Федеральное агентство связи
Федеральное государственное образовательное бюджетное учреждение
высшего профессионального образования
«Поволжский государственный университет телекоммуникаций и информатики»

Кафедра ___систем связи_____
(наименование кафедры)

КОНСПЕКТ ЛЕКЦИЙ

ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

Системы и сети пакетной коммутации

(наименование учебной дисциплины)

по специальности (направлению подготовки):
направление 210400 – Телекоммуникации
специальности: 210404 - Многоканальные телекоммуникационные системы
210406 - Сети связи и системы коммутации
210401 - Физика и техника оптической связи
210403 - Защищенные системы связи

090106 – Информационная безопасность телекоммуникационных систем
наименование специальности (направления подготовки)

Самара
2012

УДК 681.3
621.395

Васин Н.Н.

Системы и сети пакетной коммутации. Конспект лекций. – Самара: ФГОБУ ВПО ПГУТИ, 2012. – 283 с.

Рассматриваются принципы построения систем и сетей телекоммуникаций, основные технологии локальных сетей, принципы и средства межсетевого взаимодействия, принципы построения и функционирования глобальных сетей. Описано функционирование и основные характеристики коммутаторов и маршрутизаторов, приводятся примеры конфигурирования устройств их проверки и отладки.

Данное учебное издание рекомендуется Государственным образовательным учреждением высшего профессионального образования «Московский технический университет связи и информатики» к использованию в образовательных учреждениях, реализующих образовательные программы высшего профессионального образования, по дисциплинам «Сети связи», «Системы коммутации», «Сети связи и системы коммутации», «Системы и сети передачи информации на базе коммутаторов и маршрутизаторов» по специальностям 210406 «Сети связи и системы коммутации» и 210404 «Многоканальные телекоммуникационные системы» направления подготовки дипломированных специалистов 210400 «Телекоммуникации» и направлению подготовки бакалавров 210700 «Инфокоммуникационные технологии и системы связи».

Руководитель уполномоченного
Учреждения, выдавшего рецензию А.С. Аджемов

Регистрационный номер рецензии № 1545 от 31.10.2011 г.
(*присвоенный базовой организацией*)

Федеральное государственное образовательное бюджетное учреждение
высшего профессионального образования
«Поволжский государственный университет телекоммуникаций и информатики»

ОГЛАВЛЕНИЕ

Уважаемый читатель!

Книга, которую вы держите в руках, является одним из немногочисленных примеров учебных пособий по сетевым технологиям на русском языке. Это пособие отвечает требованиям времени и подготовлено на основе накопленного автором за многие годы опыта преподавания ИТ дисциплин.

Книга примечательна тем, что материал изложен лаконично, при этом с достаточным вниманием к деталям и без ущерба содержанию. Принципы работы протолов и систем, понятия и определения изложены доступным языком. Отдельного внимания заслуживает терминологический словарь в конце книги, который не столько дает прямой перевод «слово-в-слово», сколько является «толкователем» сути определений, терминов или аббревиатур.

Компания Cisco высоко оценивает вклад автора в развитие системы образования в сфере ИТ и сетевых технологий и рекомендует настоящее издание в качестве учебного пособия студентам российских вузов, обучающихся по программам высшего профессионального образования в области проектирования, построения и обслуживания сетей передачи данных, а также в качестве дополнительного русскоязычного источника информации слушателям, обучающимся по официальным программам Академии Cisco: CCNA Exploration, CCNA Discovery.

Эксперт программы Академий Cisco по вопросам ИТ образования,
Овсянников Семён Васильевич

ПРЕДИСЛОВИЕ

Настоящий курс лекций предназначен для студентов по направлению подготовки дипломированных специалистов 210400 «Телекоммуникации» специальностей 210404 - Многоканальные телекоммуникационные системы, 210406 - Сети связи и системы коммутации, а таже направлению подготовки бакалавров 210700 «Инфокоммуникационные технологии и системы связи».

Он может быть полезен для студентов специальностей 090106 - Информационная безопасность телекоммуникационных систем, 210403 - Защищенные системы связи, а также для слушателей курсов, обучающихся по программе Академии Cisco для получения международного индустриального сертификата CCNA .

Вопросам создания компьютерных сетей посвящен достаточно обстоятельный учебник [1], который выдержал ряд изданий. Однако большой объем учебника затрудняет пользование им студентам и слушателям краткосрочных курсов. Кроме того, в учебнике не рассматриваются вопросы и примеры конфигурирования аппаратных средств сетей связи, что стало актуально в последнее время.

В учебниках [2, 3] излагаются материалы по созданию сетей и систем практически всех видов. Однако вопросы конфигурирования аппаратных средств не рассматриваются, поскольку оборудование, выпускаемое различными фирмами, существенно различается.

При создании сетей передачи данных наиболее широко в настоящее время используются аппаратные средства компании Cisco. Вопросы конфигурирования, отладки и проверки оборудования в таких сетях рассматриваются в учебных руководствах [4, 5], которые являются узкоспециализированными и характеризуются очень большим объемом.

Поэтому возникла необходимость в компактном курсе лекций для обучения студентов технологиям сетей передачи данных. Учебное пособие [6] издано малым тиражом, поэтому предпринята попытка создания курса лекций, в котором отражен переработанный и дополненный материал пособия [7].

Автор выражает благодарность сотрудникам компании Cisco Овсянникову С.В., Разумовскому Д.В., Турилину А.С. за помощь в редактировании терминов и сокращений, встречающихся в курсе лекций.

Об авторе

Васин Николай Николаевич, доктор технических наук, профессор.
Заведующий кафедрой систем связи ФГОБУ ВПО «Поволжский государственный университет телекоммуникаций и информатики».
Инструктор сетевой Академии CISCO (CCNA).
Область научных интересов – обработка измерительных сигналов.

Адрес: 443010, г. Самара, ул. Л. Толстого, дом 23, ПГУТИ, кафедра систем связи, т. (8-846) 332-08-05, 339-11-26.

ВВЕДЕНИЕ

В настоящее время Интернет является глобальной сетью передачи данных на земле, которая создала единое информационное пространство. Интернет состоит из множества больших и малых сетей, а также индивидуальных компьютеров, которые связаны между собой. Основу Интернета составляют IP –технологии.

Современные тенденции развития систем и сетей телекоммуникаций предполагают предоставление разных видов услуг: обмен данными, передача аудио- и видеоинформации по единой мультисервисной сети связи. Для этой цели создаются сети нового поколения Next Generation Network – NGN.

Передача данных по сети Интернет реализуется, главным образом, на базе протокола TCP/IP (Transmission Control Protocol / Internet Protocol – Протокол управления передачей/Межсетевой протокол). TCP/IP – это набор протоколов или правил, которые были развиты, чтобы позволить компьютерам совместно использовать ресурсы сети.

Наиболее распространенным оборудованием в сетях TCP/IP являются коммутаторы и маршрутизаторы фирмы Cisco. Сведения о создании сетей на таком оборудовании, функционировании аппаратуры и конфигурировании разбросаны по многим источникам. Поэтому в настоящем курсе лекций вопросы конфигурирования сетевых устройств рассматриваются на примере оборудования фирмы Cisco, которое используется в Самарском региональном техническом тренинг центре (СРТТЦ), на базе которого функционирует Академия Cisco – учебный центр международного стандарта, и на кафедре систем связи ПГУТИ, где работает автор.

При использовании реального оборудования, например, из 4 маршрутизаторов и 4 коммутаторов группа студентов из 6 – 7 человек вынуждена конфигурировать один маршрутизатор, что снижает эффективность обучения. Для устранения данного недостатка в дополнение к существующему оборудованию используются программные имитаторы функционирования сети. Ранее это был симулятор RouterSim CCNA3.0 [7]. В настоящее время Международная Академия Cisco предоставляет каждому слушателю курсов CCNA симулятор Packet Tracer, имеющий очень широкие возможности по моделированию сети. Конфигурирование маршрутизаторов и коммутаторов с использованием симулятора почти ничем не отличается от

работы с реальным оборудованием. При этом на каждом компьютере с установленным симулятором можно конфигурировать достаточно сложную сеть, включающую несколько маршрутизаторов, коммутаторов и компьютеров, а также некоторые другие сетевые устройства, такие как сетевые серверы, IP телефоны. Данный комплекс позволяет студентам и слушателям локальной академии Cisco полноценно освоить программирование аппаратуры Cisco без риска повредить реальную аппаратуру сетевого комплекса. На реальном же оборудовании проводится закрепление полученных знаний и навыков.

В предлагаемом курсе лекций рассматриваются принципы построения сетей передачи данных, основные технологии локальных сетей, принципы и средства межсетевого взаимодействия, функционирование и основные характеристики коммутаторов и маршрутизаторов, конфигурирование и маршрутизацию сетей и устройств. Теоретический материал закрепляется в ходе проведения лабораторных работ.

Раздел 1. ОСНОВЫ ПОСТРОЕНИЯ СЕТЕЙ

Лекция 1. ОБЩИЕ СВЕДЕНИЯ О СЕТЕВЫХ ТЕХНОЛОГИЯХ

Краткая аннотация лекции: приведены основные элементы и устройства телекоммуникационных сетей, их классификация, описание семиуровневой модели взаимодействия открытых систем.
Цель лекции: изучить основную терминологию сетевых технологий, функции уровней модели OSI.

1.1. Основы сетевых технологий

Телекоммуникационные сети представляют комплекс аппаратных и программных средств, обеспечивающих передачу информационных сообщений между абонентами с заданными параметрами качества. При создании сетей телекоммуникаций невозможно соединить всех абонентов между собой отдельными (выделенными) линиями связи. Это нецелесообразно экономически и невыполнимо практически. Поэтому соединение многочисленных абонентов (А), находящихся на большом расстоянии между собой, обычно производится через транзитные (телекоммуникационные) узлы (ТУ) связи (рис.1.1).

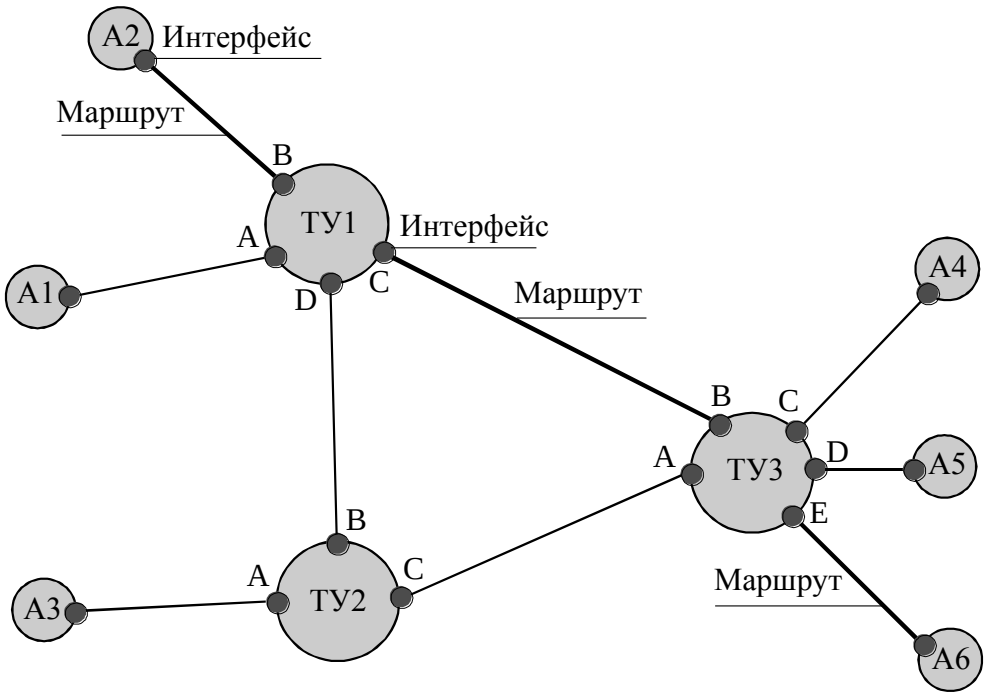


Рис.1.1. Телекоммуникационная сеть

Таким образом, **телекоммуникационная сеть** образуется совокупностью абонентов (А) и узлов связи, соединенных линиями

(каналами) связи. Узлы ТУ производят **коммутацию** поступившего сообщения с входного порта (интерфейса) на выходной. Например, в сети рис. 1.1 при передаче сообщения от абонента А2 абоненту А6 транзитный узел ТУ1 производит коммутацию сообщения с входного интерфейса В на выходной С, транзитный узел ТУ3 – с входного интерфейса В на выходной Е. При этом формируется определенный **маршрут**, по которому передается сообщение. Процесс формирования маршрута, получил название **коммутация**. Коммутацией также называют **передачу (продвижение) сообщения с входного интерфейса на выходной.**

В некоторых сетях все возможные маршруты уже созданы и необходимо только выбрать наиболее оптимальный. Процесс выбора оптимального маршрута получил название **маршрутизация**, а устройство ее реализующее – **маршрутизатор**. Выбор оптимального маршрута узлы производят на основе **таблиц маршрутизации** (или коммутации) с использованием определенного критерия – **метрики.**

Таким образом, различают сети: с **коммутацией каналов,** когда телекоммуникационные узлы выполняют функции коммутаторов, и с **коммутацией пакетов** (**сообщений**), когда телекоммуникационные узлы выполняют функции маршрутизаторов. Различие коммутации пакетов или сообщений состоит в том, что сообщение может быть очень большим. Поэтому, если в нем обнаруживается ошибка, то повторно нужно передавать все сообщение большого объема. В сетях с коммутацией пакетов большое сообщение предварительно разбивается на сравнительно небольшие пакеты (сегменты). Поэтому при потере или искажении части сообщения повторно передается только потерянный пакет (сегмент).

В сетях с коммутацией каналов предварительно устанавливается соединение между абонентами (создается канал связи), затем по созданному каналу передаются сообщения. Поскольку канал связи полностью выделяется паре абонентов, то для него можно задать требуемые параметры и характеристики, обеспечив значения **задержки** и **вариации задержек – джиттера.**

Так как скоммутированный канал связи выделяется в полное распоряжение пары абонентов, то он используется не эффективно. Паузы между словами и, особенно, между фразами могут быть достаточно большими. Коэффициент использования канала обычно оценивают

значением 0,25. В отличие от сетей с коммутацией каналов сети с коммутацией пакетов могут более эффективно использовать свои ресурсы.

Сети с коммутацией пакетов или сообщений (компьютерные сети) первоначально создавались для передачи данных, поэтому значения задержки и джиттер не играли существенной роли.

Сети с коммутацией каналов, когда телекоммуникационные узлы выполняют функции коммутаторов, и сети с коммутацией пакетов на маршрутизаторах характеризуются двумя принципиально различными видами трафика:

потоковым (равномерным), например, трафиком телефонных сетей;

пульсирующим (не равномерным) трафиком компьютерных сетей передачи данных.

При передаче аудио-сигналов телефонных сетей связи трафик будет равномерным (потоковым), как показано на рис.1.2а. Параметры **задержка** и вариация задержек (**джиттер**) должны быть минимальны, чтобы не влиять на качество передаваемой информации.

При передаче компьютерных данных трафик является неравномерным (рис.1.2б), он также называется пульсирующим или эластичным. Передаваемые данные мало чувствительны к задержкам и джиттеру, однако очень чувствительны к потерям и искажениям пакетов. Поэтому наряду со средней скоростью трафика и его пульсацией, необходимо обеспечить **надежность** приема передаваемый пакетов информации.

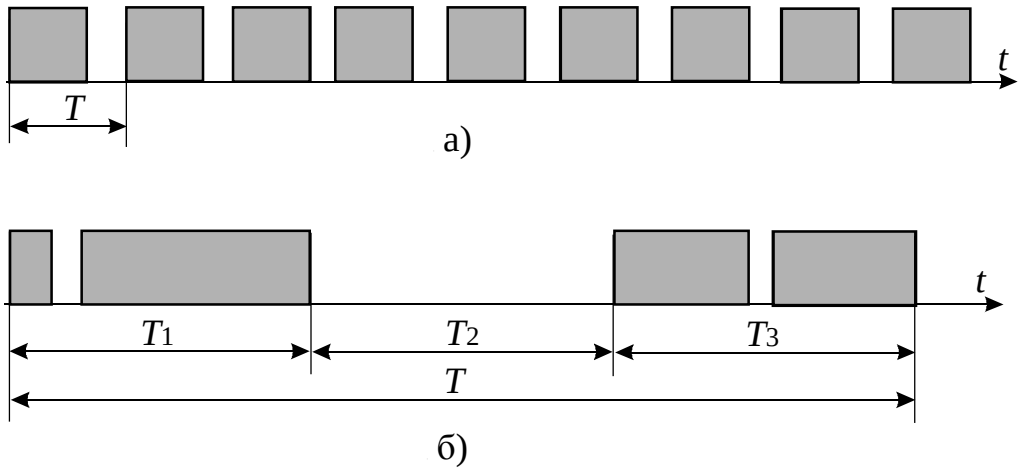


Рис.1.2. Равномерный (а) и неравномерный (б) потоки данных

Из рис.1.2б видно, что на интервале времени T_2 канал не используется парой абонентов (источником передаваемых данных и адресатом – получателем). Поэтому на этом интервале времени можно передавать информацию других абонентов, что повышает эффективность сети с пакетной коммутацией. Это и предопределило использование сетей с коммутацией пакетов для передачи всех видов трафика

В создаваемых в настоящее время **сетях следующего поколения** (Next Generation Network - **NGN**) предполагается использовать коммутацию пакетов для передачи всех видов трафика: аудио-сигналов (IP-телефония), видео-информации, компьютерных данных. Подобные сети также называют **мультисервисными (**Internet Multi Service **– IMS)** в отличие от ранее существовавших моносервисных сетей. Поскольку в сети NGN передается трафик различного вида, то и требования к **качеству обслуживания** (Quality of Service – **QoS**) разных видов передаваемого трафика будут различны.

В сетях NGN обеспечивается **слияние** (**конвергенция**) всех существующих сетей в единую информационную сеть для передачи мультимедийной информации. Пользователи такой сети должны иметь широкий выбор услуг с гарантированным качеством, что обеспечивается соответствующим уровнем управления, транспортным уровнем и уровнем доступа пользователей к мультисервисной сети (рис.1.3).

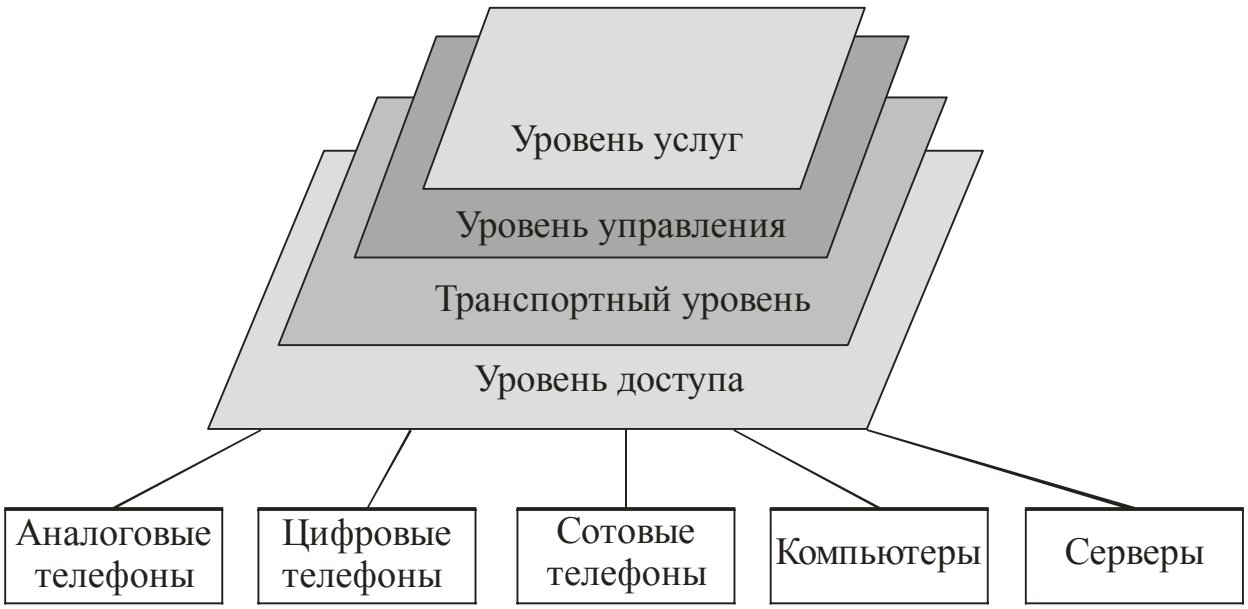


Рис.1.3. Уровни мультисервисной сети NGN

Транспортный уровень сети NGN создается на базе IP сетей с распределенной коммутацией пакетов. Доступ к транспортной сети обеспечивается через соответствующие устройства и шлюзы.

Сети следующего поколения NGN обеспечивают широкий набор услуг с гибкими возможностями по их управлению. Телекоммуникационные сети нового поколения используются для передачи всех видов информации: дискретных данных, аудио- и видеоинформации. Услуга передачи указанной триады (голоса, данных, и видеоинформации) по единой мультисервисной сети получила название *Triple Play*.

На рис.1.4 приведен пример структурной схемы сети телекоммуникаций, в которой пользователи (абоненты) через сети доступа подключаются к магистральной сети, обеспечивающей транспорт сообщений. В ряде случаев абонентам удобно объединяться в локальные сети, функционирующие в рамках ограниченного пространства (аудитория, здание, группа зданий).

