доступа к передающей среде.

Консоль (console). Терминальное оборудование, с помощью которого вводятся команды для узла.

Контрольное прослушивание (watchdog spoofing). Операции прослушивания, выполняемые маршрутизатором, работающим для клиента NetWare, который посылает серверу NetWare контрольные пакеты для поддержания активного сеанса между клиентом и сервером. См. также *спуфинг.*

Контрольный пакет (watchdog packet). Гарантирует, что клиент все еще подключен к серверу NetWare. Если сервер не получает от клиента данных в течение определенного времени, он посылает этому клиенту ряд контрольных пакетов. Если станция не отвечает на определенное количество контрольных пакетов, сервер считает, что связь с ней оборвалась, и отменяет соединение с этой станцией.

Контрольный таймер (watchdog tinier). 1. Механизм, используемый аппаратным или программным обеспечением для инициирования события или выхода из процесса после истечения определенного интервала времени. 2. В NetWare — таймер, показывающий максимальный период времени, в течение которого сервер будет ждать ответа клиента на контрольный пакет. По истечении этого времени сервер посылает еще один контрольный пакет, и так до тех пор, пока не будет получен ответ или не будет отправлено максимальное количество пакетов.

Концевик (trailer). Управляющая информация, прикрепленная к данным при их инкапсуляции для передачи по сети.

Концентратор (hub). 1. Устройство, служащее центром сети с топологией типа "звезда" Также называется *многопортовым повторителем (multipart repeater).* 2. Аппаратное или программное обеспечение, посредством которого соединяются несколько независимых модулей сети или сетевого оборудования. Концентраторы бывают активные (усиливают сигналы, проходящие через них) или пассивные (не усиливают, а просто пропускают сигналы через себя).

Кэширование (caching). Форма репликации, при которой информация, полученная во время предыдущей транзакции, используется для обработки последующих транзакций.

Л

Лавинная передача (flooding). Техника передачи данных, используемая коммутаторами и мостами. Трафик, полученный устройством, отправляется дальше через все интерфейсы этого устройства, исключая принявший интерфейс.

Латентность или время ожидания (latency). Задержка между временем отправления запроса на доступ в сеть и временем получения разрешения на передачу.

Локальная передача (local-area transport, LAT). Протокол сетевого виртуального терминала, разработанный корпорацией Digital Equipment Corporation.

Локальная сеть (local-area network, LAN). Высокоскоростная, надежная сеть передачи дан-

ных, охватывающая относительно малую географическую площадь (до нескольких тысяч метров). Локальные сети соединяют рабочие станции, терминалы, периферийные и другие устройства, находящиеся в одном здании или другом географически ограниченном пространстве. Стандарты локальных сетей определяют прокладку кабеля и прохождение сигналов на физическом и канальном уровнях эталонной модели OSI. Ethernet, FDDI и Token Ring — примеры широко используемых технологий локальных сетей.

Локальная фильтрация трафика (local traffic filtering). Процесс, с помощью которого мост фильтрует (отбрасывает) кадры с MAC-адресами источника и приемника, которые относятся к одному и тому же интерфейсу моста, предотвращая таким образом избыточный трафик через этот мост. Локальная фильтрация трафика описывается стандартом IEEE 802.1.

M

Магистраль (backbone). Основная часть любой распределенной сети, соединяющая воедино все компоненты сети для обеспечения связи.

Магистральная прокладка кабеля (backbone cabling). Прокладка соединительных кабелей между монтажными шкафами, между монтажными шкафами и точкой присутствия (POP), а также между зданиями, являющимися частью одной локальной сети.

Максимальная единица передачи данных (maximum transmission unit, MTU). Максимальный размер пакета, измеряемый в байтах, который может обрабатываться конкретным интерфейсом.

Максимальная скорость передачи (maximum rate). Суммарное максимальное количество данных, переданных по заданному виртуальному каналу в единицу времени. Равно сумме гарантированного и негарантированного графика, полученного от источника. В случае перегрузки сети негарантированный трафик может быть отброшен. Максимальная скорость, **которая** не может превышать среднюю, представляет собой наибольшую пропускную способность виртуального канала, измеряемую в битах или ячейках в секунду.

Малый офис/домашний офис (small office/home office, SOHO). Такой офис объединяет несколько пользователей, нуждающихся в соединении, которое обеспечивало бы более быструю и надежную связь, чем аналоговое коммутированное соединение.

Маркер (token). Фрейм, содержащий управляющую информацию. Владение маркером дает сетевому устройству право на передачу данных по сети. См. также *передача маркера.*

Маркерная шина (token bus). Архитектура локальной сети с шинной топологией и доступом с передачей маркера. Такая сеть является основой для спецификации LAN IEEE 802.4.

Маршрутизатор (router). Устройство сетевого уровня, которое использует одну или несколько метрик для определения оптимального пути прохождения потока данных. Маршрутизаторы перенаправляют пакеты из одной сети в другую, основываясь на информации сетевого уровня. Иногда называются *шлюзами (gateway),* хотя это название все более устаревает.

Маршрутизация (routing). Определение пути к получателю. Маршрутизация в больших сетях очень сложна, так как пакет по дороге к получателю может пройти через множество потенциальных промежуточных точек.

Маршрутизация по кратчайшему пути (shortest-path routing). Маршрутизация, при которой с помощью специального алгоритма минимизируется расстояние, или путевые затраты.

Маршрутизация с коммутацией по запросу (dial-on-demand routing, DDR). Вид маршрутизации при котором маршрутизатор открывает и закрывает сеанс коммутации цепей только тогда, когда в этом нуждаются оконечные передающие станции.

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

Маска (mask). См. *адресная маска* и *маска подсети.*

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

Мбайт, мегабайт (megabyte, MB). Равен 1024 Кбайт, или 1048576 байт. **Мбит, мегабит (megabit, Mb).** Равен 1024 Кбит, или 1048576 бит.

Мбит/с, мегабит в секунду (megabits per second, Mbps). Скорость передачи данных, выраженная в количестве Мбит, переданных по каналу связи в единицу времени.

Мгновенное изменение (flash update). Отправка сообщения об изменении до истечения стандартного периода времени отправки таких сообщений. Используется для уведомления других маршрутизаторов о смене метрики.

Международная организация по стандартизации (International Organization for Standardization, ISO). Международная организация, отвечающая за большое количество стандартов, включая стандарты, относящиеся к работе в сетях. Эта организация разработала популярную Эталонную модель OSI.

Международная электротехническая комиссия (International Electrotechnical Commission IEC). Промышленная группа, которая **создает и** распространяет стандарты электрической продукции и ее компонентов.

Международный консультативный комитет по телефонии и телеграфии (Consultativ Committee for International Telegraph and Telephone, CCITT). Международная организация, которая отвечает за развитие телекоммуникационных стандартов. В настоящее время переименована и называется ITU-T. См. *ITU-T.*

Местное ответвление (local loop). Кабель (обычно медный провод), идущий от лини демаркации до центрального офиса провайдера распределенной сети.

Метрика (metric). Стандартизованная числовая характеристика (например, длина пути), используемая протоколами маршрутизации для нахождения оптимального пути пункту назначения.

Метрика маршрутизации (routing metric). Метод, используемый маршрутизатором для определения лучшего из нескольких маршрутов. Эта информация хранится в таблицах маршрутизации. Метрики могут использовать такие параметры, как ширина полосы пропускания, стоимость соединения, величину задержки, количество переходов, величину нагрузка MTU, стоимость пути и надежность. Часто называется просто *метрикой.*

Микросегментация (microsegmentation). Разделение сети на более мелкие сегменты (Обычно с целью увеличения полосы пропускания сетевых устройств).

Министерство обороны США (Department of Defense, DOD). Правительственная организация США, которая отвечает за национальную безопасность. Министерство обороны CLLL часто

участвует в финансировании развития коммуникационных протоколов.

Многомодовый волоконно-оптический кабель (multimode fiber). Волоконно-оптически кабель, обеспечивающий передачу световых сигналов на нескольких разных частотах.

Многоточечное соединение (point-to-multipoint connection). Один из двух фундаментальных типов связи. В ATM многоточечное соединение является однонаправленным, при котором одиночная конечная система-источник (называемая корнем) подключается нескольким конечным системам-приемникам (называемым листьями).

Множественный доступ с контролем несущей и обнаружением коллизий (carrier sense multiple access collision detect, CSMA/CD). Механизм доступа, в котором устройства готовые к отправке, сначала, проверяют канал на наличие передачи. Если она не определена за заданный период времени, устройство может начать передачу. Если два устройства передают одновременно, происходит столкновение, которое определяете всеми устройствами, вовлеченными в конфликт. Для разрешения конфликта на некоторое время задерживается передача с этих устройств. Сети Ethernet и IEEE 802.3 используют CSMA/CD.

Модем (модулятор-демодулятор) (Modulator-demodulator, modem). Устройство, преобразующее цифровые сигналы в аналоговые и наоборот. На станции-отправителе модем преобразует цифровые сигналы в форму, соответствующую передаче по каналам аналоговой связи. В пункте назначения аналоговые сигналы преобразуются в цифровую форму. Модемы позволяют передавать информацию по телефонным линиям.

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

Модуль данных протокола моста (bridge protocol data unit, BPDU). Пакет приветствия протокола распределенного связующего дерева, посылаемый через заданные интервалы для обмена информацией между мостами в сети.

Модуль множественного доступа (multistation access unit, MSAU). В сетях Token Ring — концентратор, внутри которого образовано кольцо из конечных станций, подключаемых к MSAU радиально. MSAU образует интерфейс между ними и интерфейсом Token Ring маршрутизатора. Иногда называется MAU.

Мост (bridge). Устройство, которое соединяет два сегмента сети, использующих один протокол связи, и передает пакеты от одного к другому. Мосты работают на канальном уровне (второй уровень) эталонной модели OSI. Вообще мост фильтрует, перенаправляет или рассылает входящий кадр, базируясь на его MAC-адресе.

Мостовая технология (bridging). Технология, в которой мост соединяет два или более сегмента локальной сети (LAN).

Мультиплексирование (multiplexing). Схема одновременной передачи нескольких логических сигналов по одному физическому каналу.

Мультипротокольная маршрутизация или маршрутизация, использующая несколько протоколов (multiprotocol routing). Используется в применении к маршрутизаторам, которые выполняют пересылку пакетов различных маршрутизирующих протоколов, таких как TCP/IP или IPX через одни и те же каналы передачи данных.

Н

Нагрузка (load). Величина, отражающая сетевую активность некоторого ресурса, такого, например, как маршрутизатор или канал.

Надежность (reliability). Величина, представляющая собой отношение числа ожидаемых подтверждений активности к числу полученных. Если этот коэффициент велик, то канал считается надежным. Используется в качестве одной из метрик маршрутизации.

Национальный институт стандартизации США (American National Standards Institute,

ANSI). В ANSI входят корпоративные, государственные и другие организации с целью координации действий в отношении стандартов. ANSI определяет национальные стандарты США, а также участвует от имени США в международных организациях стандартизации. ANSI помогает создавать международные и национальные стандарты, в частности, в области сетей и телекоммуникаций. ANSI является членом IEC и ISO. См. также *IEC* и *ISO*.

Начальная загрузка (bootstrap). Простая, заранее установленная операция загрузки начального блока инструкций, которые, в свою очередь, вызывают загрузку в память других инструкций или вход в другой конфигурационный режим. **Негарантированная доставка или "доставка в лучшем случае" (best-effort delivery).** Такая доставка осуществляется в том случае, когда сетевая система не использует сложные механизмы подтверждений для гарантированной доставки информации. **Неисходный маршрутизатор (nonseed router).** В сетях AppleTalk — маршрутизатор, который перед началом работы должен сначала получить, а затем проверить свою конфигурацию по отношению к исходному маршрутизатору. См. также *исходный маршрутизатор*.

Неоднородная сеть (multivendor network). Сеть, построенная на основе оборудования от разных производителей. В такой сети возникает гораздо больше проблем совместимости, чем в сети с однотипным оборудованием.

Нерасширяемая сеть (nonextended network). Сеть AppleTalk Phase 2, которая поддерживает адресацию до 253 узлов только одной зоны.

Несущая частота (carrier). Электромагнитные колебания фиксированной частоты, модулируемые другим сигналом для передачи данных.

Нетупиковая зона (nonstub area). Насыщенная ресурсами OSPF-зона, которая передает стандартные, статические, внутризонные, межзонные и внешние маршруты. Только в таких OSPF-зонах существуют конфигурированные виртуальные каналы и только в них содержатся ASBR. Ср. с *тупиковая зона*.

Неэкранированная витая пара (unshielded twisted-pair, UTP). Кабель из четырех пар, использующийся для различных сетей. UTP не требует фиксированного пространства между соединениями, которое необходимо для коаксиальных кабелей. Всего существует пять часто используемых типов кабелей UTP. Они называются категориями с первой по пятую.

Номер сокета (socket number). Восьмиразрядное число, идентифицирующее сокет. В узле AppleTalk может быть назначено не более 254 различных номеров сокетов.

Номер хоста (host number). Часть IP-адреса, которая обозначает адресуемый узел подсети. Также называется *адресом хоста*.

O

Обновление маршрутной информации (routing update). Сообщение, посылаемое маршрутизатором о доступности сети и содержащее дополнительную информацию о стоимости маршрута. Эти сообщения обычно посылаются регулярно или после изменения сетевой топологии. Ср. с *мгновенное изменение.*

Обновление с расщеплением горизонта (split horizon updates). Метод маршрутизации, при котором запрещается передача маршрутной информации через интерфейс маршрутизатора, через который эта информация была получена. Обновление с расщеплением горизонтов предотвращает образование маршрутных петель.

Оборонная сеть обмена данными (Defense Data Network, DDN). Глобальная сеть Министерства обороны США, состоящая из несекретной части (MILNET), а также секретной и совершенно секретной частей. Управляется и поддерживается DISA.

Оборудование заказчика (customer premises equipment, CPE). Оконечное оборудование, такое как терминалы, телефоны и модемы, поддерживаемые телефонной компанией, установленные на территории клиента этой компании и подключенные к ее сети.

Оборудование оконечной цепи (data circuit-terminating equipment, DCE). Устройство, используемое для конвертирования данных пользователя из DTE в форму, допускаемую оборудованием службы распределенной сети.

Оборудование терминала данных (data terminal **equipment, DTE).** Устройство, расположенное на пользовательском конце интерфейса пользователь-сеть, которое может выступать в качестве источника данных, получателя данных или в качестве обоих. DTE соединяется с сетью данных посредством устройства DCE (например, модема) и обычно использует временные сигналы, генерируемые **DCE.** Оборудование терминала данных включает в себя такие устройства, как компьютеры, трансляторы протоколов и мультиплексоры.

Обратная передача (Reverse Path Forwarding, RPF). Метод многоадресной передачи, при котором многоадресные дейтаграммы направляются через все интерфейсы кроме принимающего, если принимающий интерфейс используется для передачи одноадресных дейтаграмм к источнику многоадресной дейтаграммы.

Обратное исправление (poison reverse update). Свойство протокола IGRP, имеющее целью избежать возникновения маршрутных петель. Как только обрывается связь с некоторой сетью, анонсирующий ее маршрутизатор сохраняет в своей таблице данные об этой сети на время посылки нескольких периодических сообщений об обновлении. При этом в широковещательных сообщениях указывается бесконечная стоимость маршрута к сети, с которой отсутствует связь.

Обратное явное уведомление о перегрузке (Backward Explicit Congestion Notification, BECN). Бит, устанавливаемый во фреймах протокола Frame Relay, которые передаются в направлении, обратном тому, в котором передаются кадры, столкнувшиеся с перегруженным маршрутом. DTE-устройства, получающие фреймы с BECN-битом, могут потребовать, чтобы протоколы высшего уровня предприняли соответствующие действия по управлению потоком данных.

Обрезной инструмент (punch tool). Снабженный пружиной инструмент, используемый для резки кабеля и для подсоединения его к гнезду или к коммутационной панели.

Объединенная сеть (internetwork). Комплекс сетей, связанных маршрутизаторами и другими устройствами. Обычно функционирует как единая сеть. Иногда называется internet. Этот термин не следует путать с названием глобальной сети Internet.

Одиночная передача (unicast). Сообщение, направленное единственному адресату. **Одиноч-**

ный адрес (unicast address). Адрес, определяющий отдельное сетевое устройство.

Одноранговые вычисления (peer-to-peer computing). Процесс выполнения клиентской и серверной части приложения на одном сетевом устройстве. Также описывает соединение между двумя разными сетевыми устройствами, принадлежащими к одному уровню эталонной модели OSI.

Однородная сеть (single-vendor network). Сеть, состоящая из оборудования одного производителя. В однородных сетях проблемы совместимости очень редки. См. также *неоднородная сеть*.

Окно (window). Число октетов, которое может послать отправитель до ожидания сигнала подтверждения приема.

Октет, восьмибитовый байт (octet). В вычислительных сетях чаще говорят "октет", чем | "байт", поскольку в архитектуре некоторых машин используются байты другой длины.

Оперативное запоминающее устройство, ОЗУ (Random-Access Memory, RAM). Временное j запоминающее устройство, данные которого заносятся и считываются микропроцессором.

Операционная система NetWare (NetWare). Широко распространенная операционная | система, разработанная корпорацией Novell. Обеспечивает прозрачный доступ к удаленным файлам и многие другие сетевые услуги.

Определение пути (path determination). Принятие решения о том, по какому пути направить поток данных в **сетевом** пространстве. Определение пути происходит на сетевом уровне эталонной модели OSI.

Основной уровень (core layer). Уровень, который обеспечивает быстрое соединение между географически удаленными точками, соединяя несколько университетских сетей в распределенную сеть корпорации или предприятия.

Открытая сеть передачи данных (public data network, PDN). Принадлежащие государству (как в Европе) или частным концернам (как в США) сети, обеспечивающие общедоступную компьютерную связь, обычно платную. PDN позволяют небольшим организациям создавать распределенные сети без затрат на прокладку каналов связи на дальние расстояния.

Открытый канальный интерфейс (Open Data-Link Interface, ODI). Спецификация Novell, описывающая стандартный интерфейс для сетевых адаптеров (network interface cards, NIC), благодаря которому разные протоколы могут использовать один NIC. См. также *сетевая плата*.

Отображение адреса (address mapping). Метод, обеспечивающий взаимодействие разных протоколов за счет преобразования формата адреса. Например, для передачи IP-пакетов по сети X.25 IP-адреса должны преобразовываться в адреса X.25. См. также *преобразование адресов (address resolution).*

Оценка (cost). Величина любого типа, вычисляемая на основе количества переходов, ширины полосы пропускания передающей среды и других параметров, задаваемая сетевым администратором и используемая для сравнения различных путей в сетевом пространстве.