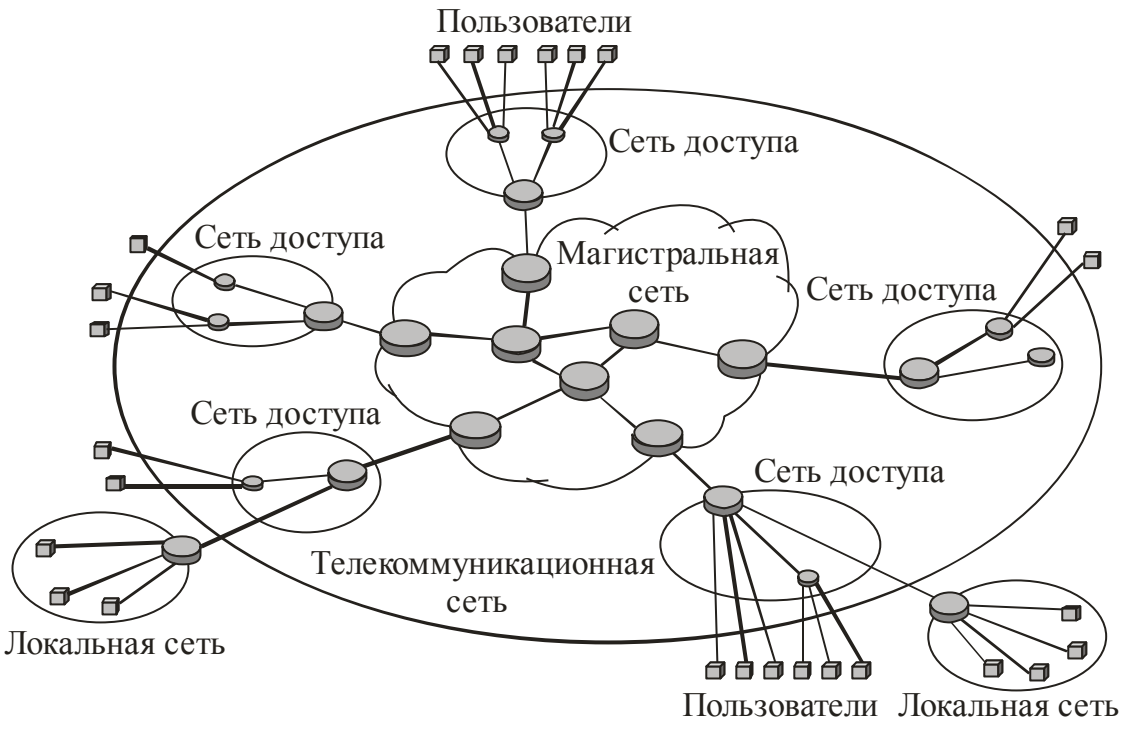


Рис.1.4. Структурная схема телекоммуникационной сети

Для доставки сообщения адресату назначения сообщение необходимо адресовать, поскольку оно проходит по соединениям многоканальных систем и сетей передачи, где одновременно передаются данные множества

абонентов. Адресация сообщений позволяет адресату назначения получать только ему предназначенную информацию. Адресация реализуется принципиально по-разному в сетях с коммутацией каналов и в сетях с коммутацией пакетов.

В сетях с коммутацией каналов каждой паре абонентов выделяется индивидуальный канал связи. Поскольку по линии связи может передаваться множество сообщений, то в линии формируется множество каналов. Сигналы по каналу передаются в виде цифровых значений дискретных отсчетов, следующих с определенным периодом дискретизации $T_д$. **Совокупность каналов,** передаваемых по линии связи за период $T_д$**, образует кадр**. Начало кадра отмечается соответствующим **заголовком** с многоразрядным сигналом синхронизации. Каждый канал находится на определенном месте кадра, что позволяет на приемной стороне точно определить местонахождение своего канала. Таким образом, адрес каждого дискретного отсчета сигнала определяется его местоположением в кадре. При объединении потоков частота передаваемой по каналу информации увеличивается, но период следования кадров остается постоянным (в телефонных сетях $T_д$ = 125 мкс).

В сетях с коммутацией пакетов задают адреса источника и получателя сообщения. Различают физические и логические адреса. Логические адреса принадлежат пользователям (абонентам), а физические адресуют устройства, обычно интерфейсы телекоммуникационных узлов и устройства абонентов.

К логическим адресам относятся, например, **IP-адреса** пользователей. В документации, используемой в настоящее время версии **IPv4**, адреса IP отображаются в десятичной форме в виде четырех групп чисел. Каждая группа может содержать числа от 0 до 255. Группы разделены между собой точками, например, 192.168.10.21; 172.16.250.17; 10.1.10.122.

В дополнение к логическим адресам в заголовке сообщения задаются физические адреса устройства-источника и устройства-назначения. В широко распространенной сетевой технологией Ethernet или её модификациях (Fast Ethernet, Gigabit Ethernet, 10Gigabit Ethernet) в качестве физических адресов используются **MAC-адреса** (Media Access Control) . В документации MAC-адреса представлены в виде 12 шестнадцатеричных чисел, например, 00-05-A8-69-CD-F1. Тот же адрес может быть представлен и в несколько другой форме 00:05:A8:69:CD:F1 или 0005.A869.CD-F1. MAC-адреса компьютеров прошиты в ПЗУ сетевой карты.

1.2. Классификация сетей передачи данных

Методы и устройства, используемые в вычислительных (компьютерных) сетях передачи данных, широко применяются при создании сетей **NGN.** Поэтому в настоящем курсе лекций основное внимание уделено аппаратным и программным средствам вычислительных (компьютерных) сетей, т.е. сетей передачи данных, на базе которых и создаются современные мультисервисные сети. В сетях передачи данных (компьютерных или вычислительных) поток может быть представлен различными информационными единицами: битами, байтами, кадрами, пакетами, ячейками, образующими информационный поток. **Сети передачи данных,** как правило, **относятся к сетям с коммутацией пакетов.**

Согласно одной из классификаций сети передачи данных подразделяются на **локальные** и **глобальные** (рис. 1.5). Сеть может размещаться на ограниченном пространстве, например, в отдельном здании, в аудитории. При этом она называется **локальной сетью** (Local Area Network - **LAN**). Основными технологиями локальных вычислительных сетей, которые применяются в настоящее время, являются Ethernet, Fast Ethernet, Gigabit Ethernet. Другие технологии ЛВС (Token Ring, 100VG-AnyLAN, FDDI и др.) используются редко.

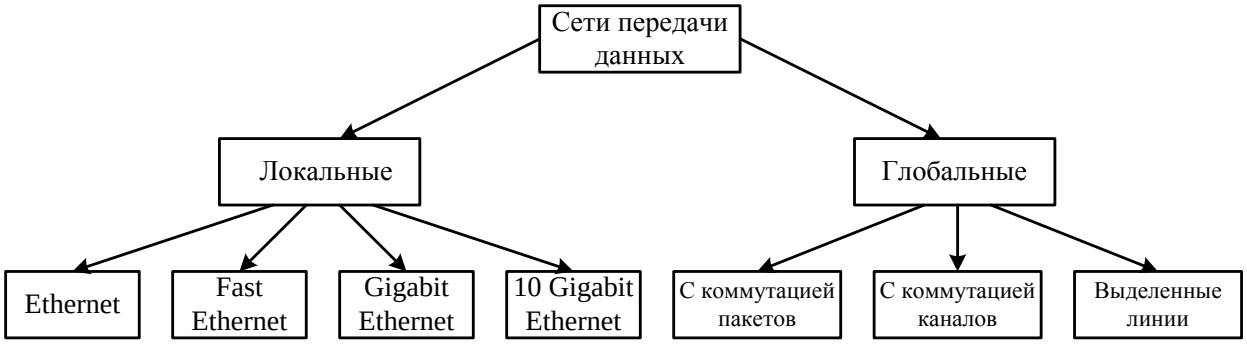


Рис. 1.5. Классификация сетей передачи данных

Совокупность нескольких локальных сетей называют **составной, распределенной** (internetwork, internet) или **глобальной сетью** (Wide Area Network - **WAN**). В составную сеть могут входить **подсети** (subnet) различных технологий. Крупные фирмы (корпорации) создают свои собственные *корпоративные сети* (intranet), которые используют технологии как глобальных, так и локальных сетей. Таким образом, объединение

пользователей, расположенных на широком географическом пространстве, например, в разных городах, для совместного использования информационных данных, производится с помощью глобальных сетей.

Глобальные сети передачи данных часто классифицируют (рис.1.5) на:

- сети с коммутацией каналов;
- сети, использующие выделенные линии;
- сети с коммутацией пакетов.

Сети с коммутацией каналов и с использованием выделенных линий строят на основе различных сетевых технологий. При этом используются следующие технологии и линии связи:

- цифровые линии, которые бывают постоянные, арендуемые, а также коммутируемые. В цифровых линиях применяют технологии **плезиохронной цифровой иерархии** (Plesiochronous Digital Hierarchy - **PDH**), **синхронной цифровой иерархии** (Synchronous Digital Hierarchy - **SDH**), а также технологии оптических транспортных сетей (**ОТС**) со **спектральным уплотнением по длине волны** (Wave-length Division Multiplexing – **WDM)** и плотным спекиральным уплотнением (Dense WDM – **DWDM**).
- **цифровые сети с интегрированными услугами (**Integrated Services Digital Network **– ISDN);**
- **цифровые абонентские линии** (Digital Subscriber Line – **DSL**);
- аналоговые выделенные линии и линии с коммутацией каналов (dialup) с применением модемов, т.е. аналоговые **АТС**.

Технологии PDH, SDH характеризуются высокой скоростью передачи данных. Например, скорость передачи данных по сетям технологии PDH составляет от 2 Мбит/с до 139 Мбит/с; технологии SDH – от 155 Мбит/с до 10 Гбит/с и выше. Дальнейшее увеличение скорости передачи данных достигнуто в системах со спектральным уплотнением по длине волны (технологии WDM, DWDM) на волоконно-оптических кабелях. Основными аппаратными средствами высокоскоростных технологий с коммутируемыми цифровыми линиями являются мультиплексоры (**MUX**).

Широкое распространение в настоящее время получили **сети с коммутацией пакетов**, в которых применяются следующие сетевые технологии:

- технологии виртуальных каналов, к которым относятся сети X.25; сети **трансляции кадров** (Frame Relay **– FR**); сети **асинхронного способа передачи данных** (Asynchronous Transfer Mode **– ATM);**

- технологии сетевого интернет протокола (Internet Protocol – **IP),** использующие **дейтаграммный метод** передачи сообщений.

Таким образом, в сетях с коммутацией пакетов могут использоваться технологии **виртуальных каналов**, применяемые в сетях X.25, Frame Relay, ATM, или технологии передачи **дейтаграммных** сообщений – сети IP в зависимости от предъявляемых требований.

Технологии виртуальных каналов предусматривают предварительное соединение конечных узлов (источника и назначения), при этом прокладывается маршрут (виртуальный канал), по которому затем передаются данные. Получение данных подтверждается приемной стороной. Технология X.25 ориентирована на ненадежные аналоговые линии связи, поэтому характеризуется низкой скоростью передачи данных (до 48 кбит/с). Однако данная технология применяется до настоящего времени, например, в сетях банкоматов, из-за своей высокой надежности при ненадежных линиях. Технология Frame Relay обеспечивает более высокую по сравнению с X.25 скорость передачи данных до 2 – 4 Мбит/с. Но линии связи должны быть более надежными по сравнению с X.25. Наибольшую скорость передачи данных (155 Мбит/с, 620 Мбит/с, а также 2,4 Гбит/с) обеспечивают сети ATM. Однако развитие этих сетей сдерживает их высокая стоимость.

Сети технологии **IP** являются **дейтаграммными**, когда отсутствует предварительное соединение конечных узлов и нет подтверждения приема сообщения. Поэтому отдельные части большого сообщения могут передаваться по разным маршрутам и потеря отдельной части сообщения может остаться незамеченной. Такой метод характеризуется высокой скоростью передачи, но низкой надежностью, поскольку нет подтверждения принятых данных. Высокую надежность обеспечивает протокол управления передачей **TCP** (Transmission Control Protocol). Набор (стек) протоколов TCP/IP обеспечивает компромиссное решение по цене, скорости и надежности передачи данных. Поэтому на базе протоколов TCP/IP создается транспортный уровень мультисервисных сетей следующего поколения NGN с распределенной коммутацией пакетов. В свою очередь, **сети с**

коммутацией каналов играют роль транспорта для сетей с коммутацией пакетов.

Следует отметить еще одну сетевую технологию, которая стремительно развивается в последнее время, это технология **виртуальных частных сетей** (Virtual private network - **VPN**). Даная технология использует сеть общего пользования Интернет, в которой формирует защищенные каналы связи с гарантированной полосой пропускания. Таким образом, при экономичности и доступности Интернет сети VPN обеспечивают **безопасность и качество** передаваемых сообщений. Используя VPN, сотрудники фирмы могут получить безопасный дистанционный доступ к корпоративной (частной) сети компании через Интернет.

1.3. Семиуровневая модель взаимодействия открытых систем

Сложность сетевых структур и разнообразие телекоммуникационных устройств, выпускаемых различными фирмами, привели к необходимости стандартизации как устройств, так и процедур обмена данными между пользователями. Международная организация по стандартизации (International Standards Organization - **ISO**) создала базовую эталонную модель взаимодействия **открытых систем** (Open System Interconnection reference model - **OSI**), которая определяет концепцию и методологию создания сетей передачи данных. Модель описывает стандартные правила функционирования устройств и программных средств при обмене данными между узлами (компьютерами) в открытой системе. Открытая система состоит из программно-аппаратных средств, способных взаимодействовать между собой **при использовании стандартных правил и устройств сопряжения** (интерфейсов).

Модель ISO/OSI включает семь уровней. На рис. 1.6 показана модель взаимодействия двух устройств: **узла источника** (source) и **узла назначения** (destination). **Совокупность правил, по которым происходит обмен данными между программно-аппаратными средствами, находящимися на одном уровне, называется протоколом**. Набор протоколов называется **стеком** протоколов и задается определенным стандартом. Взаимодействие между уровнями определяется стандартными **интерфейсами.**

Рис. 1.6. Семиуровневая модель ISO/OSI

Взаимодействие соответствующих уровней является **виртуальным**, за исключением физического уровня, на котором происходит обмен данными по физической среде, соединяющей компьютеры. На рис. 1.6 приведены также примеры протоколов, управляющих взаимодействием узлов на различных уровнях модели OSI. Взаимодействие уровней между собой внутри узла происходит через межуровневый **интерфейс,** и каждый нижележащий уровень предоставляет услуги вышележащему.

Виртуальный обмен между соответствующими уровнями узлов A и B (рис. 1.7) происходит определенными единицами информации. На трех верхних уровнях – это **сообщения** или данные (Data). На транспортном уровне – **сегменты** (Segment), на сетевом уровне – **пакеты** (Packet), на канальном уровне – **кадры** (Frame) и на физическом – последовательность битов.

Для каждой сетевой технологии существуют свои протоколы и свои технические средства, часть из которых имеет условные обозначения, приведенные на рис.1.7. Данные обозначения введены фирмой **Cisco** и стали общепринятыми. Среди технических средств физического уровня следует отметить кабели, разъемы, повторители сигналов (repeater), многопортовые повторители или концентраторы (**hub**), преобразователи среды (transceiver), например, преобразователи электрических сигналов в оптические и наоборот. На канальном уровне это мосты (bridge), коммутаторы (**switch**). На сетевом

уровне – маршрутизаторы (**router**). **Сетевые карты** или **адаптеры** (Network Interface Card – **NIC**) функционируют как на канальном, так и на физическом уровне, что обусловлено сетевой технологией и средой передачи данных.

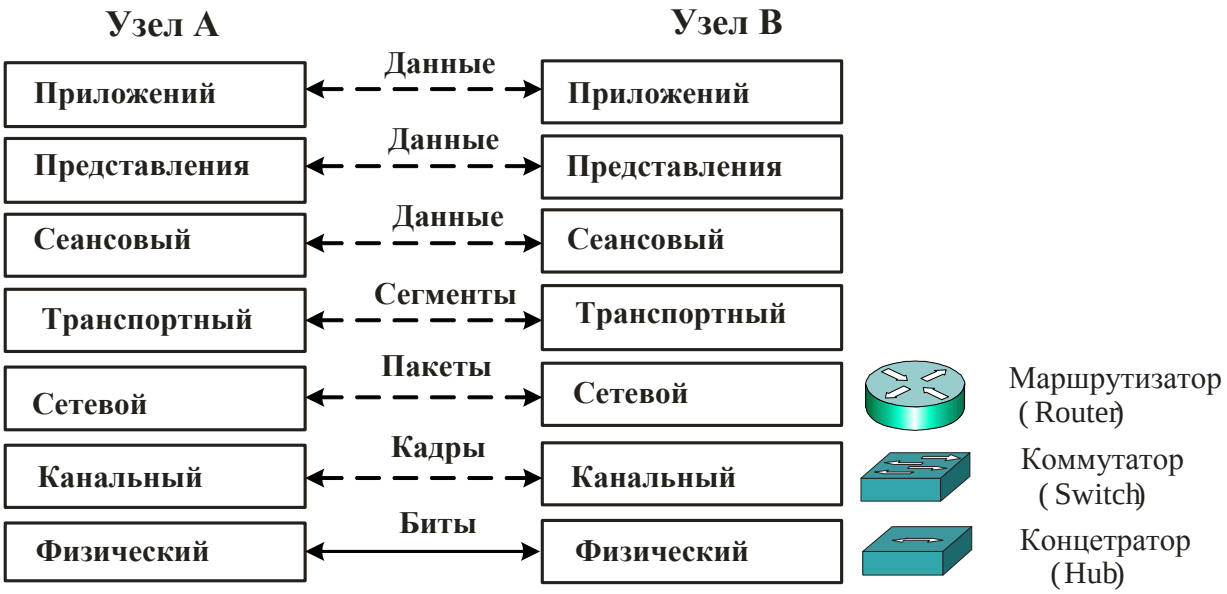


Рис.1.7. Устройства и единицы информации соответствующих уровней

При передаче данных от источника к узлу назначения, подготовленные передаваемые данные последовательно проходят от самого верхнего 7-го уровня Приложений узла источника информации до самого нижнего – Физического уровня 1, затем передаются по физической среде узлу назначения, где последовательно проходят от нижнего уровня 1 до уровня 7.

Самый верхний уровень **Приложений** (Application Layer) 7 оперирует наиболее общей единицей данных – сообщением. На этом уровне реализуется управление общим доступом к сети, потоком данных, сетевыми службами (протоколами), такими как FTP, TFTP, HTTP, SMTP, SNMP и др.

Уровень 6 **Представления** (Presentation Layer) изменяет форму представления данных. Например, передаваемые с уровня 7 данные преобразуются в общепринятый формат ASCII. При приеме данных происходит обратный процесс. На уровне 6 также происходит шифрация и сжатие данных (протоколы MPEG, JPEG).

Сеансовый (Session Layer) уровень 5 устанавливает сеанс связи двух конечных узлов (компьютеров), определяет, какой компьютер является

ведущим, а какой ведомым, задает для передающей стороны время передачи. Этот уровень определяет также сеанс связи с сетью Интернет.

Транспортный уровень (Transport Layer) 4 делит большое сообщение узла источника информации на части, при этом добавляет заголовок и формирует **сегменты** определенного объема, а короткие сообщения может объединять в один сегмент. В узле назначения происходит обратный процесс. В заголовке сегмента задаются **номера порта** источника и назначения, которые адресуют службы верхнего уровня приложений для обработки данного сегмента. Кроме того, транспортный уровень обеспечивает **надежную доставку пакетов**. При обнаружении потерь и ошибок на этом уровне формируется запрос повторной передачи, при этом используется протокол **TCP**. Когда необходимость проверки правильности доставленного сообщения отсутствует, то используется более простой и быстрый **протокол дейтаграмм пользователя** (User Datagram Protocol – **UDP**).

Сетевой уровень (Network Layer) 3 адресует сообщение, задавая единице передаваемых данных (**пакету**) **логические сетевые адреса** узла назначения и узла источника (**IP-адреса**), определяет **маршрут**, по которому будет отправлен **пакет данных**, транслирует логические сетевые адреса в физические, а на приемной стороне – физические адреса в логические. Сетевые логические IP-адреса принадлежат пользователям.

Канальный уровень (Data Link) 2 формирует из пакетов **кадры** данных (frames). На этом уровне задаются **физические адреса** устройства-отправителя и устройства-получателя данных, например, MAC-адреса при использовании технологии Ethernet. Физический адрес устройства может быть прописан в ПЗУ сетевой карты компьютера. На этом же уровне к передаваемым данным добавляется контрольная сумма, определяемая с помощью алгоритма циклического кода. На приемной стороне по контрольной сумме определяют ошибки.

Физический уровень (Physical) 1 осуществляет передачу потока битов по соответствующей физической среде (электрический или оптический кабель, радиоканал) через соответствующий интерфейс. На этом уровне производится кодирование данных, синхронизация передаваемых битов информации.

Протоколы трех верхних уровней являются сетенезависимыми, три нижних уровня являются сетезависимыми. Связь между тремя верхними и тремя нижними уровнями происходит на транспортном уровне.