Очередность (queuing). Положение, при котором списки управления доступом задают обработку маршрутизатором некоторых пакетов ранее всех остальных данных.

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

Ошибка качества сигнала (signal quality error, SQE). Сообщение, посылаемое трансиве-ром контроллеру и уведомляющее последний о работоспособности канала. Также называется пульсацией (heartbeat).

П

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

Память, адресуемая по содержимому (content-addressable memory, CAM). Вид организации данных, при которой доступ к данным происходит не по адресу ячейки, а по ее содержимому.

Параллельная передача (parallel transmission). Способ передачи данных, при котором / биты символов передаются одновременно по нескольким каналам. Ср. с *последова- I тельная передача.*

Перегрузка сети (congestion). Ситуация, когда величина потока передаваемых данных превышает пропускную способность сети.

Передача маркера (token passing). Метод доступа, с помощью которого сетевые устройства получают доступ к физической среде в порядке очереди, в зависимости от владения маленьким фреймом-маркером. Противоположен коммутации каналов (circuit switching) и конкуренции (contention). См. также *маркер.*

Перенаправление (redirect). Часть протоколов ICMP и ES-IS, которые позволяют маршрутизатору извещать хост о том, что использование другого маршрутизатора будет более эффективным.

Пересылка данных (forwarding). Процесс передачи фрейма к приемнику с помощью маршрутизирующего устройства.

Пересылка фреймов (frame forwarding). Механизм, посредством которого трафик, генерируемый такими протоколами как HDLC и SDLC, передается в виде ячеек по сети ATM.

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

Петлевой контроль (loopback test). Тест, основанный на передаче и обратном получении сигналов от некоторого источника к некоторому приемнику по заданному каналу связи. Петлевой контроль часто используется для проверки исправности сетевого интерфейса.

Петля (loop). Маршрут, в котором пакеты никогда не достигают места назначения, так как циркулируют по одной и той же цепочке сетевых узлов.

Платная часть сети (toll network). Коллективные коммутаторы и другие устройства (называемые магистралями или стволами) в среде провайдера распределенной сети.

Повторитель (repeater). Устройство, которое восстанавливает и распространяет электрические сигналы между двумя сегментами сети.

Пограничный маршрутизатор (border router). Маршрутизатор, расположенный на границе сети и обеспечивающий функции защиты некоторой частной области сети от внешних сетей или от более доступных областей сети.

Пограничный маршрутизатор автономной системы (autonomous system boundary router, ASBR). Маршрутизатор, расположенный между автономной системой, в которой используется протокол OSPF и системой, в которой протокол OSPF не используется. Он может работать с протоколом OSPF и другими протоколами маршрутизации, например RIP. ASBR должен находиться в открытой зоне OSPF.

Подсеть (subnetwork). 1. Сеть, которая разделена на ряд сетей небольшого размера. 2. В IP-сетях — сети, которым назначен общий адрес сети.

Подтверждение (уведомление) (acknowledgment). Специальный сигнал, который посылается от одного сетевого устройства к другому для подтверждения, что произошло некоторое событие (например, получение сообщения). Иногда используется сокращение АСК.

Подынтерфейс или вспомогательный интерфейс (subinterface). Один из нескольких вир-

туальных интерфейсов одного физического интерфейса.

Полезная нагрузка (payload). Часть ячейки, кадра или пакета, которая содержит информацию верхнего уровня (данные).

Полно-сеточная топология (fully meshed topology). Топология, в которой каждое устройство сети ретрансляции фреймов имеет PVC со всеми остальными устройствами многоточечной распределенной сети.

Полудуплексная передача (half duplex). Способность канала в каждый момент времени или передавать, или принимать информацию. Примером полудуплексного протокола является BSC. Ср. *с дуплексной и симплексной переданей.*

Полудуплексная сеть Ethernet (half-duplex Ethernet). Возможность передачи данных за один раз только в одном направлении между передающей и принимающей станциями.

Порт (port). 1. Интерфейс сетевого устройства (например, маршрутизатора). 2. Охватывающий разъем на коммутационной панели, к которому подключается разъем такого же размера, например RJ-45. Чтобы соединить компьютеры, подключенные к коммутационной панели, используются распределительные шнуры. Это называется перекрестным соединением (кроссировка), которое позволяет функционировать локальной сети. 3. В терминологии протокола IP — процесс верхнего уровня, который получает информацию от процесса нижнего уровня. Порты пронумерованы и большинство из них ассоциировано с конкретным приложением или протоколом. Например, протоколу SMTP соответствует порт 25. Номера протоколов этого типа называются стандартными, или широко известными (well-known)

Последовательная передача (serial transmission). Метод передачи данных, при котором биты символов передаются последовательно по одному каналу. Ср. с *параллельная передача.*

Постоянное запоминающее устройство (read-only memory, ROM). Энергонезависимая память, данные которой можно прочитать, но нельзя записать.

Постоянный виртуальный канал (permanent virtual circuit, PVC). Виртуальный канал, установленный на постоянный режим работы. Постоянные виртуальные каналы экономят полосу пропускания, затрачиваемую на создание канала и на его ликвидацию, в ситуациях, когда виртуальная цепь должна существовать постоянно.

Поток (flow). Совокупность данных, проходящих в сети между двумя конечными точками (например, от одной LAN-станции к другой). В одном канале могут передаваться сразу несколько потоков.

Почта, телефон и телеграф (post, telephone and telegraph, PIT). Государственная организация, предоставляющая телефонные услуги в США. Филиалы PTT имеются в большинстве регионов и за пределами Северной Америки; они обеспечивают местные, междугородные и международные телефонные услуги.

Преобразование адресов (address resolution). Способ обнаружения различий между схемами адресации компьютеров. Обычно определяет способ отображения адресов сетевого уровня (уровень 3) на адреса канального уровня (уровень 2). См. также *отображение адреса (address mapping).*

Преобразование имен (name resolution). Обычно так называют процесс связывания имени с сетевым адресом.

Прерывание (trap). Сообщение, посылаемое агентом SNMP на NMS, консоль ил? терминал, чтобы известить о значительном событии, таком как выполнение некоторого условия или дос-

тижение предельного значения.

Приложение (application). Программа, выполняющая некоторую функцию непосредственно для пользователя. Клиентские программы FTP **и Telnet являются** примерами сетевых приложений.

Приложение типа клиент/сервер (client/server application). Приложение, которое хранится централизовано на сервере и используется рабочими станциями. За счет подобной организации облегчается обслуживание и защищенность приложений.

Приоритетная очередность (priority queuing). Функция маршрутизации, которая присваивает фреймам в выходной очереди интерфейса приоритет на основе различных характеристик, таких как размер пакета и тип интерфейса.

Провайдер (оператор связи) (common carrier). Зарегистрированная частная компания — владелец сети передачи данных, которая предоставляет всем желающим платные телекоммуникационные услуги.

Проверка доступности адресата (packet internet groper, ping). Эхо-сообщение ICMP и ответ на него. Часто используется в IP-сетях для проверки доступности сетевого устройства.

Программа управления сетью (Network Control Program, NCP). Программа, осуществляющая маршрутизацию и управление потоком данных между коммуникационным контроллером и другими сетевыми ресурсами.

Программируемое постоянное запоминающее устройство (programmable read-only memory, PROM). ПЗУ, которое можно запрограммировать с помощью специального устройства. Модули PROM можно запрограммировать только один раз. Ср. с *EEPROM.*

Прокси (proxy). 1. Объект, который, для большей эффективности, дублирует другой объект. 2. Специальные шлюзы, которые ретранслируют один сеанс H.323 другому сеансу.

Промежуточная распределительная станция, ПРС (intermediate distribution facility, IDF).

Вторичная коммуникационная комната здания, в котором используется звездообразная сетевая топология. ПРС зависима от ГРС.

Простая сеть (flat network). Сеть, состоящая из одного широковещательного домена, в которой между коммутаторами нет маршрутизаторов. Широковещательные пакеты и передачи на канальном уровне посылаются каждому коммутируемому порту.

Простой протокол передачи файлов (Trivial File Transfer Protocol, TFTP). Упрощенная версия протокола FTP, которая позволяет передавать файлы по сети с одного компьютера на другой.

Простой протокол управления сетью (Simple Network Management Protocol, SNMP). Протокол управления сетью, используемый почти исключительно в сетях TCP/IP. SNMP предоставляет средства контроля и управления сетевыми устройствами, конфигурациями, производительностью и безопасностью, а также сбора статистической информации.

Протокол (protocol). Формальное описание набора соглашений и правил, которые определяют обмен информацией между устройствами в сети.

Протокол "точка-точка" (Point-to-point Protocol, PPP). Разработанный с целью замены SLIP, протокол, обеспечивающий соединения между маршрутизаторами и соединение хоста с сетью по синхронным и асинхронным каналам связи.

Протокол IP (Internet Protocol, IP). Протокол сетевого уровня из семейства TCP/IP, предназначенный для объединения сетей на основе технологии не требующей установки соединения с получателем. Протокол IP обладает возможностями адресации, спецификации типа обслуживания, фрагментации и сборки, а также обеспечения безопасности. Описан в RFC 791.

Протокол IP версии б (IP version 6, IPv6). Усовершенствованный вариант используемой в настоящее время версии 4 протокола IP. Для идентификации потоков в заголовок пакета помещается специальный идентификатор. Прежде назывался *IPng (IP next generation).* **Протокол IPX для распределенной сети (IPX wide-area network IPXWAN).** Протокол, согласующий параметры сквозной передачи данных для новых каналов. При включении нового канала первыми посылаются пакеты IPXWAN для согласования параметров этого канала. После их успешного прохождения начинается обычная передача данных по протоколу IPX. Описан в RFC 1362.

Протокол X.25. ITU-T-стандарт, определяющий способ поддержка соединений между DTE и OCE для удаленного терминального доступа и компьютерных коммуникаций в открытых сетях передачи данных. В настоящее время заменен протоколом ретрансляции фреймов (Frame Relay).

Протокол аутентификации паролем (Password Authentication Protocol, PAP). Протокол проверки подлинности, который позволяет устройствам одного ранга распознать друг друга. От удаленного маршрутизатора, который пытается подсоединиться к локальному маршрутизатору, требуется, чтобы он послал запрос на проверку подлинности. В отличие от CHAP, PAP передает пароль, имя хоста или имя пользователя в виде открытого текста (т.е. незашифрованным). Сам по себе PAP не предотвращает несанкционированный доступ, но идентифицирует пункт назначения' после этого маршрутизатор или сервер доступа определяет, разрешен ли доступ данному пользователю. PAP поддерживается только на линиях PPP.

Протокол аутентификации с предварительным согласованием вызова (Challenge Handshake Authentication Protocol, CHAP). Средство обеспечения безопасности, которое предотвращает несанкционированный доступ за счет использования инкапсуляции PPP. Сам по себе CHAP не предотвращает несанкционированный доступ, но указывает удаленный пункт назначения; после этого маршрутизатор или сервер доступа определяет, разрешен ли доступ данному пользователю.

Протокол выбора первого кратчайшего пути (Open Shortest Part First, OSPF) Иерархический маршрутизирующий протокол состояния канала связи, предложенный в качестве замены RIP в Internet сообществе. Функции OSPF включают уменьшение маршрутизационных затрат, маршрутизацию с несколькими путями и балансировку нагрузки. **Протокол динамического конфигурирования хоста (Dynamic Host Configuration Protocol, DHCP).** Обеспечивает механизм динамического распределения и повторного использования освобождаемых IP-адресов.

Протокол доставки дейтаграмм (Datagram Delivery Protocol DDP). Протокол сетевого уровня AppleTalk, который отвечает за доставку дейтаграмм между сокетами в сетях AppleTalk.

Протокол доступа к D-каналу (Link Access Procedure on the D channel, LAPD). В сетях ISDN протокол канального уровня для D-канала. LAPD получен из LAPB и разработан, в основном, для удовлетворения требований сигнгнализации основного доступа ISDN. Определяется в соответствии с Рекомендациями ITU-T (International Telecommunications Union, Международный телекоммуникационный союз) Q.920 и Q.921.

Протокол информации о зоне (Zone Information Protocol, ZIP). Протокол сеансового уровня для сетей AppleTalk, выполняющий взаимное преобразование номеров сетей и имен зон. NBP определяет с помощью ZIP, какие сети содержат узлы, принадлежащие зоне.

Протокол логического канала (logical link protocol, LLC). Верхний из двух подуровней канального уровня, определенных IEEE. Подуровень LLC выполняет контроль ошибок, управле-

ние потоком, создание фреймов и адресацию MAC-подуровня. Наиболее часто используется LLC-протокол IEEE 802.2, который существует в двух вариантах: с установлением соединения и без него.

Протокол маршрутизации AppleTalk на базе обновлений (AppleTalk Update-Based Routing Protocol, AURP). Метод инкапсуляции трафика AppleTalk в заголовке внешнего протокола, обеспечивающий соединение двух и более несмежных сетей AppleTalk через сеть другого типа (например, на базе TCP/IP) с образованием глобальной сети Apple-Talk. Такое подключение называется AURP-туннелем. Кроме инкапсуляции, AURP обеспечивает обновление таблиц маршрутизации для всей глобальной сети AppleTalk путем обмена маршрутной информации между внешними маршрутизаторами.

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

Протокол маршрутизации внутреннего шлюза (Interior Gateway Routing Protocol, IGRP).

Разработан корпорацией Cisco для определения проблем связанных с маршрутизацией, в больших гетерогенных сетях.

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

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

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

Протокол межсетевого обмена пакетами (Internetwork Packet Exchange, IPX). Протокол сетевого уровня, созданный фирмой Novell для сетей NetWare и используемый для передачи данных от серверов к рабочим станциям. Протокол IPX аналогичен протоколам IP и XNS.

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

Протокол начальной загрузки (Bootstrap Protocol, BOOTP). Используется сетевым узлом для определения IP-адреса интерфейса Ethernet при начальной загрузке.

Протокол обмена данными между промежуточными системами (Intermediate System-to-Intermediate System, IS-IS). Иерархический протокол маршрутизации OSI, основанный на протоколе DECNet Phase V. Для определения сетевой топологии IS-маршрутизаторы обмениваются маршрутной информацией на основе единственной метрики.

Протокол обратного преобразования адресов (Reverse Address Resolution Protocol, RARP).

Протокол семейства TCP/IP, представляющий собой метод определения IP-адресов по MAC-

адресам.

Протокол обслуживания таблиц маршрутизации (Routing Table Maintenance Protocol, RTMP). Собственный протокол маршрутизации Apple Computer. RTMP устанавливает и обновляет маршрутную информацию, которая необходима дейтаграммам маршрутизации, проходящим по сети AppleTalk от сокета-источника к сокету-приемнику. Используя RTMP, маршрутизаторы динамически обновляют таблицы маршрутизации, внося в них изменения топологии. Предшественником RTMP является RIP. См. также *протокол маршрутизирующей информации.*

Протокол общей управляющей информации (Common Management Information Protocol, CMIP). Стандартный протокол сетевого управления для сетей OSI, стандартизованный ISO для мониторинга и управления неоднородными сетями. См. также *служба общей управляющей информации.*

Протокол объявления служб (Service Advertising Protocol, SAP). IPX-протокол, предоставляющий средства оповещения клиентов о доступных сетевых ресурсах и услугах через серверы и маршрутизаторы.

Протокол пакетного уровня (packet level protocol, PLP). Протокол сетевого уровня в наборе протоколов X.25. Иногда называется X.25 уровня 3 и протоколом X.25. См. также *протокол x. 25.*

Протокол передачи гипертекста (Hypertext Transfer Protocol, HTTP). Протокол, используемый Web-броузерами и Web-серверами для передачи файлов, например текстовых и графических.

Протокол передачи файлов (File Transfer Protocol, FTP). Протокол прикладного уровня, входящий в семейство протоколов TCP/IP, который используется для передачи файлов между машинами сети. Описан в RFC 959.

Протокол пограничного шлюза (Border Gateway Protocol, BGP). Протокол маршрутизации для обмена информацией между доменами. В настоящее время постепенно заменяет внешний шлюзовой протокол (Exterior Gateway Protocol, EGP). Протокол BGP обменивается информацией о достижимости пунктов назначения с другими системами BGP и определяется стандартом RFC 1163.

Протокол последовательного обмена пакетами (Sequenced Packet Exchange, SPX). Надежный, ориентированный на установку соединения протокол, дополняющий услуги по обработке дейтаграмм, предоставляемые протоколами сетевого уровня. Корпорация Novell разработала этот широко используемый транспортный протокол на основе протокола SPP из набора протоколов XNS.

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

Протокол распределенного связующего дерева (Spanning-Tree Protocol). Мостовой протокол, / который использует алгоритм распределенного связующего дерева и тем самым позволяет ' мосту динамически обходить петли в топологии сети путем построения соответствующего дерева. Мосты обмениваются BPDU-сообщениями для нахождения петель, а затем удаляют эти петли, отключая выбранные интерфейсы мостов. Понятие Spanning-Tree Protocol обозначает два одноименных протокола: протокол стандарта IIEE 802.1 и более ранний протокол Digital Equipment Corporation, на котором он основан. Версия IEEE поддерживает домены мостов и позволяет мосту построить беспетельную топологию в расширенной LAN. В целом версия IEEE предпочтительнее, чем разработка Digital.

Протокол резервирования ресурсов (Resource Reservation Protocol, RSVP). Протокол резервирования ресурсов в IP-сети. Приложения, выполняющиеся на конечных IP-системах, могут использовать RSVP для указания другим узлам основных свойств потока пакетов (полоса пропускания, разброс, максимальный размер пакета и т.д.), которые они хотят получить. RSVP зависит от IPv6. Также известен как *Resource Reservation Setup Protocol.* См. также *протокол IP версии 6.*

Протокол ретрансляции фреймов или протокол Frame Relay (Frame Relay). Стандартный промышленный коммутируемый протокол канального уровня, который обслуживает большое количество виртуальных цепей, используя HDLC-инкапсуляцию между соединенными устройствами. **Frame Relay** более эффективен, чем протокол X.25, и рассматривается в качестве его замены.

Протокол синхронизации сетевого времени (Network Time Protocol, NTP). Протокол, основанный на TCP, который гарантирует точную локальную синхронизацию с радио-или атомными часами, размещенными в Internet. NTP может в течение длительного времени синхронизировать часы сетевых рабочих с точностью до миллисекунд.

Протокол служб канального уровня NetWare (NetWare Link Services Protocol, NLSP).

Протокол маршрутизации канального уровня, базирующийся на IS-IS. Cisco-реализация NLSP также включает в себя MIB-переменные, средства перераспределения маршрутизации и SAP-информации между NSLP и другими IPX-протоколами маршрутизации.

Протокол таблиц маршрутизации (Routing Table Protocol, RTP). Протокол маршрутизации VINES, основанный на RIP. Распространяет информацию о топологии сети и позволяет серверам VINES находить соседних клиентов, серверы и маршрутизаторы. В качестве метрики маршрутизации использует величину задержки.