Важным процессом при передаче данных является **инкапсуляция** (encapsulation) данных. Передаваемое сообщение, сформированное приложением, проходит три верхних сетенезависимых уровня и поступает на транспортный уровень, где делится на части и каждая часть инкапсулируется (помещается) в сегмент данных (рис. 1.8). В заголовке сегмента содержится номер протокола уровня приложений, с помощью которого подготовлено сообщение, и номер протокола, который будет обрабатывать данный сегмент.

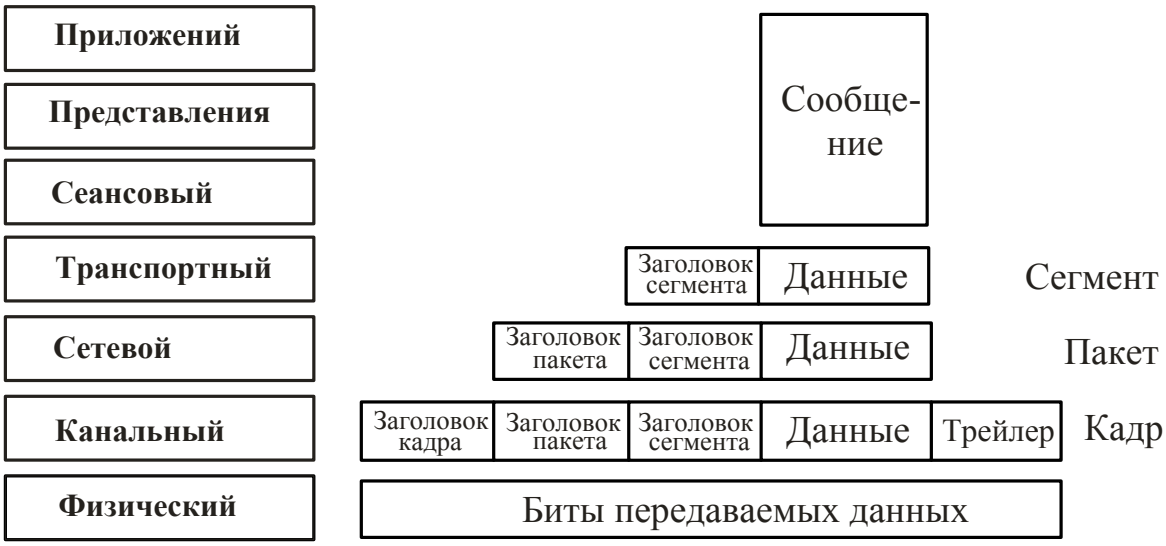


Рис. 1.8. Инкапсуляция данных

На сетевом уровне сегмент инкапсулируется в **пакет** данных, заголовок (**header**) которого содержит, кроме прочего, сетевые (логические) адреса отправителя информации (источника) – Source Address (**SA**) и получателя (назначения) – Destination Address (**DA**). В данном курсе – это **IP-адреса.**

На канальном уровне пакет инкапсулируется в **кадр** или **фрейм** данных, заголовок которого содержит физические адреса узла передатчика и приемника, а также другую информацию. Кроме того, на этом уровне добавляется **трейлер** (концевик) кадра, содержащий информацию, необходимую для проверки правильности принятой информации. Таким образом, происходит обрамление данных заголовками со служебной информацией, т.е. **инкапсуляция** данных.

Название информационных единиц на каждом уровне, их размер и другие параметры инкапсуляции задаются согласно протоколу единиц данных (Protocol Data Unit – PDU). Итак, на трех верхних уровнях – это **сообщение (Data)**, на Транспортном Уровне 4 – **сегмент (Segment)**, на Сетевом Уровне 3 – **пакет (Packet)**, на Канальном Уровне 2 – **кадр (Frame),** на Физическом Уровне 1 – **последовательность битов**.

Помимо семиуровневой OSI модели на практике применяется четырехуровневая модель TCP/IP (рис. 1.9).

Рис.1.9. Модели OSI и TCP/IP

Уровень Приложений модели TCP/IP по названию совпадает с названием модели OSI, но по функциям гораздо шире, поскольку охватывает три верхних сетенезависимых уровня (Приложений, Представления и Сеансовый). Транспортный уровень обеих моделей и по названию, и по функциям одинаков. Сетевой уровень модели OSI соответствует межсетевому (**Internet**) уровню модели TCP/IP, а два нижних уровня (канальный и физический) представлены объединенным уровнем доступа к сети (**Network Access**).

Ниже в табл.1.1 приведены обобщенные сведения об основной информации, добавляемой в заголовках сообщений на разных уровнях OSI модели.

Таблица 1.1

Основная информация в заголовках сообщений

Физический уровень	Канальный уровень	Сетевой уровень	Транспортный уровень	Верхние уровни
Частотно-временные параметры и синхронизация	Физические адреса источника и назначения	Логические адреса источника и назначения	Номера порта источника и назначения	Сопряжение пользователей с сетью

На транспортном уровне в заголовке сегмента задаются номера портов приложений источника и назначения. Номера портов адресуют приложения или службы (сервисы) верхнего уровня, которые создавали сообщение и будут его обрабатывать на приемной стороне. Например, сервер электронной почты с номерами портов 25 и 110 позволяет посылать e-mail сообщения и принимать их, № порта 80 адресует веб-сервер.

Вместе с физическими, например, MAC-адресами и логическими IP-адресами задание номеров портов образует тройную систему адресации, которая позволяет адресовать устройства, пользователей и программное обеспечение приложений.

Поскольку на трех нижних уровнях модели OSI функционируют аппаратно программные средства, то обработка сообщения проводится с высокой скоростью. На верхних же уровнях функционируют программные средства, что увеличивает время обработки (задержку). В выше приведенных примерах (рис. 1.6, 1.7) два конечных узла взаимодействовали непосредственно между собой. Поэтому сформированное на узле источнике сообщение последовательно проходило все семь уровней с 7 по 1, на что тратилось много времени. В реальных сетях сообщение от одного конечного узла до другого проходит через целый ряд промежуточных устройств, таких как коммутаторы, маршрутизаторы. Поэтому для снижения времени задержки (повышения быстродействия) на промежуточных устройствах сообщение обрабатывается средствами только трех, или даже двух, нижних уровней (рис.1.10).

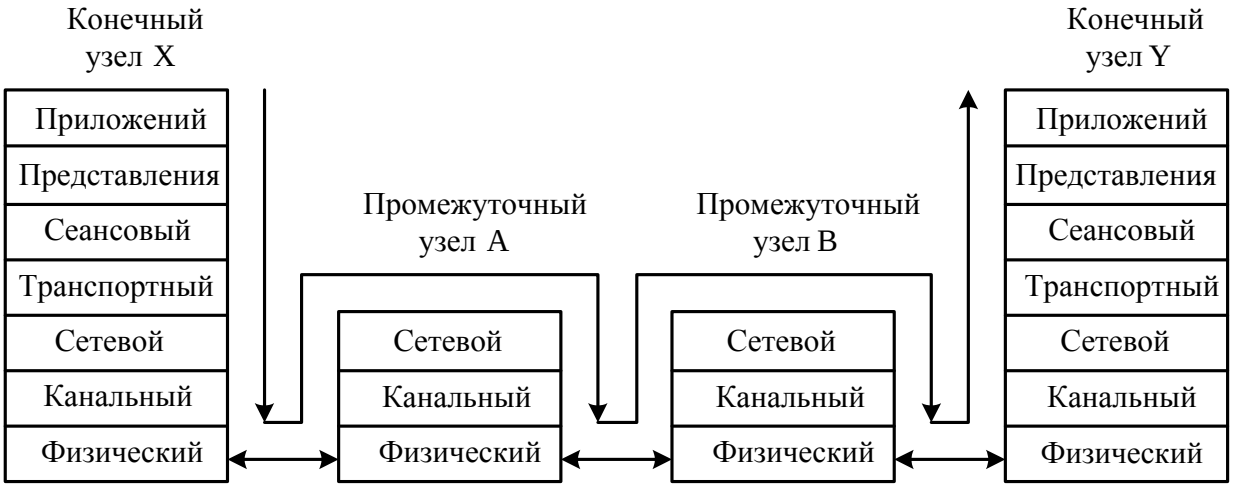


Рис. 1.10. Передача сообщения по сети

Таким образом, Транспортный уровень, обеспечивающий надежность передачи данных, и верхние уровни (Приложений, Представления, Сеансовый) функционирует только на конечных узлах, что снижает задержку передачи сообщения по всей сети от одного конечного узла до другого. В приведенном примере (рис. 1.10) протокол IP функционирует на всех узлах сети, а полный стек протоколов TCP/IP – только на конечных узлах.

Краткие итоги лекции 1

1. Телекоммуникационная сеть образуется совокупностью абонентов и узлов связи, соединенных линиями (каналами) связи.
2. Различают сети: с коммутацией каналов, когда телекоммуникационные узлы выполняют функции коммутаторов, и с коммутацией пакетов (сообщений), когда телекоммуникационные узлы выполняют функции маршрутизаторов.
3. Для создания маршрута в разветвленной сети необходимо задавать *адреса* источника и получателя сообщения. Различают физические и логические адреса.
4. Сети передачи данных с коммутацией пакетов подразделяются на локальные и глобальные.
5. Сети технологии IP являются дейтаграммными, когда отсутствует предварительное соединение конечных узлов и нет подтверждения приема сообщения.
6. Высокую надежность обеспечивает протокол управления передачей TCP.
7. Эталонная модель взаимодействия открытых систем ISO/OSI определяет концепцию и методологию создания сетей передачи данных и включает семь уровней.
8. Виртуальный обмен между соответствующими уровнями конечных узлов происходит определенными единицами информации. На трех верхних уровнях – это сообщения или данные. На транспортном уровне – сегменты, на сетевом уровне – пакеты, на канальном уровне – кадры и на физическом – последовательность битов.
9. Технические средства физического уровня представлены кабелями, разъемами, повторителями сигналов, многопортовыми повторителями или концентраторами (hub), преобразователями среды (transceiver). На канальном уровне это мосты (bridge) и коммутаторы (switch). На сетевом уровне – маршрутизаторы (router). Сетевые карты или адаптеры (Network Interface Card – NIC) функционируют на канальном и на физическом уровне.
10. Обрамление единиц информации заголовками со служебной информацией, называется инкапсуляцией.
11. Тройная система адресации (логические адреса, физические адреса, номера портов) позволяет адресовать устройства, пользователей и программное обеспечение приложений.

Вопросы по лекции 1

1. Что собой представляют телекоммуникационные сети?
2. Чем отличаются сети с коммутацией каналов от сетей с коммутацией сообщений?
3. Какие функции выполняет маршрутизатор?
4. Что собой представляет метрика протокола маршрутизации?
5. В чем различие коммутации пакетов или сообщений?
6. В чем различие между локальными и глобальными сетями передачи данных?
7. Каковы основные функции Уровня 1 модели OSI?
8. Каковы основные функции Уровня 2 модели OSI?
9. Каковы основные функции Уровня 3 модели OSI?
10. Каковы основные функции Уровня 4 модели OSI?
11. Каковы основные функции Уровня 5 модели OSI?
12. Каковы основные функции Уровня 6 модели OSI?
13. Каковы основные функции Уровня 7 модели OSI?
14. Что собой представляет инкапсуляция данных?
15. Какие устройства функционируют на Уровне 3 модели OSI?
16. Какие устройства функционируют на Уровне 2 модели OSI?
17. Какие устройства функционируют на Уровне 1 модели OSI?
18. Перечислите уровни модели TCP/IP.
19. Какие три системы адресации используются в сетевых технологиях?
20. На каком уровне модели OSI задаются IP адреса?

Упражнения

1. Изобразите эталонную модель взаимодействия открытых систем ISO/OSI.
2. Сравните функции уровней моделей OSI и TCP/IP.
3. Изобразите схему инкапсуляции единиц информации на транспортном, сетевом и канальном уровнях.
4. Приведите примеры логических и физических адресов.
5. Объясните, почему в сетях используется три системы адресации.

Лекция 2. ВЕРХНИЕ УРОВНИ МОДЕЛЕЙ OSI, TCP/IP

Краткая аннотация лекции: приведены основные функции протоколов уровня приложений и транспортного уровня. Показаны примеры функционирования протоколов транспортного уровня, форматы заголовков сегментов.
Цель лекции: изучить основы функционирования протоколов уровня приложений и транспортного уровня модели OSI.

2.1. Уровень приложений

Уровень приложений модели OSI обеспечивает сопряжение человека с сетевыми технологиями, что позволяет пользователям общаться между собой через сеть. Другими словами, уровень приложений создает интерфейс между приложениями конечных устройств при передаче сообщений по сети. Уровень 7 представляет собой комплекс программных средств, представленных в двух формах: в виде **приложений (**applications**)** и программ **служб сервиса (**services**)**.

Сопряжение человека с сетью обеспечивают приложения. Широко известны такое приложение этого уровня, как **web-браузер всемирной паутины – сервиса, предоставляющего доступ к гипертекстовой информации** (World Wide Web – **WWW)**, что позволяет людям готовить сообщения для передачи по сети и принимать такие сообщения. Наиболее известными web-браузерами являются Internet Explorer, Mozilla Firefox, Opera.

Программы служб сервиса готовят данные для передачи по сети, обеспечивая эффективное использование ресурсов сети. Разные типы информации (аудио-, видео-, текстовая информация) требуют различных услуг, поскольку разнотипную информацию необходимо передать через общую сеть.

Протоколы уровня приложений определяют правила обмена данными между узлом источником информации и узлом назначения. Каждый вид приложений и сервиса использует свои протоколы, которые определяют стандарты и форматы передаваемых данных.

Протоколы и службы уровня приложений обычно представлены соответствующими серверами. Однако сервер, как отдельное устройство, может объединять функции нескольких служб сервиса; или наоборот, служба

одного вида услуг может быть представлена многими серверами разного уровня.

Наиболее распространенными протоколами и службами уровня приложений являются:

- протоколы электронной почты (Simple Mail Transfer Protocol – **SMTP**, Post Office Protocol – **POP**, Internet Messaging Access Protocol – **IMAP**);

- протокол передачи гипертекстовой информации или web-сервер (Hypertext Transfer Protocol – **HTTP**);

- протокол передачи файлов (File Transfer Protocol – **FTP**) и простой протокол передачи файлов (Trivial FTP – **TFTP**);

- система доменных имен (Domain Name System – **DNS**);

- протокол удаленного доступа (**Telnet**), обеспечивающий виртуальное соединение с удаленными сетевыми устройствами и прототокол удаленного доступа, обеспечивающий шифрование передаваемых данных (Secure Shell – **SSH**);

- протокол динамического конфигурирования узлов (Dynamic Host Configuration Protocol – **DHCP**).

Таким образом, **приложения** уровня 7 модели OSI обеспечивают интерфейс (сопряжение) человека с сетью. **Службы сервиса** – используют программные средства протоколов, чтобы подготовить информацию для передачи по сети.

Существуют две модели построения сети:

1. Модель «**клиент – сервер**»;
2. Модель соединения равноправных узлов сети (**peer-to-peer**).

В сети peer-to-peer связанные через сеть конечные узлы разделяют общие ресурсы (принтеры, файлы) без выделенного сервера. Каждое конечное устройство (peer) может функционировать либо как сервер, либо как клиент. Компьютер может выполнять роль сервера для одного соединения и роль клиента для другого.

Согласно модели **«клиент – сервер»** клиент запрашивает информацию, пересылая запрос **выделенному серверу** (upload), который в ответ на запрос посылает (download) файл, принимаемый клиентом. Следовательно, клиент инициирует процесс обмена информацией в среде «клиент – сервер» и получает от сервера требуемую информацию. Главным достоинством модели

«клиент – сервер» является централизация управления сетью и обеспечение безопасности.

Ниже приведены краткие характеристики некоторых наиболее широко используемых протоколов уровня приложений.

Протоколы передачи электронной почты

При передаче электронной почты и взаимодействии почтовых серверов между собой используется простой протокол передачи почты (Simple Mail Transfer Protocol – **SMTP**), у которого номер порта 25. Для получения клиентом сообщения с сервера используется протокол почтового отделения (Post Office Protocol – **POP**) с номером порта 110 или протокол доступа к сообщениям (Internet Messaging Access Protocol – **IMAP**).

На рис.2.1 приведена модель клиент-сервер в службе электронной почты. При пересылке почты от клиента на сервер используется протокол SMTP, при этом происходит процесс upload.

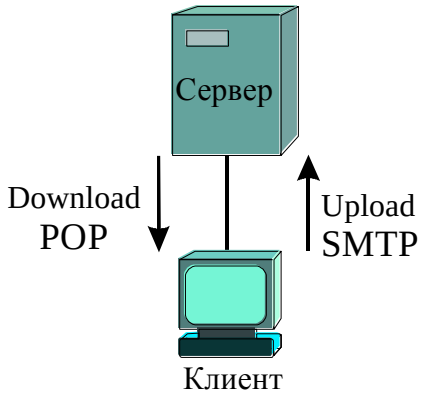


Рис.2.1. Модель клиент-сервер в службе электронной почты

Когда почтовый сервер получает сообщение, предназначенное для клиента, он хранит это сообщение и ждет, когда адресат назначения заберет свою почту. Почтовые клиенты забирают сообщения (процесс download), используя один из сетевых протоколов. Самые популярные почтовые протоколы клиента – POP3 и IMAP4, которые на транспортном уровне используют протокол TCP для надежной доставки данных.

Почтовые серверы общаются друг с другом, используя протокол SMTP, который транспортирует почтовые сообщения в текстовом формате,

взаимодействуя с TCP. Протокол SMTP характеризуется низким уровнем защиты информации, поэтому серверы предоставляют услуги только пользователям своей сети.

В процессе подготовки электронной почты люди используют клиентское приложение, называемое почтовый агент пользователя, почтовый клиент (Mail User Agent – **MUA**). Приложение MUA позволяет посылать сообщения и помещать полученные сообщения в почтовый ящик клиента (рис.2.2).

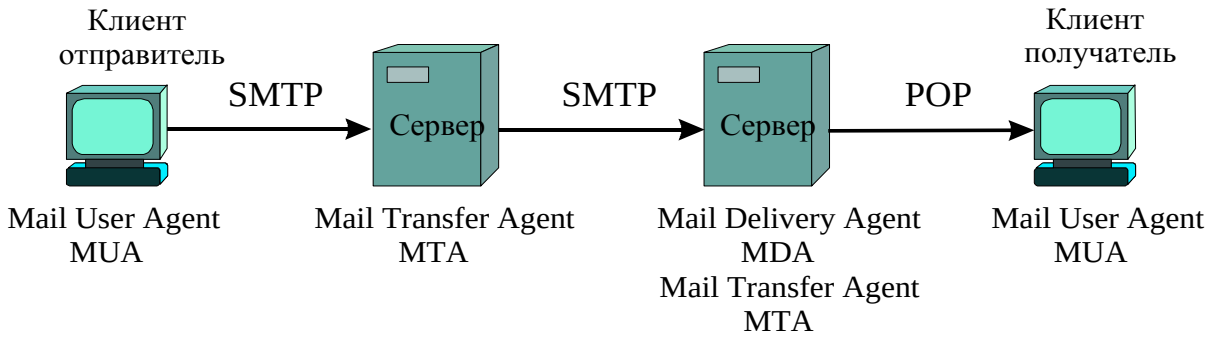


Рис.2.2. Передача электронной почты по сети

При передаче сообщений между серверами используется Агент передачи почты (Mail Transfer Agent – **MTA**). Агент MTA получает сообщения от MUA или от другого MTA и передает их по сети. Агенты MTA используют протокол SMTP, для передачи электронной почты между серверами. Если сообщение из сервера может быть отправлено сразу клиенту локальной сети, то подключается Агент доставки почты (Mail Delivery Agent – **MDA**). Агент MDA получает прибывающую почту от MTA и помещает ее в соответствующие почтовые ящики пользователей, используя протокол POP.

Протокол HTTP

Самым распространенным протоколом уровня приложений в настоящее время является **протокол передачи гипертекстовой информации** (Hypertext Transfer Protocol – **HTTP**), который работает в сети Интернет. Его основным приложением является Web-браузер, который отображает данные на Web-страницах, используя текст, графику, звук и видео. Web-страницы создаются с использованием языка разметки гипертекста Hypertext Markup Language (HTML), который определяет местоположения для размещения текста, файлов и объектов, которые

должны быть переданы от сервера по сети до Web-браузера. *Номер порта протокола HTTP – 80*, функционирует совместно с протоколом транспортного уровня TCP.

В ответ на запрос сервер посылает клиенту сети текст, аудио-, видео- и графические файлы. Браузер клиента повторно собирает все файлы, чтобы создать изображение Web-страницы, которая представляется пользователю.

Протокол HTTP характеризуется сравнительно невысоким уровнем безопасности, поскольку передаваемые по сети сообщения не зашифрованы. Для повышения уровня безопасности передачи сообщений через Интернет был разработан протокол HTTP Secure (**HTTPS**). В этом протоколе используется процесс шифрования (криптографирования) данных (*encryption*) и аутентификации (*authentication*), что существенно повышает уровень безопасности. *Номер порта протокола HTTPS – 443*.

Протоколы передачи файлов FTP и TFTP

Протокол передачи файлов (Fail Transfer Protocol – **FTP**) – служба, ориентированная на предварительное соединение (connection-oriented), которая взаимодействует с протоколом транспортного уровня TCP. Главная цель протокола FTP состоит в том, чтобы передавать файлы от одного компьютера другому, или копировать и перемещать файлы от серверов клиентам и от клиентов серверам. Это является главным отличием от протокола HTTP, который позволяет клиенту «скачивать» файлы с сервера, но не позволяет пересылать файлы на сервер.