Протокол транзакций AppleTalk (AppleTalk Transaction Protocol, ATP). Протокол транспортного уровня, обеспечивающий транзакции между сокетами без потерь. Эта служба позволяет организовать обмен данными между двумя клиентами-сокетами, при котором один клиент посылает запрос другому клиенту для выполнения определенной задачи и получения отчета о полученных результатах. ATP связывает запрос с откликом, чем обеспечивает гарантированный и надежный обмен парами "запрос-отклик".

Протокол удаленного доступа AppleTalk (AppleTalk Remote Access, ARA). Предоставляет пользователям Macintosh прямой доступ к информации и ресурсам, расположенным на удаленном узле AppleTalk.

Протокол упорядоченной передачи пакетов (Sequenced Packet Protocol, SPP). Обеспечивает надежную передачу пакетов, ориентированную на установку соединения, с контролем потока процессами клиента. Входит в набор протоколов XNS.

Протокол управления каналом (Link Control Protocol, LCP). Протокол, обеспечивающий средства установки, поддержания и окончания соединения типа "точка-точка".

Протокол управления передачей (Transmission Control Protocol, TCP). Ориентированный на соединение протокол транспортного уровня, обеспечивающий надежную дуплексную передачу данных. TCP входит в набор протоколов TCP/IP.

Протокол управления передачей/Шегпе!-протокол (Transmission Control Protocol/Internet Protocol, TCP/IP). Общее название семейства протоколов, разработанных Министерством обороны США в 1970-е гг. для всемирной распределенной сети. Наиболее известные протоколы из этого набора — TCP и IP.

Протоколом передачи пользовательских дейтаграмм (User Datagram Protocol, UDP).

Протокол транспортного уровня, не требующий установки соединения с получателем. Входит в семейство протоколов TCP/IP. UDP является простым протоколом для обмена дейтаграммами без подтверждения или гарантии доставки. Обработка и передача ошибок выполняется другими протоколами. UDP описан в RFC 768.

Прямая, или "плоская", адресация (flat addressing). Схема адресации, в которой не используется логическая иерархическая структура для определения получателя.

Прямое явное уведомление о перегрузке (Forward Explicit Congestion Notification, FECN). Бит, устанавливаемый во фреймах протокола Frame Relay для уведомления DTE-устройств, получающих фреймы, о перегрузке участка сети между источником и получателем. DTE-устройства, получающие фреймы с установленным FECN-битом могут потребовать, чтобы протоколы высшего уровня предприняли соответствующие действия по управлению потоком данных.

P

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

Разделение нагрузки (load sharing). Использование двух или более путей для отправки пакетов к одному и тому же пункту назначения; при этом, за счет равномерного распределения нагрузки балансируется работа сети и повышается ее эффективность.

Размер окна (window size). Количество сообщений, которые могут быть переданы за время ожидания подтверждения.

Распределение нагрузки (load balancing). Способность маршрутизатора распределять трафик по всем сетевым портам, которые находятся на одинаковом расстоянии от адреса приемника. В хороших алгоритмах распределения нагрузки используется информация о пропускной способности и надежности каналов. Распределение нагрузки повышает интенсивность использования сетевых сегментов, а следовательно, и эффективную пропускную способность сети в целом.

Распределенная сеть (wide-area network, WAN). Сеть передачи данных, охватывающая значительное географическое пространство. Часто использует передающие устройства, предоставленные общими поставщиками каналов связи. В качестве примеров технологий распределенных сетей можно назвать Frame Relay, SMDS и X.25.

Распределенное связующее дерево (spanning tree). Нециклическая часть сетевой топологии 2-го уровня.

Распределенный интерфейс передачи данных по волоконно-оптическим каналам (Fiber Distributed Data Interface, FDDI). Стандарт LAN, определенный в ANSI X3T9.5 для сети с эстафетным доступом и пропускной способностью 100 Мбит/с с использованием волоконно-оптического кабеля длиной не более 2 км. FDDI использует архитектуру двойного кольца для обеспечения избыточности. Ср. с *распределенный интерфейс передачи данных по проводным каналам* и *FDDI II.*

Распределенный интерфейс передачи данных по проводным каналам (Copper Distributed Data Interface, CDDI). Реализация протокола FDDI для экранированной и неэкранированной

витой пары. CDDI применяется для передачи данных на сравнительно короткие расстояния (около 100 метров), обеспечивая скорость передачи до 100 Мбит/с на основе архитектуры сдвоенного кольца для обеспечения избыточности. Основан на стандарте ANSI TPPMD. Ср. *с распределенным интерфейсом передачи данных по волоконно-оптическим каналам (FDDI).*

Расширенный пользовательский интерфейс NetBIOS (NetBIOS Extended User Interface, NetBEUI). Расширенная версия протокола NetBIOS, используемая такими сетевыми операционными системами, как LAN Manager, LAN Server, Windows for Workgroups и Windows NT. NetBEUI формализует транспортный фрейм и создает дополнительные функции. NetBEUI реализует протокол OSI LLC2.

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

Расширенный список управления доступом (extended access control list, Extended ACL).

Список управления доступом, проверяющий адреса отправителя и получателя.

Расширяемость (scalability). Способность сети к увеличению своих размеров без каких-либо существенных изменений общего устройства.

Расщепление горизонта (split horizon). Свойство протокола IGRP, имеющее целью не допустить выбора маршрутизаторами ошибочных путей. Расщепление горизонта предотвращает образование петель между соседними маршрутизаторами и уменьшает количество сообщений об изменениях.

Региональная вычислительная сеть (metropolitan-area network, MAN). Сеть, которая покрывает некоторую территорию. Обычно для MAN эта территория больше, чем для LAN, но меньше, чем для WAN.

Региональное отделение компании Bell (Regional Bell operating company, RBOC). Местная или региональная телефонная компания, которая владеет и осуществляет управление телефонными линиями и коммутаторами в одном из семи регионов США. Эти компании были созданы при ликвидации компании AT&T.

Режим асинхронной передачи (Asynchronous Transfer Mode, ATM). Международный стандарт ретрансляции ячеек, в котором множество типов данных (таких как голосовые, видео и другие) передаются в ячейках фиксированной длины (53 байта). Фиксированная длина ячеек позволяет выполнять их обработку на аппаратном уровне, уменьшая, таким образом, задержки передачи. ATM разрабатывался в расчете на использование преимуществ высокоскоростных передающих сред, таких как E3, SONET и T3.

Резервирование полосы пропускания (bandwidth reservation). Выделение полосы пропускания для пользователей и приложений, обслуживаемых сетью. При этом разным видам трафика присваиваются разные приоритеты в зависимости от их важности и чувствительности к задержкам. Это позволяет наилучшим образом использовать доступную полосу пропускания. Например, при значительной перегрузке сети передача трафика с самым низким приоритетом может быть прекращена. Иногда этот процесс называется выделением полосы пропускания (bandwidth allocation).

C

Самотестирование при включении питания (power-on self-test, POST). Набор диагностических средств, которые проверяют функционирование аппаратуры при включении питания.

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

Сбалансированный протокол доступа к каналу (Link Access Procedure, Balanced, LAPB).

Протокол канального уровня в стеке протокола X.25. LAP B является бит-ориентированным протоколом, разработанным на базе протокола HDLC.

Сбалансированный протокол доступа к каналу связи (Link Access Procedure, Balanced, LAPB). Протокол канального уровня в семействе протоколов X.25. LAPB — бит-ориентированный протокол, являющийся частью протокола HDLC.

Сборка (reassembly). Процесс сборки IP-дейтаграммы, разделенной на фрагменты узлом-источником или промежуточным узлом, в исходное состояние на устройстве-приемнике. См. также *фрагментация.*

Сеанс (session). 1. Взаимосвязанный набор коммуникационных транзакций между двумя и более сетевыми устройствами. 2. В SNA — логическое соединение для обмена данными между двумя NAU.

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

Сегмент, (segment). Участок сети, ограниченный мостами, маршрутизаторами или коммутаторами.

Сегментация (segmentation). Процесс разделения коллизионного домена на два или более доменов с целью уменьшения конфликтов и перегрузки сети. **Сектор стандартизации при международном телекоммуникационном союзе (International Telecommunication Union Telecommunication Standardization Sector, ITU-T).** Международная организация, утверждающая всемирные стандарты в области телекоммуникационных технологий. Ранее функции ITU-T выполнял комитет CCITT. См. также *Международный консультативный комитет по телефонии и телеграфии.* **Сервер (server).** Узел или программа, предоставляющие услуги клиентам.

Сервер имен (name server). Специализированный сервер, выполняющий преобразование сетевых имен в сетевые адреса.

Сервер предприятия (enterprise server). Сервер, обслуживающий всех **пользователей в** сети, предоставляя им различные службы, такие как *электронная почта (e-mail)* или *служба доменных имен (DNS).*

Сервер рабочей группы (workgroup server). Сервер, обслуживающий определенную группу (или группы) пользователей, и предоставляющий им такие службы, как текстовый процессор или совместный доступ к файлам, то есть службы, который могут понадобиться только некоторым группам пользователей.

Сетевая базовая система ввода-вывода (Network Basic Input/Output System, NetBIOS).

Стандартный сетевой API-интерфейс, используемый в локальных сетях IBM для запроса у низкоуровневых сетевых процессов таких служб, как установка и разрыв сеанса, а также передача информации.

Сетевая нагрузка 1-го типа (network termination type 1, NT1). Устройство, соединяющее че-

тырех проводного абонента и стандартное двухпроводное устройство местной линии.

Сетевая нагрузка 2-го типа (network termination type 2, NT2). Устройство, направляющее поток данных между разными абонентскими устройствами и NT1. NT2 является интеллектуальным устройством, которое осуществляет коммутацию и концентрацию.

Сетевая операционная система (Network Operating System, NOS). Операционная система, используемая для обеспечения работы сетей, таких, например, как Novell NetWare или Windows NT.

Сетевая плата (network interface card, NIC). Плата, обеспечивающая коммуникационные возможности компьютерных систем. Называется также *адаптером*.

Сетевая файловая система (Network File System, NFS). Широко распространенный набор протоколов распределенной файловой системы, созданный Sun Microsystems, для удаленного доступа к файлам по сети. В этот набор входит одноименный протокол NFS, а также протоколы RFC, XDR и др. Они являются частью более широкой архитектуры, которую Sun называет ONC.

Сетевое управление (network management). Общий термин, используемый для описания систем и действий по поддержанию работоспособности, диагностике и разрешению проблем в сети.

Сетевой администратор (network administrator). Человек, управляющий сетью и отвечающий за ее нормальную работу.

Сетевой адрес (network address). Адрес сетевого уровня, определяющий логическое, а не физическое сетевое устройство. Также называется *адресом протокола (protocol address).*

Сетевой анализатор (network analyzer). Устройство или программа, предоставляющее разные средства разрешения сетевых проблем, включая коды дешифровки пакетов специфических протоколов, специальные перепрограммируемые тесты идентификации сетевых проблем, фильтрацию и передачу пакетов.

Сетевой интерфейс (network interface). Граница между сетью-носителем и подключенным к ней устройством.

Сетевой информационный центр (Network Information Center, NIC). Организация, функции которой определяются InterNIC. См. InterNIC.

Сетевой коммутатор или просто коммутатор (LAN **switch).** Коммутатор локальной сети. Высокоскоростной коммутатор, перенаправляющий пакеты между сегментами сети. Большинство коммутаторов локальной сети передают поток данных на основе MAC-адресов. Коммутаторы локальных сетей подразделяются на категории, в соответствии с методом коммутации: с буферизацией или без буферизации пакетов. Пример коммутатора локальной сети — Cisco Catalyst 5000.

Сетевой номер (network number). Часть IP-адреса, которая указывает, какой сети принадлежит данный хост.

Сетевой порядок байтов (network byte order). Стандартный для Internet порядок байтов, соответствующий числовым значениям.

Сетевой уровень (network layer). Третий уровень эталонной модели OSI. Уровень, на котором происходит маршрутизация. Обеспечивает соединение и выбор пути между двумя конечными системами. Примерно соответствует уровню контроля пути в модели SNA.

Сетка (mesh). Сетевая топология, в которой устройства организованы управляемым и сегмен-

тированным образом, часто с большим количеством избыточных стратегических взаимосвязей между сетевыми узлами.

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

Сеть предприятия (enterprise network). Сеть предприятия, агентства, школы или другой организации, объединяющая их данные, коммуникации, вычислительные мощности и файловые серверы.

Сеть провайдера (carrier network). Сеть провайдера услуг, по которой выполняется передача данных пользователей.

Сигнал отрицательного подтверждения приема (negative acknowledgment, NAC). Отклик, посланный устройством-приемником устройству-передатчику с уведомлением о том, что полученная информация содержит ошибки.

Сигнализация (signaling). В контексте ISDN — процесс установки соединения (инициализации вызова). Используется для обозначения установки соединения, разрыва соединения, передаваемой информации и различных сообщений, включающих в себя установку, подключение, освобождение линии, пользовательскую информацию, отмену соединения, состояние соединения и отключение.

Сигнальная земля (signal reference ground). Соединительная точка, используемая вычислительными устройствами для измерения и сравнения поступающих входных цифровых сигналов.

Сигнальная система 7 (Signaling System 7, SS7). Стандартная система сигнализации, разработанная корпорацией Bellcore. Она использует управляющие телефонные сообщения и сигналы при вызове пункта назначения.

Симплексная передача (simplex). Однонаправленная передача данных между станцией-источником и станцией-приемником. Примером симплексной технологии является широковещательное телевидение (Ср. с *дуплексной* и *полудуплексной* передачей).

Синхронный канал (synchronous circuit). Канал, по которому сигналы передаются с точным учетом времени. Такие сигналы имеют одну и ту же частоту. При синхронной передаче отдельные символы инкапсулируются в управляющие биты (называемые битами начала и остановки), которые указывают на начало и конец каждого символа.

Система доменных имен (Domain Name System, DNS). Система, используемая в Internet для преобразования имен сетевых узлов в сетевые адреса.

Система управления доступом к контроллеру терминального доступа (Terminal Access Controller Access Control System, TACACS). Протокол аутентификации, разработанный сообществом DNN, который обеспечивает аутентификацию при удаленном доступе и связанные с ней службы, такие как регистрация событий. Пароли пользователей хранятся не в отдельных маршрутизаторах, а в центральной базе данных, что обеспечивает хорошо масштабируемую систему сетевой безопасности.

Система управления сетью (network management system, NMS). Система, отвечающая за управление сетью или ее частью. Это обычно достаточно мощный и хорошо оснащенный компьютер, например инженерная рабочая станция. NMS-система взаимодействует с агентами для оказания помощи в сборе статистики для сети и отдельных ресурсов.

Системная сетевая архитектура (System Network Architecture, SNA). Архитектура крупных, сложных, многофункциональных сетей, разработанная IBM в 1970-х гг. В некотором отношении подобна эталонной модели OSI, но имеет ряд отличий. SNA состоит из семи основных уровней.

Системы сетей Xerox (Xerox Network Systems, XNS). Набор протоколов, первоначально спроектированный PARC. Многие компании, подключающие персональные компьютеры к сети, такие как 3Com, Banyan, Novell и UB Networks использовали или в настоящее время используют вариации XNS в качестве основного транспортного протокола.

Скользящее окно (sliding window). Окно, размер которого согласовывается динамически во время TCP-сеанса.

Скорость локального доступа (скорость порта) (local access rate). Скорость установки соединения (локального ответвления) со средой протокола передачи фреймов. Она характеризует скорость поступления данных в сеть и получения данных из нее.

Служба общей управляющей информации (Common Management Information Service, CMIS).

Служба сетевого управления для сетей OSI, стандартизованная ISO для мониторинга и управления неоднородными сетями. См. также *протокол общей управляющей информации*.

Смежность (adjacency). Отношение, устанавливаемое между избранными соседними маршрутизаторами и конечными узлами для обмена маршрутной информацией. В основе смежности лежит общий сегмент сетевой среды.

Совет по архитектуре Internet (Internet Architecture Board, IAB). Техническая группа, которая отвечает за развитие архитектуры Internet и состоит из таких групп, как IANA, IESG и IRSG. IAB назначается ISOC.

Согласованная скорость передачи информации (committed information rate, CIR). Скорость передачи данных, измеряемая в битах в секунду, с которой протокол передачи фреймов соглашается передавать данные.

Соединительная точка (reference point). Спецификация, которая определяет соединения между специфическими устройствами в зависимости от их функций в непосредственном соединении.

Сокет (socket). 1. Программная структура, которая при обмене данными с сетевым устройством играет роль конечной точки. 2. Адресуемый объект, узел которого подключен к сети AppleTalk; сокеты принадлежат программным процессам, называемым клиентами сокетов. Сокеты AppleTalk делятся на две группы: SAS, зарезервированные для таких клиентов, как протоколы дара AppleTalk, и DAS, назначаемые DDP динамически по запросу клиентов в узле. По принципу действия сокет AppleTalk подобен порту TCP/IP.

Сообщение (message). Логическая группа информации уровня приложений (уровень 7), часто состоящая из нескольких низкоуровневых групп — пакетов. Для описания логических групп информации на разных уровнях модели OSI и в разных технологических циклах также используются термины *дейтаграмма*, *кадр*, *пакет* и *сегмент*.

Сообщение об активности (keepalive). Сообщение, посылаемое одним сетевым устройством другому устройству о том, что виртуальный канал между ними остается в активном состоянии.

Сообщество Internet (Internet Society, ISOC). Международное некоммерческое профессиональное объединение, основанное в 1992 г., которое координирует развитие и эволюцию Internet. Кроме того, ISOC делегирует полномочия другим группам, связанным с Internet, на-

пример IAB. Штаб-квартира ISOC находится в Рестоне, штат Виргиния (Reston, Virginia).

Соседние маршрутизаторы (neighboring routers). В OSPF — это два маршрутизатора, обладающие интерфейсами с общей сетью. В сетях с множественным доступом соседние маршрутизаторы динамически обнаруживаются протоколом приветствия OSPF.

Спаренные кольца со встречной циркуляцией (Dual counter-rotating rings). Сетевая топология с двумя противоположными путями прохождения сигнала в сети с эстафетной передачей маркера. Эта топология лежит в основе сетей FDDI и CDDI.

Список контроля доступа (access control list, ACL). Список, сохраняемый маршрутизатором Cisco, для управления доступом ряда служб к маршрутизатору или с него (например, для предотвращения отправки пакетов с некоторым адресом с указанного интерфейса маршрутизатора).