Протокол передачи файлов FTP сначала устанавливает соединение между клиентом и сервером, используя команды запроса клиента и ответы сервера. При этом *номер порта – 21*. Затем производится обмен данными, когда *номер порта – 20*. Передача данных может производиться в режиме кода ASCII или в двоичном коде. Эти режимы определяют кодирование, используемое для файла данных, которое в модели OSI является задачей уровня представления (presentation). После завершения передачи файла, соединение для передачи данных заканчивается автоматически. Управление сеансом связи происходит на сеансовом (Session) уровне.

Простой протокол передачи файлов (Trivial Fail Transfer Protocol – **TFTP**) – служба без установления соединения (connectionless), которая работает совместно с протоколом транспортного уровня (User Datagram Protocol – **UDP**). Протокол TFTP используется на маршрутизаторах, чтобы передавать файлы конфигурации и операционную систему Cisco IOS, а также для передачи файлов между системами, которые поддерживают TFTP. Протокол TFTP характеризует простота и малый объем программного обеспечения. Протокол TFTP может читать или записывать файлы при соединении с сервером, но не ведет списки и каталоги. Поэтому протокол TFTP работает быстрее, чем протокол FTP.

Система доменных имен DNS

Система доменных имен (Domain Name System – **DNS**), используется в Интернете для того, чтобы переводить имена сайтов или доменов в числовые значения IP адреса. Людям легче запомнить доменное имя, например, www.cisco.com, чем числовой адрес 198.133.219.25. Кроме того, числовые адреса могут со временем меняться. Например, в настоящее время указанный выше числовой адрес сайта www.cisco.com изменен на 72.163.4.161. Поскольку в ряде случаев требуется знание числового адреса, то хост может обратиться к DNS-серверу и по имени получить соответствующий адрес. DNS использует распределенный набор серверов разного уровня иерархии, чтобы получить соответствие между именем и числовым адресом.

Операционные системы компьютеров содержат утилиту **nslookup**, которая позволяет пользователю вручную запрашивать имя сервера и идентифицировать название хоста. Когда клиент делает запрос, локальный сервер сначала проверяет собственные записи. Если соответствующих пар «имя – адрес» у него нет, то он связывается с другими серверами DNS более высокого уровня иерархии.

На рис.2.3 приведен пример выполнения команды **nslookup**, которая позволяет пользователю вручную запросить адрес DNS сервера. Команда выполняется в режиме командной строки (**Пуск → Программы →**

Стандартные → Командная строка). В приведенном примере выполнено четыре команды:

1. По команде **nslookup** был получен адрес DNS сервера – 10.0.6.10.

2. Затем был произведен запрос адреса сайта www.cisco.com, IP-адрес которого – 72.163.4.161.

3. Был запрошен адрес сайта cisco.netacad.net – 128.107.229.50.

4. Запрос сайта www.psuti.ru дал результат – 89.186.238.202.

Рис.2.3. Пример выполнения команды **nslookup**

Служба прикладного уровня DNS характеризуется *номером порта 53* и взаимодействует как с протоколом транспортного уровня TCP, так и с протоколом UDP.

Протокол удаленного доступа Telnet

Протокол Telnet обеспечивает подключение к командной строке удаленного узла, т.е. виртуальное соединение пользователя с удаленными сетевыми устройствами: компьютерами, маршрутизаторами, коммутаторами. Чтобы сделать подключение клиента по протоколу Telnet, обычно задают имя удаленного хоста. В качестве имени хоста используется IP-адрес или имя доменной системы DNS удаленного устройства. Вся обработка информации и использование памяти производится на процессоре удаленного устройства, а отображение результатов конфигурирования протокол Telnet транслирует на монитор пользователя. Telnet работает на уровне приложений модели TCP/IP, поэтому охватывает все уровни модели OSI. *Номер порта протокола Telnet – 23*.

Протокол Telnet поддерживает аутентификацию, поэтому на удаленном устройстве задается пароль, который должен знать пользователь. Однако Telnet не поддерживает криптографирование данных, которые передаются по сети как простой текст. Это означает, что данные могут быть перехвачены. Для защиты передаваемой информации разработан протокол удаленного доступа, обеспечивающий шифрование передаваемых данных (**Secure Shell – SSH**). Он обеспечивает криптографирование данных и более надежную аутентификацию, *номер порта – 22*. Протокол SSH заменяет Telnet.

Протокол динамического конфигурирования узлов DHCP

Всем устройствам, которые обмениваются сообщениями через сеть Интернет, необходимы уникальные IP-адреса. Эти адреса могут назначаться в статическом или динамическом режиме. В статическом режиме адреса вручную назначает администратор при конфигурировании устройства. **Рекомендуется назначать статические IP-адреса на маршрутизаторы, серверы, сетевые принтеры** и другие устройства, адреса которых меняется редко. В то же время, адреса рабочих станций могут изменяться достаточно часто. Некоторые пользователи в Интернет выходят эпизодически, поэтому им нужны IP-адреса не постоянно.

Протокол динамического конфигурирования узлов (Dynamic Host Configuration Protocol – **DHCP**) позволяет автоматизировать процесс назначения IP-адресов рабочим станциям из диапазона, предоставленного администратору провайдером. Динамическое назначение адресов протоколом DHCP производится по запросу клиента на определенный промежуток времени, для продления которого пользователь должен периодически обращаться к серверу. При освобождении IP-адресов они возвращаются DHCP-серверу, который перераспределяет их. При повторном запросе клиента, освободившего IP-адрес, сервер пытается назначить ранее использовавшийся адрес. Помимо IP-адреса протокол DHCP предоставляет пользователю еще целый ряд параметров (маску подсети, шлюз по умолчанию, IP-адрес сервера DNS и др.)

2.2. Транспортный уровень моделей OSI, TCP/IP

Транспортный уровень моделей OSI и TCP/IP одинаков как по функциям, так и по названию (см. рис. 1.9). Термин TCP/IP – это комбинация двух протоколов. **Протокол IP** функционирует на сетевом Уровне 3 модели OSI, он является **протоколом дейтаграммного типа** без предварительного соединения (*connectionless*), который обеспечивает доставку сообщения через сеть по возможности, т.е. доставку с наибольшими возможными усилиями (**best-effort delivery)**, но без гарантий, т.е. *доставка не надежная*. **Протокол управления передачей TCP** работает на транспортном Уровне 4 модели OSI и является протоколом, ориентированным на предварительное соединение (*connection-oriented*), что обеспечивает *контроль потока и надежность доставки*. Когда эти протоколы объединены, они обеспечивают более широкий объем услуг: малую задержку и высокую надежность. Всемирная сеть Интернет строится на основе набора (стека) протоколов TCP/IP.

Основной функцией транспортного уровня является транспортировка сообщений и управление потоком информации от источника до устройства назначения, с обеспечением надежности доставки. Контроль доставки сообщения из одного конца соединения до другого и надежность обеспечены целым рядом параметров, передаваемых в заголовках сегментов:

номерами последовательности передаваемых сегментов данных,

размером, так называемого, скользящего окна,

квитированием, т.е. подтверждением приема сообщения.

Транспортный уровень устанавливает логическое соединение между двумя конечными точками сети. Протоколы транспортного уровня (см. рис. 1.6) сегментируют данные, посланные приложениями верхнего уровня на передающей стороне, и повторно собирают (реассемблируют) из полученных сегментов целое сообщение на приемной стороне.

Таким образом, протоколы транспортного уровня:

- реализуют *сегментацию данных* и повторную сборку целого сообщения из полученных сегментов. Большинство сетей имеет ограничение на объем передаваемых сообщений. Поэтому Транспортный уровень делит большое сообщение уровня приложений на сегменты данных, размер которых соответствует требованиям **протокола единиц данных** Protocol Data Unit – **PDU** более низких уровней сетевой модели. Кроме того, если в процессе

контроля обнаружится, что принятое сообщение содержит ошибку, то возникает необходимость повторной передачи всего большого сообщения. При обнаружении ошибки в одном из принятых сегментов только данный сегмент будет передан повторно. Сегменты могут быть направлены одному или многим узлам назначения;

- *обеспечивают многочисленные* одновременно протекающие процессы обмена данными. На каждом конечном узле сети может быть запущено много разных приложений. Множество одновременно протекающих процессов обмена данными верхнего уровня может быть мультиплексировано поверх одного логического транспортного соединения. Чтобы передавать потоки данных соответствующим приложениям, протокол транспортного уровня должен идентифицировать каждое приложение. В протоколах TCP и UDP в качестве **идентификатора приложения используют номер порта**. Номер порта в заголовке сегмента транспортного уровня указывает, какое приложение создало передаваемое сообщение, и какое должно обрабатывать полученные данные на приемной стороне. При множестве одновременно протекающих обменах данными каждому из приложений или услуг назначается свой **адрес** (**номер порта**) так, чтобы транспортный уровень мог определить, с каким конкретно приложением или службой передаваемые данные должны взаимодействовать.

Наиболее известными протоколами транспортного уровня являются **протокол контроля передачи** (Transmission Control Protocol – **TCP**) и **протокол дейтаграмм пользователя** (User Datagram Protocol – **UDP**). Кроме того, на транспортном уровне функционирует **протокол надежной доставки** (Reliable Transport Protocol – **RTP**), взаимодействие которого с протоколом EIGRP, рассмотрено в лекции 11.

Протокол контроля передачи TCP является ориентированным на предварительное соединение (connection-oriented). Помимо деления сообщения на сегменты и идентификации приложений TCP обеспечивает *контроль потока и надежность*. Он взаимодействует с протоколами прикладного уровня: HTTP, SMTP, FTP, Telnet и другими. Протокол UDP является протоколом дейтаграммного типа connectionless, взаимодействует с такими протоколами прикладного уровня, как система доменных имен – DNS, передачи потока видеоданных – *Video Steaming*, голос поверх IP – *Voice*

over IP и рядом других. Следует отметить, что система DNS взаимодействует как с TCP, так и с UDP.

Итак, протокол транспортного уровня TCP помимо деления сообщения на сегменты и идентификации приложений обеспечивает:

1. Контроль потока.
2. Надежность доставки сообщения.

Для облегчения контроля и обеспечения надежности сообщения передаются частями (порциями), т.е. сегментами. При этом протокол транспортного уровня узла источника должен прослеживать каждый сегмент данных при передаче и повторно передавать любую часть сообщения, прием которой не был подтвержден устройством назначения. Транспортный уровень конечного узла на приемной стороне должен отследить получение данных и подтвердить это получение.

Контроль потока необходим, чтобы гарантировать, что источник, передавая данные с некоторой скоростью, не переполняет буферные устройства узла назначения. Если узел назначения не может обрабатывать данные в темпе их поступления, то может произойти переполнение буферов и потеря данных. Управление скоростью передачи данных обеспечивается изменением **размера окна** (**Window Size**), который указывает, сколько байт данных должно быть передано за одну порцию. При переполнении буферных устройств узел назначения посылает источнику требование уменьшения размера окна.

После получения каждой порции данных узел назначения посылает источнику **подтверждение принятых данных** или **подтверждение доставки** (**acknowledgment**).

Подтверждение (квитирование) обеспечивает **надежность** сети передачи данных. Если подтверждение не получено, то неподтвержденная порция данных передается узлом источником повторно.

В дейтаграммных IP-сетях пакеты одного сообщения между двумя конечными устройствами могут проходить разными путями. Поэтому на узел назначения сегменты могут прийти не в том порядке, в котором были переданы. Надежный протокол транспортного уровня (TCP) должен восстановить правильный порядок сегментов и собрать переданное сообщение (реассемблировать его).

Адресация приложений, надежность, контроль потока, сегментация сообщений и их реассемблирование, реализуются путем задания ряда параметров в заголовке сегмента TCP (рис.2.4), размер которого 20 байт.

<table>
<tr><td colspan="1">1</td><td colspan="1">2</td><td colspan="1">3</td><td colspan="1">4</td><td colspan="1">5</td><td colspan="1">6</td><td colspan="1">7</td><td colspan="1">8</td><td colspan="1">9</td><td colspan="1">10</td><td colspan="1">11</td><td colspan="1">12</td><td colspan="1">13</td><td colspan="1">14</td><td colspan="1">15</td><td colspan="1">16</td><td colspan="1">17</td><td colspan="1">18</td><td colspan="1">19</td><td colspan="1">20</td><td colspan="1">21</td><td colspan="1">22</td><td colspan="1">23</td><td colspan="1">24</td><td colspan="1">25</td><td colspan="1">26</td><td colspan="1">27</td><td colspan="1">28</td><td colspan="1">29</td><td colspan="1">30</td><td colspan="1">31</td><td colspan="1">32</td></tr>
<tr><td colspan="16">Номер порта источника</td><td colspan="16">Номер порта назначения</td></tr>
<tr><td colspan="32">Номер последовательности</td></tr>
<tr><td colspan="32">Номер подтверждения</td></tr>
<tr><td colspan="4">ДЗ</td><td colspan="6">Резерв</td><td colspan="6">Код</td><td colspan="16">Размер скользящего окна</td></tr>
<tr><td colspan="16">Контрольная сумма</td><td colspan="16">Индикатор</td></tr>
<tr><td colspan="32">Опции</td></tr>
<tr><td colspan="32">Данные</td></tr>
</table>

Рис.2.4. Формат заголовка сегмента TCP

Поля заголовка TCP сегмента определяют следующее:

- **Номер порта источника (**Source Port**)** – 16 бит номера порта, который посылает данные;

- **Номер порта назначения (**Destination Port) – 16 бит номера порта, который принимает данные;

- **Номер последовательности (**Sequence Number) – 32 бита номера первого байта в сегменте, используемого, чтобы гарантировать объединение частей (порций) данных в корректном порядке в устройстве назначения;

- **Номер подтверждения (**Acknowledgment Number) – 32 бита последовательного номера подтверждения принятых данных, (начальный номер байта следующей ожидаемой порции данных);

- **ДЗ** – длина заголовка (число 32-разрядных слов в заголовке);

- **Резерв** – разряды поля, установленные в ноль;

- **Код** – 6 разрядов, определяющих тип сегмента, например, сегмент установки соединения (SYN) и завершения сеанса (FIN), сегмент подтверждения принятых данных (ACK), срочного сообщения (URG);

- **Размер окна (**Window Size) – число байтов, передаваемых за одну порцию;

- **Контрольная сумма (**Checksum) – значение контрольной суммы заголовка и поля данных;

- **Индикатор** (Urgent pointer) – индицирует конец срочных данных;

- **Опции (**Option) – каждая текущая опция определяет максимальный размер TCP сегмента;

- **Данные (**Data) – сообщение протокола верхнего уровня.

Поскольку UDP является протоколом дейтаграммного типа, то в заголовке его сегмента (рис.2.5) отсутствуют такие параметры, как Номер последовательности, Номер подтверждения, Размер окна.

Рис.2.5. Формат сегмента UDP

Поля UDP сегмента определяют следующее:

- **Номер порта источника (**Source Port**)** – 16 бит номера порта, который посылает данные;

- **Номер порта назначения (**Destination Port) – 16 бит номера порта, который принимает данные;

- **Длина (**Length) – число байтов в заголовке и в поле данных;

- **Контрольная сумма (**Checksum) – контрольная сумма заголовка и поля данных;

- **Данные (**Data) – сообщение протокола верхнего уровня.

Поскольку протокол UDP не обладает механизмами надежности, то она обеспечивается протоколами верхнего уровня приложений. Однако небольшой размер заголовка UDP и отсутствие дополнительной обработки номера последовательности, размера окна и пересылки подтверждения получения данных повышают скорость обработки и передачи сообщений по сравнению с протоколом TCP.

Комбинация номера порта и IP-адреса образует комплексный адрес, так называемый **сокет** (**socket address**), который определяет не только уникальное устройство, но и программное обеспечение, используемое для создания и обработки сообщения, например, 192.168.10.17:1275; 10.1.10.6:53.

Номера портов делятся на несколько типов:

- **известные номера** (Well Known Ports), диапазон адресов которых находится в пределах от 0 до 1023;
- **зарегистрированные** порты с номерами от 1024 до 49151;
- **динамические** порты с номерами от 49151 до 65535, которые обычно динамически присваиваются пользователям.

Номера известных портов заданы организацией Internet Assigned Numbers Authority (**IANA**), распределяющей адреса в Интернете. Номера известных портов назначаются протоколам и службам сервиса уровня приложений. Номера некоторых известных портов протокола TCP приведены в табл.2.1

Таблица 2.1

Номера известных портов

Протоколы	FTP	Telnet	SMTP	HTTP	HTTPS	POP3
Порты	20, 21	23	25	80	443	110

В приложении протокола передачи файлов FTP используются два известных (стандартных) номера порта 20 и 21. Порт 20 используется для передачи данных, а порт 21 – для управления соединением.

Среди номеров известных портов протокола UDP наиболее распространенными являются: протокол TFTP – 69, RIP – 520.

Служба DNS с номером порта 53 и простой протокол управления сетью (Simple Network Management Protocol – **SNMP**) с номером порта 161 взаимодействуют как с протоколом TCP, так и с UDP.

Зарегистрированные порты назначаются как пользователям, так и приложениям. Когда зарегистрированные порты не используются для ресурсов сервера, они могут быть использованы динамически клиентом как номер порта источника. Из зарегистрированных портов можно отметить альтернативные порты протокола HTTP – 8008 и 8080.

Заголовок TCP сегмента (рис.2.4) содержит последовательный номер (Sequence Number), используемый, чтобы гарантировать объединение частей (сегментов) сообщения в том порядке, в котором они были переданы. Протокол UDP не имеет такого механизма, поэтому возможны ошибки при объединении сегментов данных при передаче по сложной сети. Однако скорость передачи данных с использованием протокола UDP выше, чем TCP.

Если необходимо узнать, какие TCP соединения активны на сетевом конечном узле, то можно использовать команду **netstat** в режиме командной строки. В распечатке команды (рис.2.6) указаны: протокол (TCP), локальные адреса узлов с динамически назначенными номерами порта, внешние адреса (или имена) узлов назначения с номером порта, а также состояние связи.

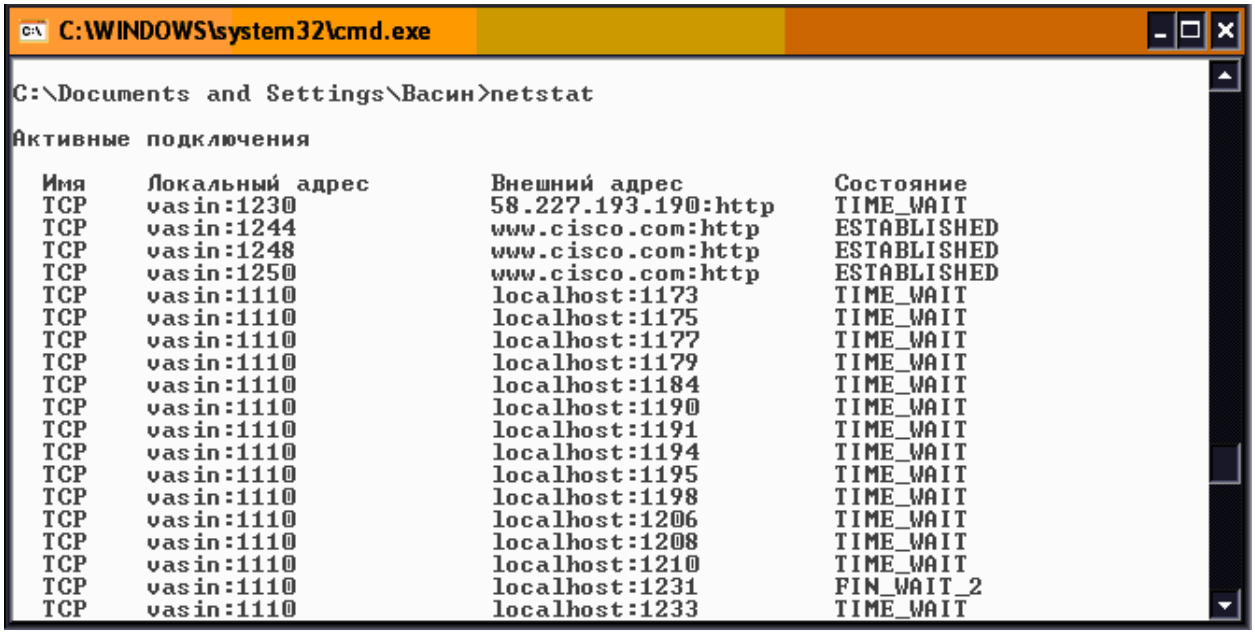


Рис.2.6. Результат выполнения команды **netstat**

В данном примере номер порта локального адреса является динамически назначаемым зарегистрированным портом источника с номером больше 1023. Для адреса www.cisco.com внешний порт задан символически: http. Состояние связи может быть с установленным соединением (ESTABLISHED) или с ожиданием окончания соединения (TIME_WAIT), когда был послан запрос окончания соединения (FIN).

Установление соединения

Поскольку TCP является протоколом, ориентированным на предварительное соединение (connection-oriented), то сначала необходимо установить сессию между приложениями конечных устройств. Узел отправитель инициализирует соединение, которое должно быть подтверждено узлом получателем. Программное обеспечение протокола TCP обмениваются сообщениями через сеть, чтобы проверить, что передача разрешена и что обе стороны готовы к ней.

Соединение между двумя устройствами производится в три этапа (рис.2.7).