Спуфинг (spoofing). 1. Схема, используемая маршрутизаторами для того, чтобы хост обслуживал интерфейс, как если бы он (маршрутизатор) был активен и поддерживал сеанс. Маршрутизатор посылает хосту "дезинформирующие" ответы, чтобы последний продолжал посылать сообщения и считал, что сеанс все еще существует. Спуфинг удобно использовать в среде маршрутизации типа DDR, в которой при отсутствии трафика коммутируемый канал закрывается, в целях сокращения затрат на передачу. 2. Состояние, когда в пакете значится ложный адрес отправителя. Спуфинг позволяет обойти механизмы сетевой безопасности, такие как фильтры и списки доступа.

Стандарт (standard). Набор правил или процедур, которые либо широко используются, либо утверждены официально.

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

Стандартный список управления доступом (standard access control list, standard ACL). Список управления доступом, осуществляющий фильтрацию на основе адреса источника и шаблон маски. Стандартные списки управления доступом разрешают или запрещают доступ всему набору протоколов TCP/IP.

Станция с двойным подключением (dual-homed station). Сетевая топология, в которой устройство подключается к сети с помощью двух независимых точек доступа (points of attachment). Одна из них является первичным подключением, а другая — резервным, которое активируется в случае сбоя первичного подключения.

Станция с простым подключением (Single Attachment Station, SAS). 1. Устройство, подключенное только к первичному кольцу FDDI. 2. Также известна как станция B-класса.

Статическая виртуальная сеть (static VLAN). Виртуальная сеть, в которой конфигурация портов коммутатора не изменяется.

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

Стек протоколов (protocol stack). Набор связанных коммуникационных протоколов, которые функционируют совместно и направляют данные на некоторые или на все семь уровней эталонной модели OS1. Не все протоколы стека охватывают все уровни модели. Часто один протокол стека соответствует сразу нескольким уровням. Типичным примером стека протоколов является TCP/IP.

Структура информации для управления сетью (Structure of Management Information, SMI). Документ (RFC 1155), определяющий правила управления объектами в MIB. См. также *база управляющей информации.*

Суммирование маршрутов (route summarization). Объединение объявленных адресов в OSPF и IS-IS. В OSPF это приводит к объявлению пограничным маршрутизатором зоны единого суммарного маршрута к другим зонам.

Таблица маршрутизации (routing table). Таблица, хранящаяся в маршрутизаторе или другом сетевом устройстве, которая содержит маршруты к определенным пунктам назначения в сети и, в некоторых случаях, метрики, связанные с этими маршрутами.

Таймаут (timeout). Событие, которое происходит, когда одно устройство в сети ожидает сообщения от другого устройства в заданное время, но не получает его. Из-за тай-маута обычно приходится заново посылать информацию или прерывать сеанс связи между устройствами.

Такт задержки (tick). Задержка в канале данных, осуществляемая с использованием периода срабатывания таймера (встроенного в персональные компьютеры). Равна примерно 55 миллисекундам. Точное значение 1/18 секунды.

Телефонная станция (центральный офис) (Central Office, CO). Офис местной телефонной компании, к которому подсоединены все местные линии и в котором происходит коммутация каналов абонентских линий.

Терминальное оборудование 1-го типа (terminal equipment type 1, TE1). Устройство, совместимое с ISDN-сетью. TE1 подключается к сетевой нагрузке 1-го, либо 2-го типа.

Терминальное оборудование 2-го типа (terminal equipment type 2, TE2). Устройство, не совместимое с ISDN-сетью и требующее использования терминального адаптера.

Терминальный адаптер (terminal adapter, TA). Устройство, используемое для подключения BRI-соединений службы ISDN к существующим интерфейсам, таким как EIA/TIA-232. Как правило, терминальный адаптер представляет собой ISDN-модем.

Технология объединенных сетей (internetworking). Общий термин, используемый для обозначения индустрии, связанной с организацией межсетевых **соединений. Относится к** продуктам, процедурам и технологиям.

Топология (topology). Физическое расположение узлов сети и передающей среды внутри предприятия.

Топология типа "звезда", звездообразная топология (star topology). Топология локальных сетей, в которой оконечные точки соединены с общим центральным коммутатором посредством связей типа "точка-точка". *Кольцевая топология (ring topology),* организованная как "звезда", вместо связей "точка-точка" использует однонаправленный замкнутый шлейф.

Точечная десятичная форма записи (dotted-decimal notation). Синтаксическое представление 32-х разрядных адресов в виде четырех 8-разрядных целых чисел, записанных в десятичном формате и разделенных точками. Используется для представления IP-адресов в удобном для восприятия виде, например 192. 67. 67 .20.

Точка доступа к службе (service access point). Поле, определенное спецификацией IEEE, являющееся частью адресной спецификации.

Точка доступа к службе отправителя (source service access point, SSAP). SAP сетевого узла, указанная в поле отправителя пакета.

Точка доступа к службе получателя (destination service access point, DSAP). Точка доступа к службе (SAP) сетевого узла, указанного в поле приемника пакета. Ср. с *точкой доступа к службе отправителя.*

Точка присутствия (point of presence, POP). Точка соединения коммуникационных устройств, предоставляемых телефонной компанией с главным распределительным центром здания.

Трансляция сетевых адресов (network address translation, NAT). Механизм, позволяющий сократить потребность в глобально уникальных IP-адресах. Позволяет подключаться к Internet организации с локально уникальными адресами путем трансляции этих адресов в глобально маршрутизируемое адресное пространство.

Транспортный протокол реального времени (Real-time Transport Protocol, RTP). Обычно используется в IP-сетях. RTP разработан для сквозной передачи по сети данных реального времени, таких как аудио, видео или данные моделирования, посредством сетевых служб широковещательной или однонаправленной передачи. RTP обеспечивает для приложений реального времени реализацию таких служб, как идентификация типа полезной нагрузки, порядковая нумерация пакетов данных, организация временных меток и мониторинг доставки данных.

Транспортный уровень (Transport layer). Четвертый уровень эталонной модели OSI. Сегментирует и преобразует данные в один поток. Транспортный уровень может гарантировать надежность соединения путем реализации надежного транспортного механизма.

Туннелирование (tunneling). Архитектура, предназначенная для предоставления служб, необходимых для реализации любых стандартных схем инкапсуляции типа "точка-точка".

Тупиковая зона (stub area). Область OSPF, через которую проходит стандартный, внутризонные и межзонные, но не внешние маршруты. Через шлейфную зону нельзя прокладывать виртуальные каналы, шлейфные **зоны** не содержат ASBR. Ср. с *нетупиковая зона.*

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

У

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

Удаленный вызов процедур (remote-procedure call, RFC). Технологическая основа клиент-серверных вычислений. RPC — это вызов процедур, которые разрабатываются или определяются клиентами, выполняются на серверах, а результаты возвращаются по сети клиентам.

Удаленный мониторинг (remote monitoring, RMON). Спецификация MIB-агента, описанная в RFC 1271, которая определяет функции удаленного мониторинга сетевых устройств. Спецификация RMON предоставляет многочисленные возможности для мониторинга, определения неисправностей и отчетности.

Удержание (holddown). Свойство протокола IGRP отвергать все маршруты с одним и тем же пунктом назначения в течение некоторого периода времени.

Узел (node). Конечная точка сетевого соединения. Общая точка двух или более линий в сети.

Узлами могут быть процессоры, диспетчеры или рабочие станции. Узлы, в зависимости от маршрутизации или других функциональных возможностей, соединяются каналами и служат контрольными точками в сети. Термин "узел" иногда обозначает устройство, имеющее доступ в сеть. Слова "узел" и "устройство" взаимозаменяемы.

Уникальный идентификатор организации (organizational unique identifier, OUI). 3 октета, которые IEEE присваивает блоку 48-разрадных адресов локальной сети.

Управление безопасностью (security management). См. *управление неисправностями.*

Управление доступом к передающей среде (Media Access Control, MAC). Часть стандарта канального уровня, включающая шести байтовые (48-битовые) адреса отправителя и получателя, а также способ получения разрешения на передачу информации по сети. См. также *канальный уровень* и *протокол логического канала.*

Управление конфигурацией (configuration management). См. *управление неисправностями.*

Управление неисправностями (fault management). Одна из пяти категорий сетевого управления, предусмотренных в стандарте ISO для управления сетями OSI. Предназначается для обнаружения и управления неисправностями в сети. Существует также *управление учетными записями (accounting management), управление конфигурацией (configuration management), управление производительностью (performance management)* и *управление безопасностью (security management).*

Управление перспективного планирования научно-исследовательских работ при Министерстве обороны США (Defense Advanced Research Projects Agency, DARPA). Государственное агентство при Министерстве обороны США, которое финансировало исследовательские и экспериментальные работы по созданию Internet. Оно основало сеть ARPANET, которая в 1994 г. стала называться ARPA. См. также *АКРА*.

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

Управление потоком методом скользящего окна (sliding window flow control). Метод управления потоком, при котором приемник дает передатчику разрешение на передачу данных до заполнения окна. Когда окно заполняется, передатчик прекращает передачу до тех пор, пока приемник не объявит о расширении окна. Этот метод управления потоком используется в TCP и других транспортных протоколах, а также в некоторых протоколах канального уровня.

Управление производительностью (performance management). См. *управление неисправностями.*

Управление синхронным каналом данных (Synchronous Data Link Control, SDLC). SNA-протокол канального уровня коммуникации. SDLC является бит-ориентированным, дуплексным последовательным протоколом, ставшим основой для создания многих аналогичных протоколов, включая протоколы HDLC и LAPB.

Управление трафиком (traffic management). Средства предупреждения перегрузок, а также формирования и упорядочения трафика. Обеспечивают высокую эффективность работы каналов путем замедления передачи при перегрузке трафика с низким приоритетом, допускающего задержки.

Управление учетными записями (accounting management). См. *управление неисправностями.*

Уровень доступа (access layer). Уровень, на котором локальная сеть или группа таких сетей, обычно Ethernet или Token Ring, предоставляет пользователям непосредственный доступ к сетевым службам.

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

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

Уровень распределения (distribution layer). Уровень, на котором происходит распределение сетевых служб для отдельных локальных сетей, входящих в распределенную сеть. На этом уровне обычно находится магистраль распределенной сети. Обычно основывается на Fast Ethernet.

Уровень служб представлений (presentation services layer). Уровень 6 архитектурной модели SNA. Обеспечивает управление сетевыми ресурсами, обслуживание сеансов представлений и некоторое управление приложениями. **Приблизительно** соответствует уровню представлений модели **OS1.**

Уровень транзакций (transaction services layer). Уровень 7 в архитектурной модели SNA. Представляет функции пользовательских приложений, таких как электронные таблицы, текстовые редакторы или электронная почта, посредством которых пользователи взаимодействуют с сетью. Соответствует уровню приложений OSI.

Уровень управления маршрутом (path control layer). Уровень 3 архитектурной модели SNA. На этом уровне выполняется ряд последовательных действий, связанных с перекомпоновкой данных. Кроме того, уровень управления маршрутом обеспечивает маршрутизацию. Примерно соответствует сетевому уровню модели OSI.

Уровень управления передачей (transmission control layer). Уровень 4 архитектурной модели SNA. Отвечает за установку, поддержку и разрыв сеансов SNA, упорядочение сообщений и управление уровнем потока сеанса. Соответствует транспортному уровню модели OSI.

Уровень управления потоком данных (data flow control layer). Пятый уровень модели SNA. Определяет взаимодействие между партнерами сеанса, в частности, потоком данных, и управляет им. Соответствует сеансовому уровню в модели OSI.

Усовершенствованная одноранговая сеть (Advanced Peer-to-Peer Networking, APPN). Улучшенная версия первоначальной архитектуры IBM SNA. APPN управляет установкой сеанса между равноправными (одноранговыми) узлами, вычислением динамически прозрачного маршрута, а также заданием приоритета для потока данных протокола APPC.

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

Учрежденческая АТС (автоматическая телефонная станция) (private branch exchange, PBX).

Цифровой или аналоговый коммутационный узел, находящийся на территории абонента и соединяющий частную телефонную сеть абонента с общедоступными сетями.

Ф

Файловый протокол AppleTalk (AppleTalk Filing Protocol, AFP). Протокол уровня представлений, позволяющий пользователям совместно использовать файлы данных и прикладные программы, которые находятся на файловом сервере. AFP поддерживает AppleShare и Mac OS File Sharing.

Физическая передающая среда (Media, physical media). Употребляется как в единственном — **medium,** так и во множественном числе — **media** Типичными сетевыми передающими средами являются: витая пара, коаксиальный или волоконно-оптический кабель, электромагнитные волны (для СВЧ, лазерной и инфракрасной передачи данных). Иногда также называется *физической средой (physical media).*

Физический управляющий уровень (physical control layer). Уровень 1 в архитектурной модели SNA. Отвечает за спецификацию физических каналов между конечными системами. Соответствует физическому уровню модели OSI.

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

Фильтр (filter). Обычно процесс или устройство, которое определяет, передавать или не передавать поток данных дальше на основе заданных критериев, таких как адреса отправителя и получателя, тип протокола и др.

Флэш-память (flash memory). Энергонезависимое запоминающее устройство, содержимое которого стирается и перепрограммируется по мере необходимости Флэш-память разработана компанией Intel и лицензирована для использования другими производителями полупроводниковых приборов.

Форум ATM (ATM forum). Международная организация, основанная в 1991 г. Cisco Systems, NET/ADAPTIVE, Northern Telecom и Sprint для разработки и внедрения стандартов в области ATM-технологий. ATM Forum развивает официальные стандарты ANSI и ITU-T, а также создает соглашения о внедрении еще до появления официальных стандартов.

Фрагмент (fragment). Составная часть большого пакета, который разбит на части меньшего размера.

Фрагментация (fragmentation). Процесс разделения пакета на части меньшего размера для передачи по сети, для которой исходный размер пакета слишком велик. См. также *сборка.*

Фрейм (frame). Логически сгруппированная информация, посылаемая через передающую среду в виде блока данных канального уровня. Этот термин часто используется по отношению к заголовку и трейлеру, окружающим данные пользователя, содержащиеся в блоке, и используемым для синхронизации и определения ошибок. Термины *дейтаграмма, сообщение, пакет* и *сегмент (datagram, message, packet, segment)* также используются для описания логически сгруп-

пированных блоков информации на разных уровнях эталонной модели OSI и в различных технологических циклах.

Функциональная совместимость (interoperability). Возможность успешного сетевого взаимодействия программных и аппаратных изделий разных разработчиков.

Х-Ц-Ч

Хост (host). Обычно это компьютерная система, подключенная к сети. Хост аналогичен узлу (node), за исключением того, что хостом обычно называют компьютер, а узлом — любое сетевое устройство, включая серверы доступа и маршрутизаторы. См. также *узел.*

Цифровая сеть интегрированных служб (Integrated Services Digital Network, ISDN). Коммуникационный протокол, предложенный телефонными компаниями, который позволяет передавать информацию по телефонным сетям, в том числе голосовые данные, а также данные из других источников.

Частично-сеточная топология (partially meshed topology). Топология, в которой не каждое устройство среды Frame Relay имеет PVC с остальными устройствами.

Ш

Шаблон маски (wildcard mask). 32-битовая последовательность, используемая наряду с IP-адресом для определения того, какие биты в IP-адресе следует проигнорировать при сравнении этого адреса с другим IP-адресом. Шаблон маски указывается при установке списка управления доступом.

Шестнадцатеричный (по основанию 16) (hexadecimal (base 16)). Числовое представление, использующее цифры от 1 до 9 в обычном значении и буквы от A до F для представления десятичных чисел от 10 до 15. В шестнадцатеричном представлении самая правая цифра обозначает единицы, следующая — числа, кратные 16, следующая — кратные 16^2=256 и т.д.

Ширина полосы пропускания (bandwidth). Разность между наибольшей и наименьшей возможными частотами, допустимыми для сигнала в сети. Термин также используется для описания пропускной способности сети или протокола.

Широковещательная лавина (broadcast storm). Нежелательная, множественная, широковещательная передача, возникающая одновременно во всех сегментах сети Широковещательная лавина использует всю возможную полосу пропускания и, обычно, вызывает простои сети.

Широковещательный адрес (broadcast address). Специальный адрес, зарезервированный для передачи сообщения всем станциям Вообще говоря, широковещательным адресом называется общий MAC-адрес всех станций. Ср. с *групповым (multicast)* и *индивидуальным (umcast)* адресом.

Широковещательный домен (broadcast domain). Группа устройств, каждое из которых принимает широковещательные фреймы, отправленные с любого узла этой группы. Широковещательные домены, обычно, ограничиваются маршрутизаторами, поскольку маршрутизаторы не пересылают широковещательные фреймы.

Широковещательный пакет (broadcast). Пакет данных, переданный всем узлам в сети. Идентифицируется широковещательными адресами.

Шлюз "последней надежды" или маршрутизатор-склад (gateway of last resort). Маршрутизатор, на который направляются все пакеты, не прошедшие маршрутизацию.

Шлюз (gateway). В IP-сообществе — устаревший термин, которым обозначают маршрутизирующее устройство В настоящее время такие узлы называют маршрутизаторами, а шлюзами называют устройство специального назначения, которое выполняет преобразование информации из одного стека протоколов в другой на уровне приложений. Ср. с *маршрутизатор.*

Э-Я

Экранированная витая пара (shielded twisted pair, STP). Сетевой кабель с двумя парами проводов и экранирующим слоем, снижающим воздействие электромагнитных помех.

Энергонезависимое ОЗУ (nonvolatile RAM, NVRAM). Оперативное запоминающее устройство, содержимое которого сохраняется при отключении питания.

Эталонная модель взаимодействия открытых систем (OSI reference model). Архитектурная модель сети, разработанная ISO и ITU-T. Состоит из семи уровней, каждый из которых определяет конкретную сетевую функцию, такую как адресация, управление потоками данных, контроль ошибок, инкапсуляция и надежная передача сообщений. Самый низкий уровень (физический) наиболее близок к технологии среды передачи данных. Второй нижний уровень используется программным и аппаратным обеспечением, а пять верхних уровней применяются только программным обеспечением. Самый верхний уровень (уровень приложений) ближе всего к пользователю. Эталонная модель OSI находит универсальное использование в качестве методики изучения функционирования сетей. В некоторых отношениях OSI подобна SNA.

Эхо-канал (E channel, echo channel). Коммутируемый ISDN-канал с полосой пропускания 64 Кбит/с. Он определен в спецификации ITU-T ISDN в 1984 году, но был удален из спецификации в 1988 году.

Эхо-протокол AppleTalk (AppIeTalk Echo Protocol, AEP). Применяется для тестирования соединения между двумя узлами AppleTalk. Один узел посылает пакет другому узлу и получает в ответ дубликат (эхо) посланного пакета.

Язык гипертекстовой разметки (Hypertext Markup Language, HTML). Простой язык гипертекстового форматирования, в котором для указания способа отображения (например в Web-броузере) некоторой части документа используются теги.