Во-первых, узел отправитель инициализирует установление связи путем посылки узлу получателю запроса синхронизации SYN (1).

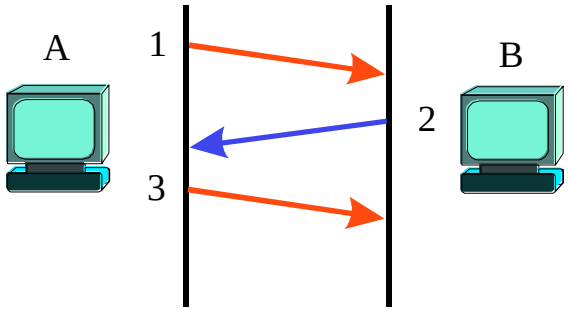


Рис.2.7. Установление соединения

Во-вторых, узел получатель подтверждает запрос синхронизации и задает свои параметры синхронизации ACK (2).

В третьих, узлу получателю посылается подтверждение, что обе стороны готовы, чтобы соединение было установлено (3).

Такой механизм получил название трехэтапного установления связи (Three-way handshake**)**. Оба узла должны согласовать начальные номера последовательности передаваемых частей информации, что происходит через обмен сегментами синхронизации (SYN) и подтверждения (ACK).

Синхронизация требует, чтобы каждая сторона послала собственный начальный номер последовательности и получила подтверждение от другой стороны. Каждая сторона, получив начальный номер последовательности от другой стороны, отвечает подтверждением ACK. Например, последовательность, соответствующая рис.2.7, будет следующей:

1. Узел отправитель (A) инициализирует соединение, посылая сегмент SYN узлу получателю (B), в котором указывает номер своей последовательности Sequence Number, например, $SEC_A = 101$.
2. Получив сегмент инициализации соединения, узел B делает запись принятого номера последовательности 101 и формирует ответ в виде $ACK_B = 101 + 1 = 102$. Ответ $ACK_B = 102$ означает, что хост B получил сегмент данных, включая байт с номером 101, и ожидает следующий

байт с номером 102. Одновременно хост В формирует начальный номер своей последовательности данных, например, $SEC_B = 51$.

3. Узел А, получив сегмент от В со значениями $ACK_B = 102$, $SEC_B = 51$, формирует ответ $ACK_A = 52$, $SEC_A = 102$, который завершает процесс соединения.

Передача данных

Сегменты данных нужно предоставить пользователю получателю в том же порядке, в котором они были переданы. Сбой происходит, если какие-то сегменты данных потеряны, повреждены или получены в неверном порядке. Поэтому получатель должен подтвердить получение каждого сегмента. Однако если бы отправитель ждал ответ ACK после посылки каждого сегмента, то производительность сети была бы низкой. Поэтому, надежный, ориентированный на предварительное соединение протокол, например TCP, позволяет послать несколько сегментов прежде, чем отправитель получит подтверждение ACK.

Размер окна (Window Size) заголовка сегмента TCP (рис.2.4) определяет, сколько байт данных передается в одной порции подтверждаемых данных. Последовательность сегментов передаваемых данных представляет собой последовательность байтов. Поэтому и размер окна в заголовке сегмента задается в количестве передаваемых байтов. Узел-получатель передает отправителю подтверждение ACK, когда примет указанное в окне количество байтов данных.

На рис.2.8 приведен пример, когда размер окна составляет 3000 байт, а каждый передаваемый сегмент содержит 1500 байт, что соответствует максимальному размеру поля данных кадра Ethernet. Поэтому узел-отправитель передает два сегмента подряд, на которые узел-получатель посылает подтверждение ACK с номером следующего ожидаемого байта, т.е. ACK = 3001. После получения узлом-отправителем подтверждения процесс передачи данных повторяется.

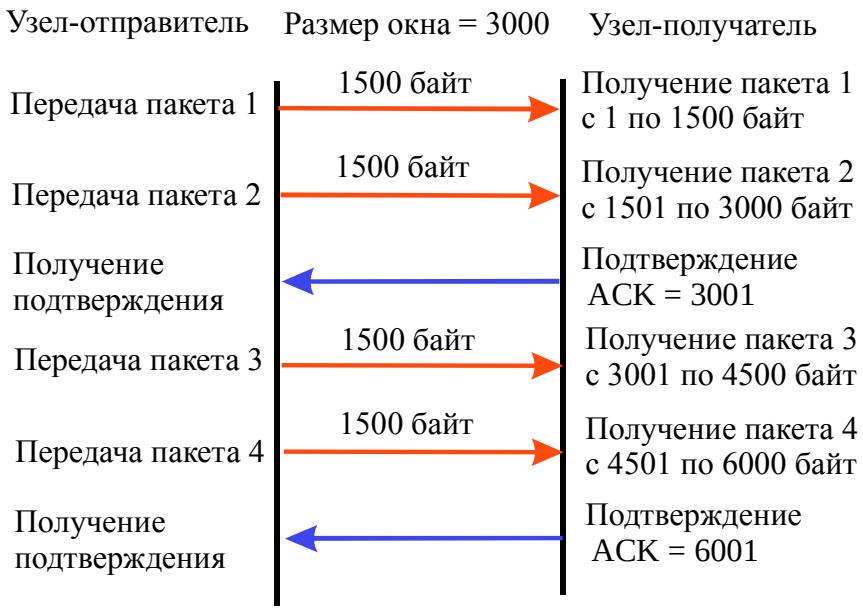


Рис.2.8. Процесс передачи байт данных

Если какой-то сегмент в процессе передачи был потерян, например, из-за перегрузки сети, то узел-получатель в ответе укажет начальный номер потерянного сегмента (рис.2.9), чтобы этот сегмент был передан повторно. При этом размер окна может быть уменьшен до 1500 байт, т.е. до размера одного передаваемого сегмента.

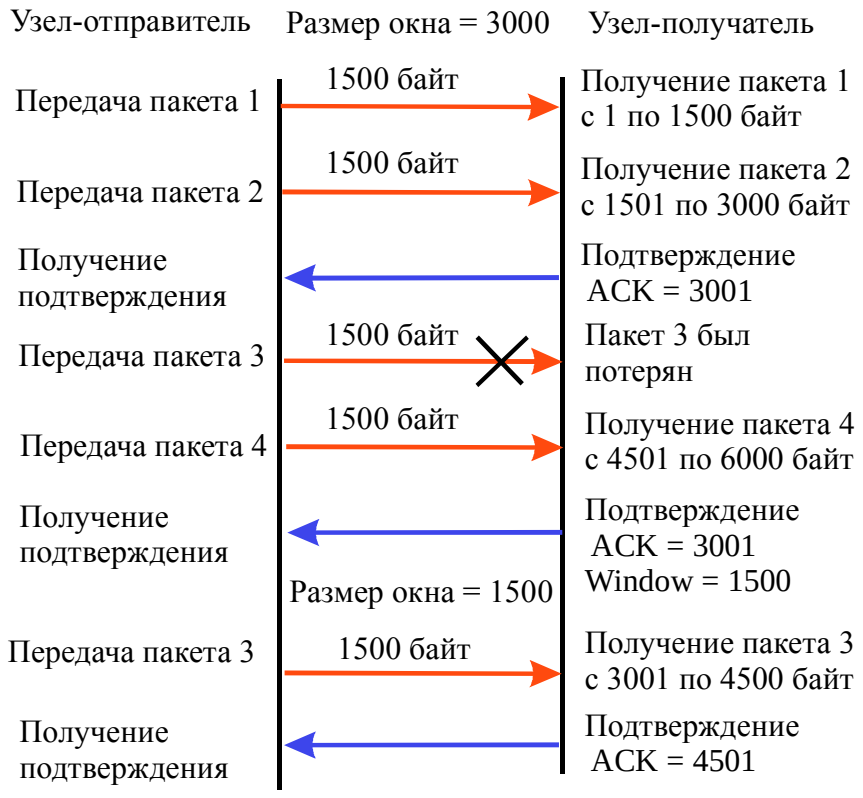


Рис.2.9. Перегрузка в процессе передачи байт данных

Перегрузка буферов данных может произойти по следующим причинам:

1. Высокоскоростной узел-отправитель генерирует трафик быстрее, чем сеть может передать его, а узел-получатель принять.
2. Несколько узлов одновременно посылают сообщения одному узлу-получателю.

Когда данные прибывают на узел-получатель слишком быстро, то буферные устройства адресата могут оказаться перегружены и приходящие пакеты будут отбрасываться. Чтобы не потерять данные, процесс TCP на узле-получателе может послать отправителю индикатор «*не готов*», чтобы отправитель приостановил передачу данных.

Когда получатель вновь сможет обрабатывать дополнительные данные, он посылает индикатор «*готов*». Когда этот индикатор получен, отправитель может продолжить передачу.

При передаче срочных сообщений используется бит URG в поле кода передаваемых сегментов. Такие сегменты передаются в первую очередь, даже за счет впереди стоящих в очереди сегментов.

Завершение соединения

Для завершения соединения в конце передачи данных, узел-отправитель, инициализировавший обмен данными, посылает сегмент конца передачи FIN. В ответ на это узел-получатель подтверждает (ACK) конец передачи и также посылает сигнал конца передачи FIN. Узел-отправитель подтверждает получение информации (ACK), на этом соединение заканчивается, т.е. завершение соединения происходит в четыре этапа.

Краткие итоги лекции 2

1. Уровень приложений представляет собой комплекс программных средств, представленных в двух формах: приложений и служб сервиса.
2. Сопряжение человека с сетью обеспечивают приложения.
3. Программы служб сервиса готовят данные для передачи по сети, обеспечивая эффективное использование ресурсов сети.
4. Наиболее распространенными протоколами и службами уровня приложений являются: протоколы электронной почты SMTP, POP, IMAP; протокол передачи гипертекстовой информации HTTP; протокол передачи файлов FTP; простой протокол передачи файлов TFTP; система доменных имен DNS; протоколы удаленного доступа Telnet и SSH; протокол динамического конфигурирования узлов DHCP.
5. В сети peer-to-peer связанные через сеть конечные узлы разделяют общие ресурсы (принтеры, файлы) без выделенного сервера.
6. В сети модели «клиент – сервер» клиент запрашивает информацию, пересылая запрос выделенному серверу, который в ответ на запрос посылает файл, принимаемый клиентом.
7. Протокол IP функционирует на сетевом Уровне 3 модели OSI и является протоколом дейтаграммного типа без предварительного соединения и без обеспечения надежной доставки.
8. Высокую надежность обеспечивает протокол управления передачей TCP, для чего используется контроль потока, нумерация последовательности и подтверждение принятых данных.
9. Протоколы транспортного уровня сегментируют данные, посланные приложениями верхнего уровня на передающей стороне, и повторно собирают его на приемной стороне.
10. В протоколах TCP и UDP в качестве идентификатора приложения используется номер порта.
11. Номера известных портов назначаются протоколам и службам сервиса уровня приложений.
12. Установление и завершение соединения производится по определенным правилам.

Вопросы по лекции 2

1. Каковы две формы программных средств уровня приложений?
2. Где находятся основные ресурсы сети модели «клиент – сервер»?
3. Где находятся основные ресурсы сети модели «peer-to-peer»?
4. Назовите протоколы передачи электронной почты.
5. Какие функции выполняет протокол HTTP?
6. В чем различие между протоколами HTTP и HTTPS?
7. В чем различие между протоколом FTP и HTTP?
8. Для чего используется система доменных имен DNS?
9. По какой команде можно получить адрес DNS сервера?
10. Какие протоколы обеспечивают удаленный доступ, т.е. подключение пользователя к командной строке удаленного узла?
11. Какой протокол обеспечивает динамическое конфигурирование узлов?
12. В чем различие между протоколами TCP и UDP?
13. По какой команде можно узнать, какие TCP соединения активны на сетевом конечном узле?
14. Какую функцию в заголовке сегмента TCP выполняет номер последовательности?
15. Какую функцию в заголовке сегмента TCP выполняет подтверждение?
16. Какую функцию в заголовке сегмента TCP выполняет размер окна?
17. Какую функцию в заголовке сегмента TCP выполняет номер порта?
18. За сколько этапов выполняется предварительное установление соединения у протокола TCP?
19. Чем определяется размер поля данных сегмента?

<u>Упражнения</u>

1. Перечислите номера портов протоколов HTTP, HTTPS, FTP, DNS, Telnet, SMTP. Укажите, какие функции выполняют данные протоколы.
2. Изобразите формат заголовка сегмента TCP. Объясните назначение полей заголовка.
3. Изобразите процесс установления соединения протокола TCP.
4. Изобразите процесс передачи данных при использовании протокола TCP.
5. Объясните, за счет чего протокол TCP реализует надежность передачи данных.

Лекция 3. ФИЗИЧЕСКИЙ УРОВЕНЬ МОДЕЛИ OSI

Краткая аннотация лекции: приведено описание основных устройств и средств физического уровня модели OSI. Даны характеристики медных и оптоволоконных кабелей, беспроводных радиоканалов. Рассмотрены понятия физической и логической топологии.
Цель лекции: познакомиться с физической средой передачи сигналов.

Три нижних уровня модели OSI являются сетезависимыми, т.е. программные и аппаратные средства физического, канального и сетевого уровней зависят от сетевых технологий. Аппаратные средства физического уровня представлены медными и оптоволоконными кабелями, беспроводной средой передачи данных, разъемами, повторителями сигналов (repeater), многопортовыми повторителями или концентраторами (hub), преобразователями среды (transceiver), например, преобразователями электрических сигналов в оптические и наоборот. Отдельно следует отметить сетевые карты или адаптеры (Network Interface Card – **NIC**), функционирование которых охватывает как канальный, так и физический уровни. В модели TCP/IP канальный и физический уровни представлены объединенным уровнем Network Access.

В качестве среды передачи в компьютерных сетях используют коаксиальный кабель (coaxial cable), неэкранированную (**UTP** – unshielded twisted pair) или экранированную витую пару (**STP** –shielded twisted pair), оптоволоконный кабель (fiber optic), беспроводные радиоканалы. Для каждой среды и технологии передачи данных определен свой стандарт.

3.1. Медные кабели

Локальные сети, как правило, строятся на основе неэкранированной витой пары UTP. Экранированная витая пара (STP), по сравнению с неэкранированной, обеспечивает лучшую защиту передаваемого сигнала от помех. Однако UTP дешевле, поэтому применяется в наиболее популярных технологиях Ethernet, Fast Ethernet, Gigabit Ethernet. Такие кабели называют также симметричными в отличие от коаксиальных медных кабелей.

В кабеле UTP четыре пары свитых медных проводов. Для подключения кабеля к компьютерам или другим сетевым устройствам используется разъем (коннектор) RJ-45, имеющий 8 контактов.

Основными характеристиками кабелей являются: максимальная частота передаваемого по кабелю сигнала, затухание, величина перекрестных наводок, сопротивление, емкость и др. Основные характеристики специфицированы международным стандартом ISO/IEC 11801. Стандарт ISO/IEC 11801специфицирует кабели по категориям (табл. 3.1). Кабели категории 7 – экранированные.

Таблица 3.1

Категории кабелей и разъемов

Категория кабеля и разъема	Макс. частота сигнала, МГц	Типовые приложения
Категория 3	16	Локальные сети Token Ring, Ethernet 10Base-T, голосовые каналы и др.
Категория 5	100	Локальные сети со скоростью передачи данных до 100 Мбит/с
Категория 7	600	Локальные сети со скоростью передачи данных до 1000 Мбит/с

Ранее использовавшийся в локальных сетях Ethernet кабель UTP категории 3 в сетях Fast Ethernet заменен кабелем категории 5. В настоящее время кабель UTP категории 5 заменяется кабелем категории 5e, по которому передаются данные со скоростью выше 125 Мбит/с. **Симметричные кабели UTP обеспечивают передачу сигналов на расстояние до 100 м.**

Для подключения **конечного узла (host)**, например компьютера, к повторителю или коммутатору (рис.3.1 а) используется прямой кабель (Straight-through Cable), схема подключения проводов которого к контактам разъемов RJ-45 приведена на рис.3.1 б. Первая пара проводов (контакты 1, 2) используется для передачи, вторая пара (контакты 3, 6) – для приема. Оставшиеся 2 пары не используются.

Прямой кабель используется для соединений:

1. Коммутатора с маршрутизатором
2. Коммутатора с компьютерами или серверами
3. Концентратора с компьютерами или серверами.

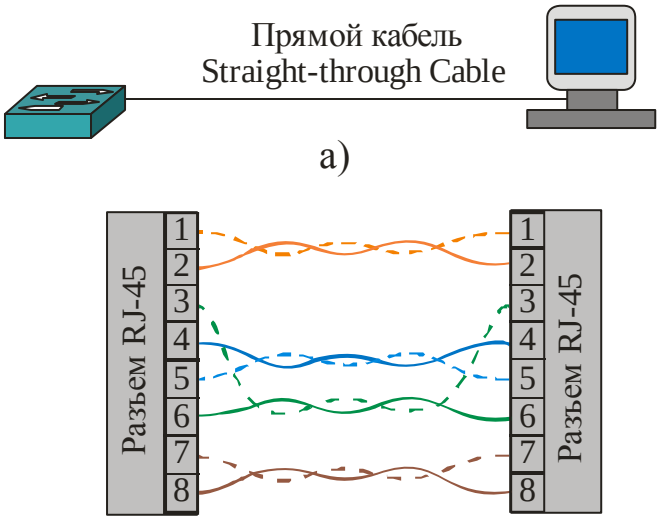


Рис. 3.1. Прямой кабель

Для соединения коммутаторов (switch) или концентраторов (hub) между собой используется **кроссовый кабель** (Crossover Cable), схема которого приведена на рис.3.2.

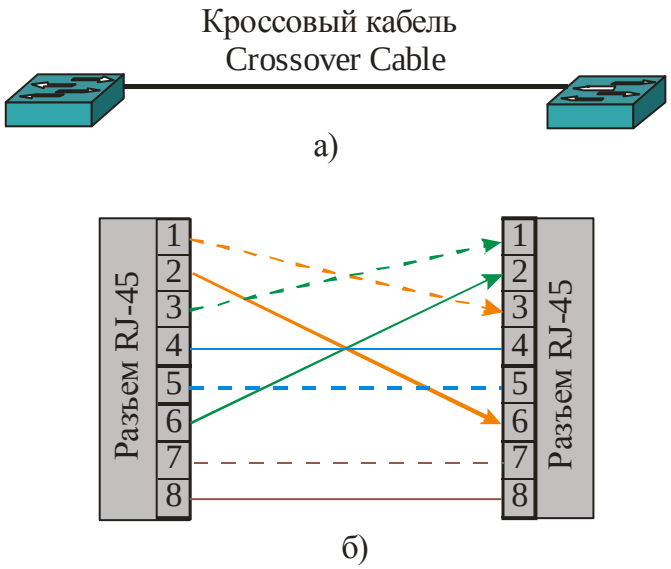


Рис.3.2. Кроссовый кабель

Кроссовый кабель использует 4 провода, причем, контакты 1 и 2 одного разъема RJ-45 соединяются с контактами 3 и 6 другого.

Кроссовый кабель используется для соединений:

1. Коммутатора с коммутатором
2. Коммутатора с концентратором
3. Концентратора с концентратором
4. Маршрутизатора с маршрутизатором

5. Маршрутизатора с компьютером
6. Компьютера с компьютером.

Для конфигурирования коммутатора или маршрутизатора их соединяют с последовательным COM-портом (RS-232) персонального компьютера. При этом используется **консольный кабель**, называемый также Rollover Cable (рис.3.3). Из рис.3.3 следует, что второй разъем кабеля имеет нумерацию контактов обратную первому. В отличие от прямого или кроссового кабелей, имеющих круглое сечение, консольный кабель – плоский, голубого или черного цвета.

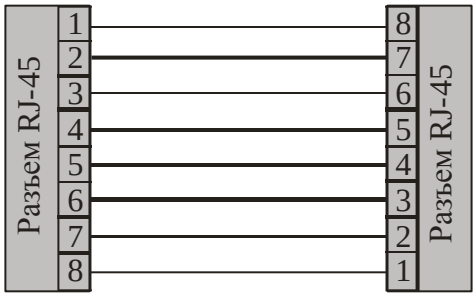


Рис.3.3. Консольный кабель

Интерфейс коммутатора или маршрутизатора для связи с терминалом называется консольным портом. При необходимости могут использоваться переходные адаптеры от разъема RJ-45 консольного кабеля к разъему DB-9 или DB-25 COM-порта терминала.

3. 2. Волоконно-оптические кабели

В качестве среды передачи в сетях наряду с электрическими кабелями широко используется кабель на **оптическом волокне** (**fiber optic**). Достоинством волоконно-оптического кабеля является отсутствие необходимости скручивания волокон или их экранирования, т.к. отсутствуют проблемы перекрестных помех (crosstalk) и электромагнитных помех от внешних источников. Это позволяет передавать сигналы на большее расстояние по сравнению с симметричным медным кабелем.

Оптическое волокно представляет собой двухслойную цилиндрическую структуру в виде сердцевины (оптического световода) и оболочки. Причем, сердцевина и оболочка имеют разную оптическую

плотность или показатель преломления n. Чем больше оптическая плотность материала, тем больше замедляется свет по сравнению со скоростью в вакууме. Значение показателя преломления сердцевины n_1 выше показателя преломления n_2 оболочки ($n_1 > n_2$).

Передача оптического излучения по световоду реализуется за счет свойства внутреннего отражения, которое обеспечивается неравенством показателей преломления сердцевины и оболочки $n_1 > n_2$, при этом сердцевина с большим показателем преломления является оптически более плотной средой.

Когда луч света 1 (рис.3.4) падает на границу раздела двух прозрачных материалов с коэффициентами преломления n_1 и n_2, причем $n_1 > n_2$, свет делится на две части.

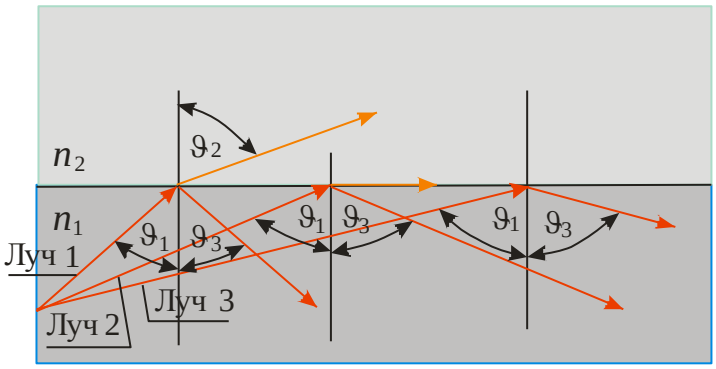
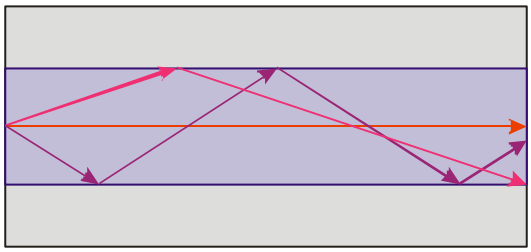


Рис.3.4. Отражение и преломление лучей света

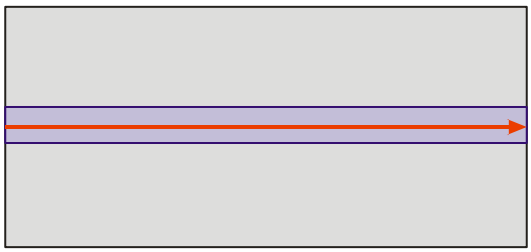
Часть светового луча отражается назад в исходную среду (сердцевину) с углом отражения ϑ_3 равным углу падения ϑ_1. Другая часть энергии светового луча пересекает границу раздела двух сред и вступает во второе вещество (оболочку) под углом ϑ_2. Эта часть энергии, попавшая в оболочку, характеризует потери энергии, которая должна была распространяться по сердцевине. При увеличении угла падения ϑ_1 возрастает угол преломления ϑ_2. При некотором значении угла ϑ_1, называемом критическим $\vartheta_{кр}$, луч 2 (рис.3.4) не преломляется; часть его отражается, а часть скользит вдоль границы раздела, т.е. угол преломления равен 90^o. При условии, что угол падения будет больше критического $\vartheta_1 > \vartheta_{кр}$ и $n_1 > n_2$, наступает эффект полного внутреннего отражения, когда вся энергия светового луча остается

внутри сердцевины, т.е. луч света распространяется по световоду без потерь на большое расстояние.

Диапазон углов падения лучей света, входящих в волокно, при котором реализуется первое условие полного внутреннего отражения, называется числовой апертурой волокна. Лучи света должны входить в сердцевину только под углом, находящимся внутри числовой апертуры волокна. Поскольку лучи входят под разными углами, то они отражаются от границы раздела сердцевины и оболочки под разными углами и проходят разное расстояние до устройства назначения (рис.3.5, а).



.а)



.б)

Рис.3.5. Многомодовое (а) и одномодовое (б) волокно

Эти составляющие лучей света называются модами. Возникновение мод в оптическом волокне возможно, если диаметр сердцевины сравнительно большой. Такое волокно называется многомодовым (multimode).

В стандартном многомодовом оптическом кабеле используется сердцевина диаметром 62,5 или 50 микрон и оболочка диаметром 125 микрон. Такие кабели обозначаются 62,5/125 или 50/125. Наличие многих мод приводит к появлению межмодовой дисперсии (размыву) передаваемого импульсного сигнала. Из-за дисперсии снижается скорость передачи данных, т.к. размытые импульсы накладываются друг на друга, и уменьшается расстояние, на которое можно передать данные. Для снижения влияния многих мод на величину дисперсии при большом диаметре сердцевины

разработано специальное многомодовое волокно с градиентным показателем преломления.

Одномодовое волокно (singlemode) имеет меньший диаметр сердцевины, что позволяет только одной моде луча света распространяться по сердцевине вдоль оси волокна. Диаметр сердцевины одномодового волокна уменьшен до значения восемь – десять микрон. Обычно одномодовое волокно маркируют следующим образом – 9/125. Это означает, что диаметр сердцевины составляет 9 микрон, а оболочки – 125 микрон. Одномодовое волокно более дорого по сравнению с многомодовым. Однако в одномодовых кабелях выше скорость передачи данных и больше расстояние, на которое могут быть переданы данные. Поэтому одномодовые кабели используется в локальных сетях для соединений между зданиями, а в технологиях линий SDH – для междугородней связи.

В одномодовом волокне межмодовая дисперсия отсутствует. Однако, оказывает влияние хроматическая дисперсия, которая характерна как для многомодового, так и для одномодового волокна. Хроматическая дисперсия возникает из-за того, что волны света разной длины проходят через оптическое волокно с несколько различными скоростями. В идеале источник света (светодиод или лазер) должны генерировать свет только одной частоты, тогда хроматической дисперсии не было бы. Однако лазеры и особенно светодиоды генерируют целый спектр частот (длин волн). Поэтому расстояние и скорость передачи данных ограничиваются дисперсией и затуханием сигнала в волокне.

В качестве источников света для оптических кабелей используются:

- Светодиоды, генерирующие инфракрасный свет с длиной волны 850 нм или 1310 нм. Светодиоды используются для передачи сигналов по многомодовому волокну на расстояние до 2000 м.
- Лазерные диоды, генерирующие инфракрасный луч света с длиной волны 1310 нм или 1550 нм. Лазеры используются с одномодовым волокном для передачи сигналов на большие расстояния в различных технологиях локальных и глобальных сетей.

Расстояние передачи сигналов в локальных сетях, определенное стандартом Gigabit Ethernet, составляет до 5 км, а стандартом 10Gigabit Ethernet – до 40 км.

Для приема оптических сигналов используют фотодиоды, которые преобразуют принятые оптические импульсы в электрические. Фотодиоды производятся для работы на длинах волн 850, 1310 или 1550 нм.

3.3. Беспроводная среда

Беспроводная среда образуется совокупностью радиоканалов, сгруппированных в несколько частотных диапазонах. Три частотных диапазона: 900 МГц, 2,4 ГГц и 5 ГГц, рекомендованы международным союзом телекоммуникаций (International Telecommunications Union – **ITU**) для использования в промышленности, науке и медицине (Industrial, Scientific, Medical – ISM) и не требуют лицензирования. В указанных частотных диапазонах и строится большинство беспроводных локальных и глобальных сетей связи. Более низкий частотный диапазон увеличивает расстояние передачи и улучшает распространение радиоволн внутри зданий. Однако число каналов и, следовательно, пользователей при этом снижается.

Техника модуляции широкополосных сигналов позволяют повысить помехозащищенность при сосредоточенных помехах высокого уровня и низком уровне сигнала. На практике широко используются технологии прямого последовательного расширения спектра (Direct Sequence Spread Spectrum – **DSSS**) и ортогонального частотного мультиплексирования (Orthogonal Frequency Division Multiplexing – **OFDM**). Устройства, использующие OFDM, имеют более высокую скорость передачи данных. Однако устройства с модуляцией DSSS – проще и дешевле. Мультиплексирование каналов производится на основе техники, называемой Множественным доступом с кодовым разделением (Code Division Multiple Access – **CDMA**).

В настоящее время широко применяются беспроводные сети, которые реализуют соединения абонентов через **точки беспроводного доступа** (Wireless Access Point – **WAP**). При этом абоненты (хосты) должны комплектоваться беспроводными сетевыми картами. В свою очередь, точки беспроводного доступа могут соединяться с другими сетевыми устройствами, например с коммутаторами, маршрутизаторами, посредством кабелей, образуя достаточно разветвленную сеть.

Беспроводная (wireless) среда регламентируется набором стандартов, которые различаются частотным диапазоном, скоростью передачи данных и расстоянием.

Стандарт IEEE 802.11 (**Wi-Fi**) является основным стандартом **беспроводных локальных сетей** (Wireless LAN – **WLAN**). Параметры беспроводных сетей в значительной мере определяются используемой техникой модуляции. Основные параметры технологий стандарта 802.11 (Wi-Fi) приведены в табл. 3.2.

Таблица 3.2

Параметры стандартов Wi-Fi беспроводной среды передачи

Стандарт (Частотный диапазон)	Скорость передачи, Мбит/с	Типовое значен, Мбит/с	Макс. значение, Мбит/с
802.11a (5 ГГц)	54	20 – 26	108
802.11b (2.4 ГГц)	11	2 – 4	11
802.11g (2.4 ГГц)	54	20 – 26	108
802.11n (2.4, 5 ГГц)	100		210

Стандарт IEEE 802.11a регламентирует работу устройств WLAN в частотном диапазоне 5 ГГц. Скорость передачи – до 54 Мбит/с, а в некоторых случаях – до 108 Мбит/с. В производственных технологических сетях, скорость передачи обычно оценивается в 20-26 Мбит/с. Использование высокочастотного диапазона 5 ГГц стандарта 802.11a ограничивает расстояние передачи и распространение радиоволн внутри зданий. Используемый вид модуляции – OFDM. Устройства стандарта 802.11a не могут взаимодействовать с устройствами стандарта 802.11b и 802.11g, поскольку последние работают в диапазоне 2,4 ГГц.

В настоящее время устройства стандарта 802.11b и 802.11g получили широкое распространение. Устройства стандарта 802.11b функционируют в частотном диапазоне 2,4 ГГц и характеризуется скоростью передачи до 11 Мбит/с, вид модуляции – DSSS.

Устройства стандарта 802.11g являются совместимыми с устройствами 802.11b, поскольку работают в том же частотном диапазоне 2,4 ГГц. В устройствах этого стандарта может использоваться как техника модуляции OFDM, так и DSSS. При технике модуляции OFDM скорость передачи данных такая же, как в устройствах стандарта 802.11a (до 54 Мбит/с). При технике модуляции DSSS скорость передачи данных – до 11 Мбит/с. В

настоящее время разработаны точки доступа, которые позволяют устройствам стандартов 802.11b и 802.11a сосуществовать в одной беспроводной сети WLAN. Точка доступа предоставляет услуги шлюза (gateway) для связи устройств двух разных стандартов. Более низкий частотный диапазон увеличивает расстояние передачи и улучшает распространение радиоволн внутри зданий по сравнению с 802.11a.

Достоинства частотного диапазона 2,4 ГГц обусловили большое количество пользователей, что приводит к его перегрузке и взаимному влиянию устройств.

Новые устройства стандарта 802.11n способны работать как в частотном диапазоне 5 ГГц, так и 2,4 ГГц. Значение скорости передачи от 100 до 210 Мбит/с.

Помимо сетей вышеприведенных стандартов создаются и эксплуатируются сети стандарта IEEE 802.15 (Wireless Personal Area Network – WPAN) или "Bluetooth", которые являются примером персональных сетей (Personal Area Network – PAN). Кроме того, сети стандарт IEEE 802.16 (Worldwide Interoperability for Microwave Access – WiMAX), которые обеспечивают широкополосную связь на значительно большее расстояние по сравнению с вышеприведенными технологиями.

3.4. Топология сетей

Объединение сетевых узлов и станций в сеть связи реализуется на основе различных топологий. Топологии локальных и глобальных сетей различаются.

Следует различать физическую и логическую топологии сети**.** **Физическая топология** представляет собой наиболее общую структуру сети и отображает схему соединения сетевых элементов кабелями связи. **Логическая топология** показывает, как по сети передаются определенные единицы информации.

В локальных сетях наибольшее распространение получили следующие физические топологии (рис.3.6): шина (bus), звезда (star), расширенная звезда

(extended star), кольцо (ring), а также полносвязная топология, где все узлы связаны между собой (mesh topology) индивидуальными линиями.

Разделяемая (shared) линия или среда передачи данных, когда пользователи делят линии связи между собой, снижает стоимость сети. Но в каждый момент времени линией может пользоваться только одна пара абонентов, из-за чего могут возникнуть очереди, а также коллизии.

Топология на основе шины (bus) характеризуется тем, что передачу данных в данный момент времени может вести только один узел. Ожидание своей очереди на передачу данных является недостатком топологии. При выходе какого-то узла из строя вся остальная сеть будет функционировать без изменений. Другими достоинствами топологии являются экономное расходование кабеля, простота, надежность и легкость расширения сети.

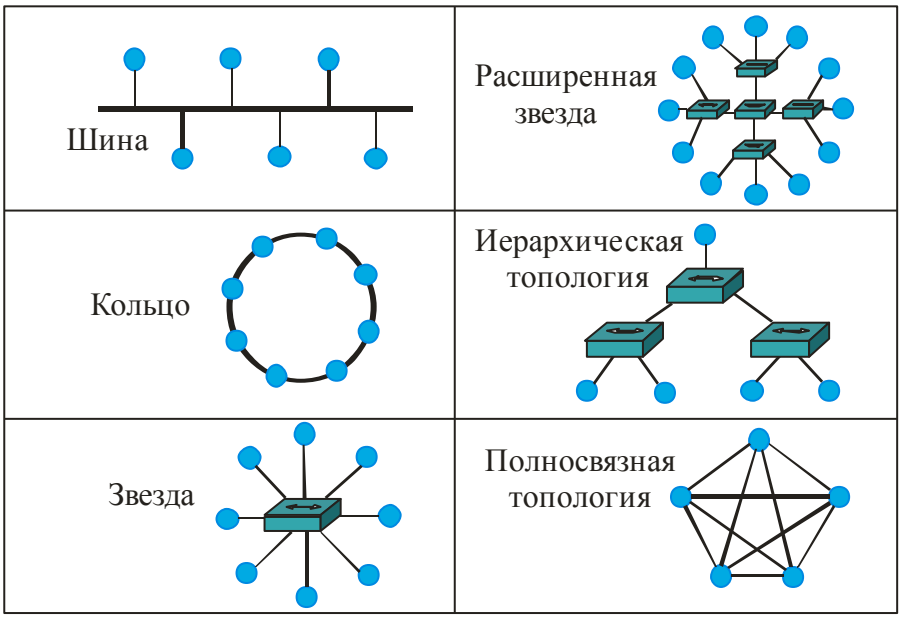


Рис.3.6. Физические топологии локальных сетей

Топология на основе звезды (star) требует применения центрального устройства. Выход из стоя одного узла не повлияет на работоспособность остальной сети. Сеть легко модифицируется путем подключения новых узлов. Из недостатков можно отметить уязвимость центра и увеличенный расход кабеля по сравнению с шинной топологией.

При использовании **топологии кольцо** (ring) сигналы передаются в одном направлении от узла к узлу. При выходе из стоя любого узла,

прекращается функционирование всей сети, если не предусмотрен обход вышедшего из строя узла.

Логическая топология сети определяет, как узлы общаются через среду, т.е. как обеспечивается управление доступом к среде. Наиболее известные логические топологии: «точка-точка» (point-to-point), множественного доступа (multi access), широковещательная (broadcast) и маркерная (token passing).

Логическая топология «точка-точка» обеспечивает передачу данных от одного узла до другого, не зависимо от промежуточных устройств между ними. Протокол управления передачей данных при такой топологии может быть очень простым, поскольку другие адресаты отсутствуют. Следовательно, при использовании этой топологии не требуются физические адреса.

Топология **множественного доступа** характерна для Ethernet-сетей, реализованных на многопортовых повторителях (hub). Доступ к разделяемой общей шине имеют все узлы, но в каждый момент времени передавать данные может только один узел. При этом остальные узлы могут только «слушать».

Использование **широковещательной** топологии определяет, что узел посылает свои данные всем другим узлам сетевой среды. При этом не известно, какие станции функционируют.

Маркерная логическая топология, также как топология множественного доступа реализует разделение общей среды. Однако, если в топологии multi access Ethernet-сетей доступ к среде случайный (не детерминированный), то в маркерной топологии доступ к среде **детерминированный**. Электронный **маркер** (token) последовательно передается каждому узлу по кольцу. Узел, получивший маркер, может передавать данные в сеть. Если в узле нет данных для передачи, то он передает маркер следующему узлу и процесс повторяется. Топологию token passing используют сети: Token Ring и Fiber Distributed Data Interface (FDDI).

Физическая и логическая топологии сети могут быть одинаковыми или разными. Например, широко известная сетевая технология Ethernet может использовать концентраторы (**hub**) и кабель “витая пара” (рис.3.7). **Физическая** топология на рис.3.7 представляет собой **звезду**, поскольку все компьютеры подключены к центральному устройству – концентратору (hub).

Логическая же топология – **шина**, поскольку внутри концентратора все компьютеры подсоединены к общей магистрали.

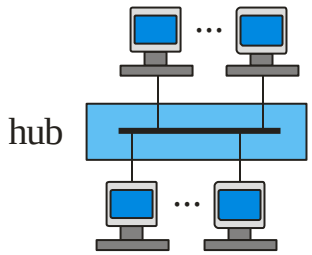


Рис.3.7. Топология: физическая – звезда, логическая – шина

На практике широко используется комбинация топологий. Например, (рис.3.8) ядро сети содержит узлы коммутации (УК1,…УК5), объединенные для повышения надежности и отказоустойчивости по полносвязной топологии. В целом топология сети представляет собой расширенную звезду или радиально-узловой способ построения сети, когда оконечные пункты (ОП) подключены к узлам У, которые в свою очередь, соединены с узлами коммутации УК ядра сети.

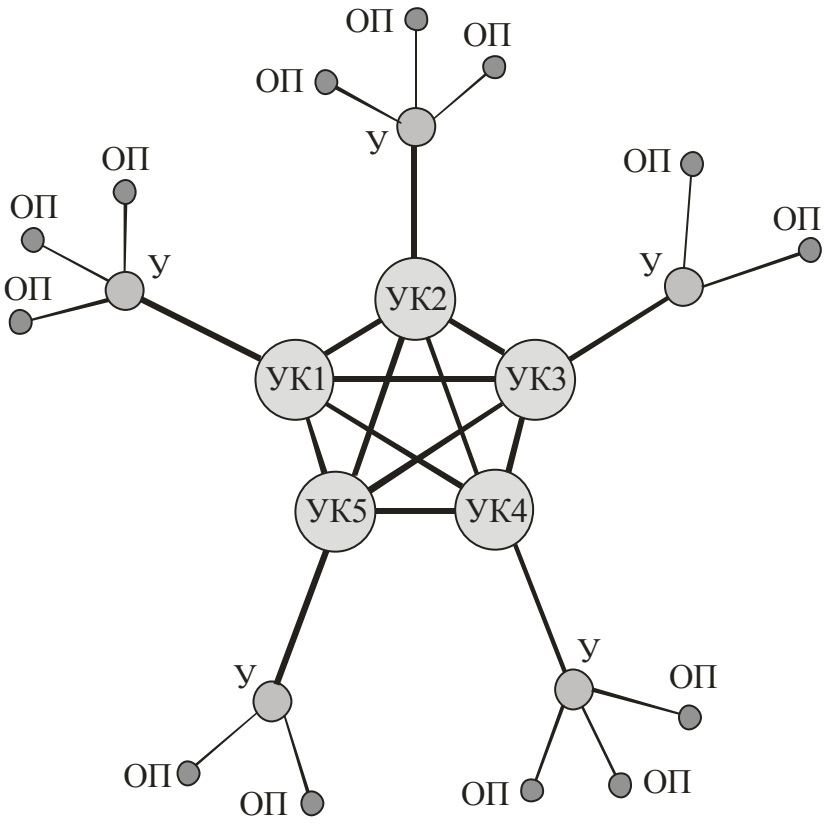


Рис.3.8. Сеть связи с комбинированной топологией

Краткие итоги лекции 3

1. В качестве среды передачи в сетях передачи данных используют коаксиальный кабель, неэкранированную UTP и экранированную STP витую пару (симметричный кабель), оптоволоконный кабель, беспроводные радиоканалы.
2. Кабель UTP содержит четыре пары свитых медных проводов, поэтому используется разъем (коннектор) RJ-45, имеющий 8 контактов.
3. Кабель UTP широко используется в локальных сетях Ethernet, Fast Ethernet, Gigabit Ethernet, обеспечивая передачу сигналов на расстояние до 100 м.
4. Для соединения устройств между собой используются прямой, кроссовый и консольный кабели.
5. Волоконно-оптические кабели характеризуются отсутствием перекрестных помех и электромагнитных помех от внешних источников. Это позволяет передавать сигналы на большее расстояние по сравнению с симметричным медным кабелем.
6. Одномодовое волокно оптических кабелей по сравнению с многомодовым позволяет передавать данные на большее расстояние с более высокой скоростью.
7. Передача данных по оптическому волокну производится на длинах волн 850, 1310 или 1550 нм.
8. Беспроводная среда образуется совокупностью радиоканалов, сгруппированных в частотных диапазонах 900 МГц; 2,4 ГГц и 5 ГГц.
9. Стандарт IEEE 802.11 (Wi-Fi) является основным стандартом беспроводных локальных сетей.
10. Объединение сетевых узлов и станций в сеть связи реализуется на основе различных топологий. Следует различать физическую и логическую топологии сети.

Вопросы по лекции 3

1. Какие типы кабелей используются в локальных сетях передачи данных?
2. Какова скорость и дальность передачи кабеля UTP 3 категории?
3. Какова скорость и дальность передачи кабеля UTP 5, 5e категории?
4. Для соединения, каких устройств используется прямой кабель?
5. Для соединения, каких устройств используется кроссовый кабель?
6. Для соединения, каких устройств используется консольный кабель?
7. В чем преимущества волоконно-оптического кабеля перед медным?
8. На какое расстояние можно передавать сигналы в локальных сетях по оптическому кабелю?
9. На каких длинах волн производится передача сигналов по оптическому кабелю?
10. Какие частотные диапазоны рекомендованы для использования в промышленности, науке и медицине и не требуют лицензирования.?
11. Какой стандарт является основным в беспроводных локальных сетях?
12. Какой стандарт предусматривает передачу данных в диапазоне 5 ГГц со скоростью до 54 Мбит/с?
13. Какой стандарт предусматривает передачу данных в диапазоне 2,4 ГГц со скоростью до 54 Мбит/с?
14. Какие топологии получили наибольшее распространение в локальных сетях?
15. Каковы достоинства и недостатки топологии «общая шина»?
16. Каковы достоинства и недостатки топологии «звезда»?
17. В чем различие физической и логической топологий?
18. К какому виду относится топология множественного доступа, для каких сетей она характерна?

Упражнения

1. Укажите скорости и дальность передачи симметричных медных кабелей.
2. Изобразите схемы прямого, кроссового и консольного кабелей.
3. Объясните условия, при которых возникает полное внутреннее отражение в волокне оптического кабеля.
4. Укажите основные параметры стандартов Wi-Fi беспроводной среды передачи.
5. Изобразите основные физические топологии локальных сетей.
6. Приведите пример, когда при одинаковой структурной схеме сети физическая и логическая топологии будут различны.

Контрольный тест по разделу 1

Задача 1.1
Вариант 1 Задачи 1.1

1. Какие сети при передаче данных используют технологию виртуальных каналов? (выбрать два ответа)
   - Frame Relay
   - PDH
   - xDSL
   - SDH
   - IP
   - ISDN
   - ATM

Вариант 2 Задачи 1.1

2. Какие сети при передаче данных используют коммутацию пакетов? (выбрать 2 ответа)
   - PDH
   - xDSL
   - SDH
   - IP
   - ATM

Вариант 3 Задачи 1.1

3. К технологиям локальных сетей относятся: (выбрать три ответа)
   - Token Ring
   - PDH
   - Ethernet
   - SDH
   - IP
   - ISDN
   - 10GEthernet

Задача 1.2
Вариант 1 Задачи 1.2

4. Что характеризует инкапсуляцию на канальном уровне? (выбрать два ответа)
   - Пакеты инкапсулируются в кадры
   - Данные помещаются в пакеты
   - Данные «нарезаются» на сегменты
   - Последовательность битов преобразуется для межсетевого уровня
   - Присоединяются физические адреса, чтобы идентифицировать непосредственно присоединенные устройства

Вариант 2 Задачи 1.2

5. Что характеризует канальный уровень? (выбрать три ответа)
   - Это соединение для передачи данных на транспортном уровне
   - Происходит инкапсуляция кадров в пакеты
   - Обеспечивает услуги для сетевого уровня
   - Происходит инкапсуляция информации сетевого уровня в кадры
   - Заголовок содержит физический адрес

Вариант 3 Задачи 1.2

6. На каком уровне OSI модели формируются сегменты?
Приложений
Сеансовый
Транспортный
Межсетевой
Сетевой
Канальный
Физический

Задача 1.3
Вариант 1 Задачи 1.3

7. Название какого уровня имеется как в OSI, так и в TCP/IP модели, но имеет разные функции?
Транспортный
Сеансовый
Приложений
Межсетевой
Физический
Сетевой
Канальный

Вариант 2 Задачи 1.3

8. Какие уровни моделей OSI и TCP/IP имеют одинаковые функции и различные названия? (выбрать два ответа)
Транспортный
Сеансовый
Приложений
Межсетевой
Физический
Сетевой
Канальный

Вариант 3 Задачи 1.3

9. На каком уровне модели OSI функционируют сетевые карты? (выбрать два ответа)
Транспортный
Сеансовый
Приложений
Межсетевой
Физический
Сетевой
Канальный

Задача 1.4
Вариант 1 Задачи 1.4

10. Какие устройства функционируют на канальном уровне модели OSI? (выбрать 2 ответа)

Повторители
Коммутаторы
Мосты
Маршрутизаторы
Многопортовые повторители (hub)

Вариант 2 Задачи 1.4

11. Какие устройства функционируют на сетевом уровне модели OSI?
Повторители
Коммутаторы
Мосты
Маршрутизаторы
Многопортовые повторители (hub)

Вариант 3 Задачи 1.4

12. Какие устройства функционируют на физическом уровне модели OSI? (выбрать 2 ответа)
Повторители
Коммутаторы
Мосты
Маршрутизаторы
Многопортовые повторители (hub)

Задача 1.5
Вариант 1 Задачи 1.5

13. Адрес 172.30.201.17 является:
+ Логическим
Физическим
Номером порта
Почтовым адресом
MAC-адресом

Вариант 2 Задачи 1.5

14. Адрес 0005.A869.CD-F1 является:
Логическим
Физическим
Номером порта
Почтовым адресом
IP-адресом

Вариант 3 Задачи 1.5

15. Приложения и службы уровня приложений адресуются:
Логическим IP-адресом
Физическим MAC-адресом
Номером порта
Совокупностью IP-адреса и MAC-адреса

Задача 1.6
Вариант 1 Задачи 1.6

16. Процесс повторной передачи источником информации неподтвержденного сообщения реализует следующий уровень модели OSI:

Прикладной
Представительский
Сеансовый
Транспортный
Сетевой
Канальный

Вариант 2 Задачи 1.6

17. Обеспечить надежную, ориентированную на предварительное соединение передачу данных между двумя узлами может следующий уровень модели OSI:

Прикладной
Представительский
Сеансовый
Транспортный
Сетевой
Канальный

Вариант 3 Задачи 1.6

18. Для управления потоками данных между узлами (источника и назначения) транспортный уровень использует: (выбрать три ответа)

Номер порта
Значение контрольной суммы
Ключи аутентификации
Номер последовательности
Алгоритм криптографирования
Номер подтверждения

Задача 1.7
Вариант 1 Задачи 1.7

19. Особенности протокола UDP: (выбрать три ответа)

Не гарантирует доставку дейтаграмм
Является протоколом типа connection-oriented
Обеспечивает надежную полнодуплексную передачу
Надежность обеспечивается уровнем приложений
Является протоколом типа connectionless
Использует технику скользящего окна

Вариант 2 Задачи 1.7

20. Если на транспортном уровне не используется контроль потока, а для надежности полагаются на протокол верхнего уровня, то используются следующие протокол и метод:

UDP, connection-oriented
UDP, connectionless
TCP, connection-oriented
TCP, connectionless

Вариант 3 Задачи 1.7

21. Одной из основных обязанностей транспортного уровня модели OSI является:
    Выбор маршрута
    Контроль потока данных
    Управление безопасностью
    Сжатие данных
    Криптографирование данных

Задача 1.8
Вариант 1 Задачи 1.8

22. Термин connection-oriented относительно протокола TCP означает:
    TCP использует только соединения LAN
    TCP работает только с непосредственно соединенными устройствами
    TCP договаривается о сессии для передачи данных между узлами
    TCP вновь собирает целое сообщение из частей данных в порядке их получения

Вариант 2 Задачи 1.8

23. Номер последовательности в заголовке сегмента используется:
    Для объединения частей данных в корректном порядке в устройстве назначения.
    Для идентификации протокола прикладного уровня.
    Чтобы показать количество байт, передаваемых в течение одной сессии
    Чтобы указать номер байта, которым закончилась передача предыдущей порции данных.

Вариант 3 Задачи 1.8

24. Номер порта TCP/UDP позволяет:
    Указывать начало процесса three-way handshake
    Переустанавливать сегменты в правильном порядке
    Идентифицировать номер пакета данных, который может быть послан без подтверждения
    Адресовать приложение, обрабатывающее данное сообщение

Задача 1.9
Вариант 1 Задачи 1.9

25. Какие разъемы используются для подключения консольного порта маршрутизатора к компьютеру? (выбрать два ответа)
    RJ-11
    RJ-12
    RJ-45
    DB-8
    DB-9
    DB-10

Вариант 2 Задачи 1.9

26. Какие провода и разъемы находятся в кабеле UTP?
    4 пары свитых экранированных медных проводов и разъем RJ-45
    4 пары свитых неэкранированных медных проводов и разъем RJ-11
    2 пары свитых неэкранированных медных проводов и разъем RJ-45

8 пар свитых экранированных медных проводов и разъем RJ-11
4 пары свитых неэкранированных медных проводов и разъем RJ-45

Вариант 3 Задачи 1.9

27. Какой кабель преимущественно используется в настоящее время в локальных сетях?
Тонкий коаксиальный
Толстый коаксиальный
Симметричный экранированный
Симметричный неэкранированный
Волоконно-оптический одномодовый

Задача 1.10
Вариант 1 Задачи 1.10

28. Для связи между компьютером и консольным портом коммутатора используют следующий кабель:
Прямой (straight-through)
STP – экранированный
Кроссовый (crossover)
Консольный (rollover)
Волоконно-оптический

Вариант 2 Задачи 1.10

29. Прямой кабель (straight-through) используется для соединения: (выбрать три ответа)
Коммутатора с маршрутизатором
Коммутатора с коммутатором
Коммутатора с концентратором
Коммутатора с компьютером или сервером
Концентратора с компьютером или сервером
Маршрутизатора с компьютером

Вариант 3 Задачи 1.10

30. Кроссовый кабель используется для соединения: (выбрать три ответа)
Коммутатора с маршрутизатором
Коммутатора с концентратором
Коммутатора с компьютером или сервером
Концентратора с компьютером или сервером
Маршрутизатора с компьютером
Коммутатора с коммутатором

Задача 1.11
Вариант 1 Задачи 1.11

31. Почему при связи между зданиями оптический кабель предпочтительней медного? (выбрать два ответа)
Более дешевый
Меньше затухание
Нет перекрестных помех и взаимного влияния между волокнами
Легче монтаж и установка разъемов

Вариант 2 Задачи 1.11

32. Диаметр сердцевины одномодового оптического волокна составляет: (выбрать 2 ответа)

8 мкм
125 мкм
50 мкм
62,5 мкм
10 мкм

Вариант 3 Задачи 1.11

33. Одномодовое оптическое волокно по сравнению с многомодовым обеспечивает передачу данных:

На большее расстояние с меньшей скоростью
На большее расстояние с большей скоростью
На меньшее расстояние с большей скоростью
На меньшее расстояние с меньшей скоростью

Задача 1.12
Вариант 1 Задачи 1.12

34. Какой стандарт позволяет передавать данные без проводов с максимальной скоростью до 11Мбит/с?

802.11a
802.11b
802.11c
802.11g

Вариант 2 Задачи 1.12

35. Какая максимальная скорость передачи обеспечивается стандартом 802.11a?

11 Mbps
27 Mbps
54 Mbps
81 Mbps

Вариант 3 Задачи 1.12

36. В диапазоне 2,4 ГГц функционируют технологии: (выбрать два ответа)

802.11a
802.11b
802.11c
802.11g

Раздел 2. ЛОКАЛЬНЫЕ СЕТИ

Лекция 4. КАНАЛЬНЫЙ УРОВЕНЬ

Краткая аннотация лекции: приведено описание верхнего подуровня логической передачи данных LLC и нижнего подуровня управления доступом к среде MAC канального уровня модели OSI; даны основные характеристики технологии Ethernet; проведен сравнительный анализ режимов работы коммутаторов.
Цель лекции: изучить функции элементов и устройств канального уровня модели OSI.

4.1. Подуровни LLC и MAC

Канальный уровень (Data Link) обеспечивает обмен данными через общую локальную среду. Он находится между сетевым и физическим уровнями модели OSI. Поэтому канальный уровень должен предоставлять сервис вышележащему уровню, взаимодействуя с сетевым протоколом и обеспечивая инкапсулированным в кадр пакетам доступ к сетевой среде. В то же время, канальный уровень управляет процессом размещения передаваемых данных в физической среде. Поэтому канальный уровень разделен на 2 подуровня (рис.4.1): верхний подуровень **управления логическим каналом передачи данных** (Logical Link Control – **LLC**), являющийся общим для всех технологий, и нижний подуровень **управления доступом к среде** (Media Access Control – **MAC**). Кроме того, на канальном уровне обнаруживают ошибки в передаваемых данных.

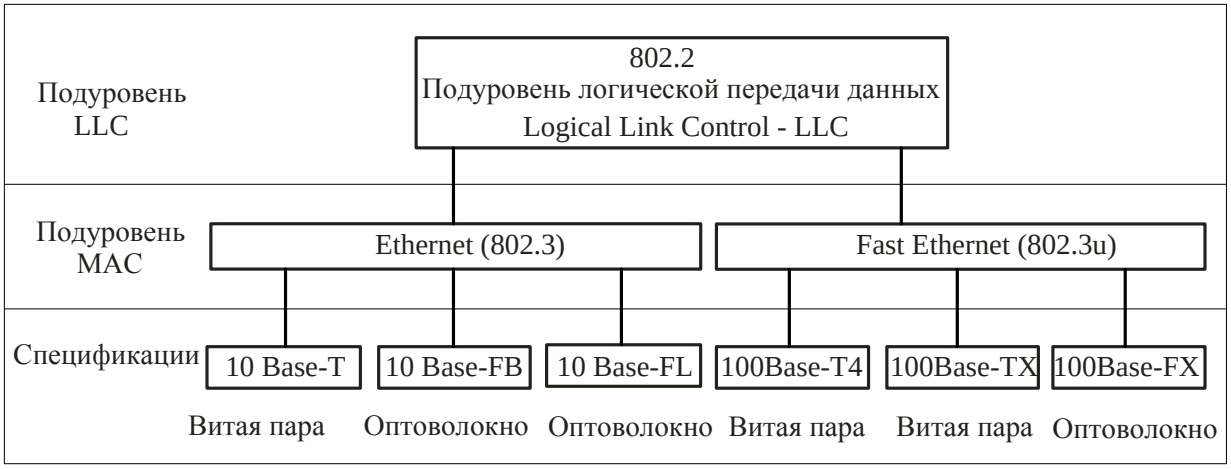


Рис. 4.1. Подуровни канального уровня

Взаимодействие узлов локальных сетей происходит на основе протоколов канального уровня. Международным институтом инженеров по электротехнике и радиоэлектронике (Institute of Electrical and Electronics Engineers – **IEEE**) было разработано семейство стандартов 802.x, которое регламентирует функционирование канального и физического уровней семиуровневой модели ISO/OSI. Ряд этих протоколов являются общими для всех технологий, например, стандарт 802.2, другие протоколы (например, 802.3, 802.3u, 802.5) определяют особенности технологий локальных сетей.

На **подуровне LLC** существует несколько процедур, которые позволяют устанавливать или не устанавливать связь перед передачей кадров, содержащих данные, восстанавливать или не восстанавливать кадры при их потере или обнаружении ошибок. Этот подуровень реализует связь с протоколами сетевого уровня. Связь с сетевым уровнем и определение логических процедур передачи кадров по сети реализует протокол 802.2. Протокол 802.1 дает общие определения локальных вычислительных сетей, связь с моделью ISO/OSI. Существуют также модификации этого протокола, которые будут рассмотрены позже в лекции 15.

Подуровень MAC определяет особенности доступа к физической среде при использовании различных технологий локальных сетей. Протоколы MAC-уровня ориентированы на совместное использование физической среды абонентами. Разделяемая среда (shared media) используется в таких широко распространенных в локальных сетях технологиях как Ethernet, Fast Ethernet, Gigabit Ethernet, Token Ring, FDDI. Использование разделяемой между пользователями среды улучшает загрузку канала связи, удешевляет сеть, но снижает скорость передачи данных между узлами.

Каждой технологии MAC-уровня соответствует несколько вариантов (спецификаций) протоколов физического уровня (рис.4.1). **Спецификация** технологии MAC-уровня – определяет среду физического уровня и основные параметры передачи данных (скорость передачи, вид среды, узкополосная или широкополосная).

Так протоколу **802.3**, описывающему известную технологию **Ethernet**, соответствуют спецификации физического уровня: 10Base-T, 10Base-FB, 10Base-FL. Число 10 показывает, что скорость передачи данных составляет 10 Мбит/с, Base – система узкополосная. Спецификация 10Base-T

предусматривает построение локальной сети на основе использования неэкранированной витой пары UTP не ниже 3 категории и концентратора. Спецификации 10Base-FB, 10Base-FL используют волоконно-оптические кабели. Более ранние спецификации 10Base-5 и 10Base-2 предусматривали использование “толстого” или “тонкого” коаксиального кабеля.

Протоколу Fast Ethernet (802.3u) соответствуют следующие спецификации физического уровня:

- 100Base-T4, где используется четыре витых пары кабеля UTP не ниже 3 категории;
- 100Base-TX – применяется две пары кабеля UTP не ниже 5 категории;
- 100Base-FX – используются волокна многомодового оптического кабеля.

Помимо Ethernet и Fast Ethernet на MAC уровне используется еще ряд технологий: Gigabit Ethernet со скоростью передачи 1000 Мбит/с – стандарты 802.3z и 802.3ab; 10Gigabit Ethernet со скоростью передачи 10000 Мбит/с – стандарт 802.3ae, а также ряд других. Например, протокол 802.5 описывает технологию сетей Token Ring, где в качестве физической среды используется экранированная витая пара STP, с помощью которой все станции сети соединяются в кольцевую структуру. В отличие от технологии Ethernet в сетях с передачей маркера (Token Ring) реализуется не случайный, а детерминированный доступ к среде с помощью кадра специального формата – маркера (token). Сети Token Ring позволяют передавать данные по кольцу со скоростями либо 4 Мбит/с, либо 16 Мбит/с. По сравнению с Ethernet технология Token Ring более сложная и надежная, однако, Token Ring не совместима с новыми технологиями Fast Ethernet, Gigabit Ethernet, 10Gigabit Ethernet. Технологии Ethernet и совместимые с ними и рассматриваются в настоящем курсе лекций.

Передаваемый в сеть пакет инкапсулируется в поле данных кадра протокола LLC, формат которого приведен на рис.4.2.

Флаг	DSAP	SSAP	Control	Data	Флаг
01111110	1 байт	1 байт	1-2 байта	46 - 1497 байт	01111110

Рис. 4.2. Формат кадра LLC

Флаги определяют границы кадра LLC. В поле данных (Data) размещаются пакеты сетевых протоколов. Поле адреса точки входа службы назначения (**DSAP** – Destination Service Access Point) и адреса точки входа службы источника (**SSAP** – Source Service Access Point) длиной по 1 байту адресуют службу верхнего уровня, которая передает и принимает пакет данных. Например, служба IP имеет значение SAP равное 0x6. Обычно это одинаковые адреса. Адреса DSAP и SSAP могут различаться только в том случае, если служба имеет несколько адресов точек входа. Таким образом, адреса DSAP и SSAP не являются адресами узла назначения и узла источника, да и не могут быть таковыми, поскольку поле длиной 1 байт позволяет адресовать только 256 точек, а узлов в сети может быть много.

Поле управления (Control) имеет длину 1 или 2 байта в зависимости от того, какой тип кадра передается: информационный (Information), управляющий (Supervisory), ненумерованный (Unnumbered). У первых двух длина поля Control составляет 2 байта, у ненумерованного – 1 байт. Тип кадра определяется процедурой управления логическим каналом LLC. Стандартом 802.2 предусмотрено 3 типа таких процедур:

LLC1 – процедура без установления соединения и подтверждения;

LLC2 – процедура с установлением соединения и подтверждением;

LLC3 – процедура без установления соединения, но с подтверждением.

Процедура **LLC1** используется при **дейтаграммном** режиме передачи данных. Для передачи данных используются ненумерованные кадры. Восстановление принятых с ошибками данных производят протоколы верхних уровней, например, протокол транспортного уровня или протокол уровня приложений. В дейтаграммном режиме функционирует, например, протокол IP.

Процедура **LLC2** перед началом передачи данных устанавливает соединение, послав соответствующий запрос и получив подтверждение, после чего передаются данные. Процедура позволяет восстанавливать потерянные и исправлять ошибочные данные, используя режим скользящего окна. Для этих целей она использует три типа кадров (информационные, управляющие, ненумерованные). Данная процедура более сложная и менее быстродействующая по сравнению с LLC1, поэтому она используется в локальных сетях значительно реже, чем LLC1, например, протоколом NetBIOS/NetBEUI.

Широкое применение процедура, подобная LLC2, получила в глобальных сетях для надежной передачи данных по ненадежным линиям связи. Например, она используется в протоколе LAP-B сетей X.25, в протоколе LAP-D сетей ISDN, в протоколе LAP-M сетей с модемами, частично – в протоколе LAP-F сетей Frame Relay.

Процедура LLC3 используется в системах управления технологическими процессами, когда необходимо высокое быстродействие и знание того, дошла ли управляющая информация до объекта.

Наиболее широкое распространение в локальных сетях получила процедура LLC1, в которой используются только ненумерованные типы кадров.

На передающей стороне кадр LLC уровня передается на MAC-уровень, где инкапсулируется в кадр соответствующей технологии данного уровня. При этом флаги кадра LLC отбрасываются. Технология Ethernet предусматривает кадры четырех форматов, которые незначительно отличаются друг от друга. На рис.4.3 приведен формат кадра стандарта 802.3/LLC.

Преамбула	SFD	DA	SA	L	DSAP	SSAP	Control	Data	FCS
7 байт	10101011	6 байт	6 байт	2 байта	1 байт	1 байт	1 байт	46 - 1497 байт	4 байта

Рис.4.3. Формат кадра Ethernet 802.3/LLC

Преамбула кадра состоит из семи байт 10101010, необходимых для вхождения приемника в режим синхронизации. Начальный ограничитель кадра (Start of Frame Delimiter - SFD) – 10101011 вместе с преамбулой в итоге составляют 8 байт. Далее следуют физические адреса узла назначения (DA – Destination Address) и узла источника (SA – Source Address). В технологиях Ethernet физические адреса получили название **MAC-адрес**ов. Они содержат 48 двоичных разрядов и представляются в шестнадцатеричной системе. В локальных сетях адресация узлов производится на основе MAC-адресов, которые «прошиты» в ПЗУ сетевых карт.

Адрес, состоящий из всех единиц FFFFFFFFFFFF, является широковещательным адресом (broadcast), когда передаваемая в кадре информация предназначена всем узлам локальной сети.

Младшие 24 разряда MAC-адреса (6 шестнадцатеричных разрядов) задают уникальный номер оборудования, например, номер сетевой карты. Следующие 22 разряда задают идентификатор производителя оборудования. Старший бит равный 0 указывает на то, что адрес является индивидуальным, а равный 1 – адрес является групповым. Второй старший бит равный 0 указывает, что идентификатор задан централизованно комитетом IEEE. В стандартной аппаратуре Ethernet идентификатор всегда задан централизованно. Например, MAC-адрес 11:5D:73:A5:00:4B является индивидуальным, заданным централизовано. Несмотря на то, что в MAC-адресе выделена старшая и младшая части, он считается **плоским** (flat).

Поле L (рис.4.3) определяет длину поля данных Data, которое может быть от 46 до 1497 байт (в информационных кадрах процедуры LLC2 – до 1496 байт, поскольку поле Control – 2 байта). Если поле данных меньше 46 байт, то оно дополняется до 46 байт.

В настоящее время используется, главным образом, формат кадра стандарта Ethernet II, в котором вместо поля L задается поле типа **T**, где указан протокол сетевого уровня. Например, при использовании на сетевом уровне протокола IPv4 шестнадцатеричное значение поля T будет 0×0800. В случае передачи кадра протокола ARP значение поля T – 0×0806. Остальные поля кадра Ethernet II идентичны кадру стандарта 802.3.

Поле контрольной суммы (FCS – Frame Check Sequence) длиной в 4 байта позволяет определить наличие ошибок в полученном кадре, за счет использования алгоритма проверки на основе циклического кода.

4.2. Локальные сети технологии Ethernet

В сетях технологии Ethernet, построенных на основе логической топологии “общая шина”, разделяемая среда передачи данных является общей для всех пользователей, т.е. реализуется множественный доступ к общей среде. Для передачи данных используется манчестерский код, скорость передачи составляет 10 Мбит/с, т.е. длительность битового интервала равна 0,1 мкс. Между кадрами должен быть интервал длительностью 9,6 мкс. Переданную в сеть информацию может получить любой компьютер, у которого адрес сетевого адаптера совпадает с адресом

DA передаваемого кадра, или все компьютеры сети при широковещательной передаче. Однако передавать информацию в любой момент времени может только один узел. Такой способ обмена данными получил название метода **множественного доступа к среде с контролем несущей и обнаружением коллизий** (Carrier Sence Multiply Access with Collision Detection – **CSMA/CD**), суть которого объясняется ниже.

При одновременной передаче данных двумя компьютерами возникает так называемая **коллизия**, когда данные двух передающих узлов накладываются друг на друга и происходит потеря информации. Поэтому прежде чем начать передачу, узел должен убедиться, что общая шина свободна, для чего узел прослушивает среду. Если какой либо компьютер сети уже передает данные, то в сети обнаруживается несущая частота передаваемых сигналов. Если по окончании передачи сразу два узла попытаются одновременно начать передачу своих данных, то возникнет коллизия, которая фиксируется компьютерами. Узел, первым обнаруживший коллизию, усугубляет ее путем передачи в сеть специальных **JAM** сигналов для оповещения всех компьютеров сети. При этом компьютеры должны немедленно прекратить передачу данных и выдержать паузу в течение некоторого случайного интервала времени. По окончании этого интервала узел может вновь попытаться передать свои данные.

Длительность паузы составляет

$$\mathbf{T_п = T_{отс} \times L,}$$

где $T_{отс}$ – интервал отсрочки, равный 512 битовым интервалам, т.е. при скорости 10 Мбит/с интервал отсрочки $T_{отс}$ = 51,2 мкс;

L – случайное целое число, выбранное из диапазона $[0, 2^N]$, где N – номер повторной попытки передачи узлом данного кадра. N изменяется от 1 до 10. Всего повторных попыток передачи может быть 16, но после 10-ой попытки число N не увеличивается. Таким образом, L может принимать значения от 0 до 1024, а пауза $T_п$ = 0 – 52,4 мс. После 16-ой неудачной попытки, приведшей к коллизии, кадр отбрасывается.

Длительность передачи кадра $T_к$ должна быть больше максимально возможного времени обнаружения коллизии $T_{вок}$. В этом случае узел, начавший передачу и затем обнаруживший коллизию, сможет повторно передать кадр, хранящийся в буфере. В противном случае переданный кадр

теряется. Наихудший случай будет при передаче кадра минимальной длительности $T_{кmin}$, когда должно выполняться условие $T_{кmin} \geq T_{вок}$. Максимально возможное время обнаружения коллизии $T_{вок}$ определяется размерами сети (диаметром сети). $T_{вок\ макс}$ – это время, за которое сигнал передаваемого кадра дойдет до самого удаленного узла и сигнал о коллизии вернется обратно. Это время получило название удвоенной задержки распространения сигнала или значения задержки в пути (Path Delay Value – **PDV**).

С учетом условия $T_{кmin} \geq T_{вок}$, а также времени задержки сигналов в устройствах сетевых адаптеров и концентраторов, максимальный диаметр сети Ethernet установлен 2500 м, а минимальная длина кадра вместе с преамбулой – 72 байта. Поэтому минимальная длина поля данных составляет 46 байт, а максимальная длина поля данных – 1497 байт. Основные технические характеристики сети Ethernet сведены в табл.4.1.

Таблица 4.1

Основные технические характеристики сети Ethernet

Параметры	Значения
Скорость передачи данных	10 Мбит/с
Максимальное число станций в сети	1024
Максимальное расстояние между узлами	2500 м
Межкадровый интервал	9,6 мкс
Минимальная длина кадра	72 байта
Скорость передачи кадров минимальной длины	14880 кадров/с
Максимальная длина кадра	1526 байт
Скорость передачи кадров максимальной длины	813 кадров/с
Длина JAM последовательности	32 бита
Интервал отсрочки	51,2 мкс
Максимальное число попыток передачи	16
Длина случайной паузы после коллизии	0 – 52,4 мс

До недавнего времени сети Ethernet строились, как правило, на основе стандарта 10 Base-T, который в качестве разделяемой среды использует неэкранированную витую пару UTP и многопортовый повторитель hub (рис.4.4). Количество портов концентраторов разных типов варьируется от 8 до 72. Выход передатчика T_x сетевого адаптера соединяется со входом приемника R_x концентратора hub, который, в свою очередь, соединен со всеми портами повторителя. Вход приемника сетевого адаптера R_x соединен

с выходом передатчика концентратора T_x. Максимальное расстояние между сетевым адаптером и концентратором составляет 100 м. Таким образом, диаметр сети, выполненной на одном концентраторе, будет 200 м.

Для построения сети с большим числом узлов несколько концентраторов соединяют между собой, однако максимальное число концентраторов между двумя любыми компьютерами не должно быть больше 4. Требования к сети определяются правилом 5-4-3, в котором 5 – общее число сегментов сети, 4 – максимальное число концентраторов между любыми хостами, 3 – хосты могут быть только в трех сегментах. При этом диаметр сети может существенно увеличиться. Структура сети должна быть древовидной, петлевые соединения запрещены.

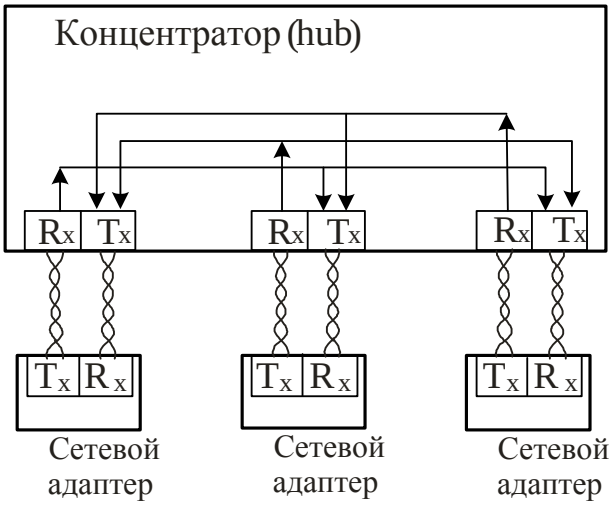


Рис.4.4. Сеть Ethernet стандарта 10 Base-T

Для реализации сетей максимального диаметра 2500 м используют оптоволоконный кабель, которым соединяют между собой концентраторы или узлы и концентраторы. Стандарт 10 Base-FB предписывает соединения только между концентраторами. Причем, между узлами сети может быть до 5 концентраторов, а диаметр сети может быть увеличен до 2740 м.

4.3. Коммутаторы в локальных сетях

Для предотвращения коллизий крупные локальные сети делятся на сегменты или домены коллизий, с помощью маршрутизаторов (routers) или коммутаторов (switches). Непосредственно к маршрутизатору конечные узлы (компьютеры) обычно не подключаются; подключение обычно выполняется

через коммутаторы. Каждый порт коммутатора оснащен процессором, память которого позволяет создавать буфер для хранения поступающих кадров. Общее управление процессорами портов осуществляет системный модуль.

Каждый сегмент, образованный портом (интерфейсом) коммутатора с присоединенным к нему узлом (компьютером) или с концентратором со многими узлами, является сегментом (доменом) коллизий. При возникновении коллизии в сети, реализованной на концентраторе, сигнал коллизии распространяется по всем портам концентратора. Однако на другие порты коммутатора сигнал коллизии не передается.

Существует два режима двусторонней связи: *полудуплексный* (*half-duplex*) и *полнодуплексный* (*full-duplex*). В полудуплексном режиме в любой момент времени одна станция может либо вести передачу, либо принимать данные. В полнодуплексном режиме абонент может одновременно принимать и передавать информацию, т.е. обе станции в соединении точка-точка, могут передавать данные в любое время, независимо от того, передает ли другая станция. Для разделяемой среды полудуплексный режим является обязательным. Ранее создававшиеся сети Ethernet на коаксиальном кабеле были только полудуплексными. Неэкранированная витая пара UTP и оптическое волокно могут использоваться в сетях, работающих в обоих режимах. Новые высокоскоростные сети 10-GigabitEthernet работают только в полнодуплексном режиме. Большинство коммутаторов могут использовать как полудуплексный, так и полнодуплексный режим.

В случае присоединения компьютеров (хостов) индивидуальными линиями к портам коммутатора каждый узел вместе с портом образует *микросегмент*. В сети, узлы которой соединены с коммутатором индивидуальными линиями, и работающей в полудуплексном режиме, возможны коллизии, если одновременно начнут работать передатчики коммутатора и сетевого адаптера узла.

В полнодуплексном режиме работы при микросегментации коллизий не возникает. При одновременной передаче данных от двух источников одному адресату буферизация кадров позволяет запомнить и передать кадры поочередно и, следовательно, избежать их потери. Отсутствие коллизий обусловило широкое применение топологии сети с индивидуальным подключением узлов к портам коммутатора.

Коммутатор является устройством канального уровня семиуровневой модели ISO OSI, где для адресации используются MAC-адреса (рис.4.5). Адресация происходит на основе MAC-адресов сетевых адаптеров узлов.

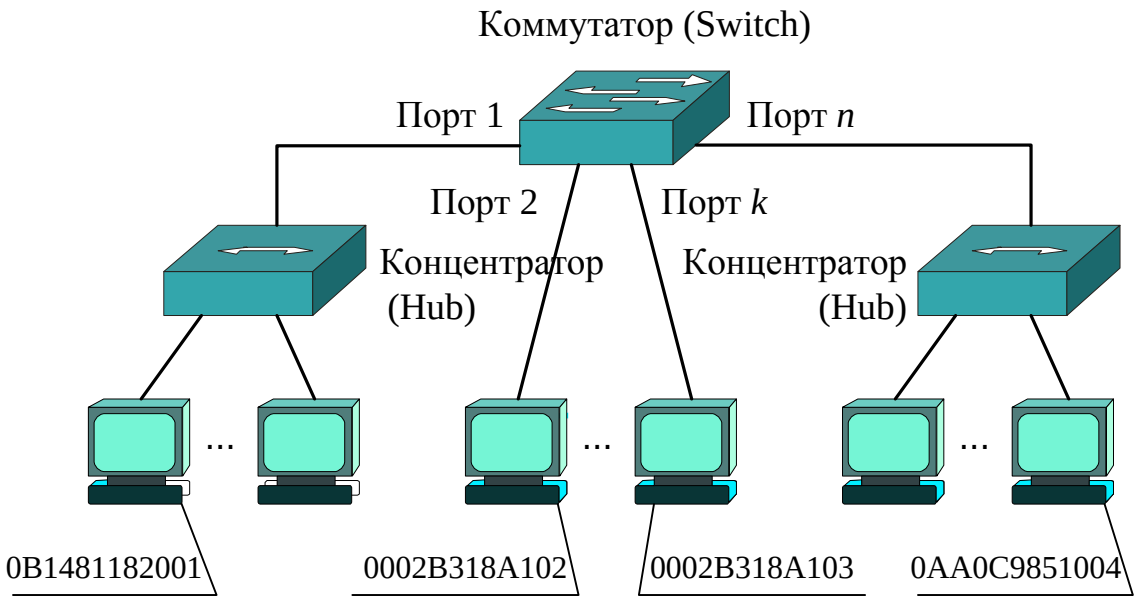


Рис.4.5. Сеть на базе коммутатора

Для передачи кадров используется алгоритм, определяемый стандартом 802.1D. Реализация алгоритма происходит за счет создания статических или динамических записей адресной таблицы коммутации. Статические записи таблицы создаются администратором. Важно отметить, что коммутатор можно не конфигурировать, он будет работать по умолчанию, создавая записи адресной таблицы в динамическом режиме. При этом в буферной памяти порта запоминаются все поступившие на порт кадры.

Первоначально в коммутаторе отсутствует информация о том, какие MAC-адреса имеют подключенные к портам узлы. Поэтому коммутатор, получив кадр, передает его на все свои порты, за исключением того, на который кадр был получен, и одновременно запоминает MAC-адрес источника в адресной таблице. Например, если узел с MAC-адресом 0B1481182001 передает кадр данных узлу 0AA0C9851004 (рис.4.5), то в таблице (табл. 4.2) появится первая запись. В этой записи будет указано, что узел с MAC-адресом 0B1481182001 присоединен к порту № 1. При передаче данных от узла 0AA0C9851004 узлу 0002B318A102 в табл. 4.2 появится вторая запись и т.д. Таким образом, число записей в адресной таблице может быть равно числу узлов в сети, построенной на основе коммутатора.

Таблица 4.2

Адресная таблица коммутации

№ записи	MAC-адрес	№ порта
1	0B1481182001	1
2	0AA0C9851004	*n*
3		
4		

Когда адресная таблица коммутации сформирована, продвижение кадров с входного интерфейса коммутатора на выходной происходит на основании записей в адресной таблице. При получении кадра коммутатор проверяет, существует ли MAC-адрес узла назначения в таблице коммутации. При обнаружении адресата в таблице коммутатор производит еще одну проверку: находятся ли адресат и источник в одном сегменте. Если они в разных сегментах, то коммутатор производит **коммутацию** или **перенаправление**, **продвижение кадра** (**forwarding**) в порт, к которому подключен узел назначения. Если адресат и источник находятся в одном сегменте, например оба подключены к одному концентратору (рис. 4.5), то передавать кадр на другой порт не нужно. В этом случае кадр должен быть удален из буфера порта, что называется **фильтрацией** (filtering) **кадров.**

С появлением в сети новых узлов адресная таблица пополняется. Если в течение определенного времени (обычно 300 сек.) какой-то узел не передает данные, то считается, что он в сети отсутствует, тогда соответствующая запись из таблицы удаляется. При необходимости администратор может включать в таблицу статические записи, которые не удаляются динамически. Такую запись может удалить только сам администратор. Эти вопросы рассмотрены в лекции 14.

При получении кадров с широковещательными адресами коммутатор передает их на все свои порты. В ряде случаев такой режим удобен. Таким образом, коммутатор не фильтрует кадры с широковещательными адресами. Поэтому если какой либо узел из-за сбоя начинает ошибочно генерировать кадры с широковещательными адресами, то сеть очень быстро оказывается перегруженной, наступает широковещательный шторм (broadcast storm), сеть “падает”. Этим же пользуются злоумышленники, желающие нарушить нормальное функционирование сети. Они «наводняют» сеть широковещательными сообщениями с ложными адресами источника,

адресная таблица коммутации переполняется, и коммутатор начинает работать, как концентратор. При этом злоумышленник получает возможность анализировать всю информацию, передаваемую по локальной сети. С широковещательным штормом может бороться только маршрутизатор (рис.4.6), который делит сеть на широковещательные домены, т.е. отдельные сети.

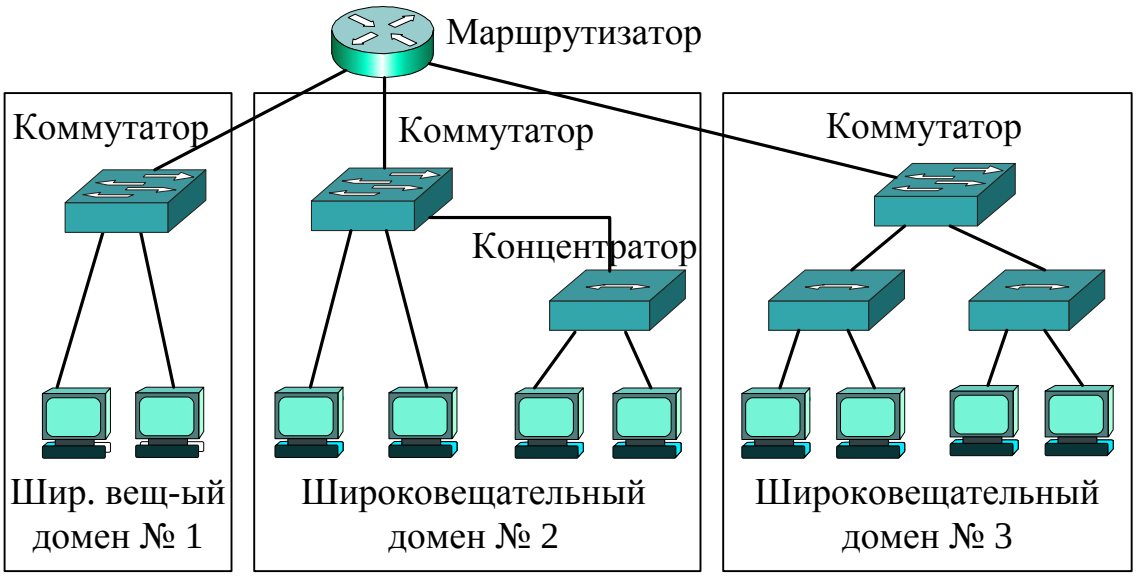


Рис.4.6. Деление сети на широковещательные домены

Быстродействие или производительность коммутатора определяются рядом параметров: скоростью фильтрации кадров, скоростью продвижения кадров, пропускной способностью, длительностью задержки передачи кадра.

Скорость фильтрации определяется временем приема кадра, запоминанием его в буфере, обращением к адресной таблице коммутации и удалением кадра из буферной памяти, если адресат и источник находятся в одном сегменте. Коммутатор обычно успевает фильтровать кадры в темпе их поступления в интерфейс, поэтому фильтрация не вносит дополнительной задержки.

Скорость продвижения кадров определяется временем приема кадра, запоминанием его в буфере, обращением к адресной таблице и передачей кадра с входного порта на выходной, который связан с устройством назначения. Скорость фильтрации и скорость продвижения задаются в кадрах в секунду, причем, для оценки этих параметров обычно берутся кадры минимальной длины 64 байта.

Пропускная способность коммутатора определяется количеством передаваемых данных, содержащихся в поле Data кадра, в единицу времени. Пропускная способность достигает своего максимального значения при передаче кадров максимальной длины.

Задержка передачи кадров определяется временем от момента появления первого байта кадра на входном порте коммутатора до момента появления этого байта на выходном порте. В зависимости от режима коммутации время задержки составляет от единиц до сотен микросекунд.

Режимы коммутации

Коммутаторы могут работать в нескольких режимах, при изменении которых меняются задержка и надежность. Для обеспечения максимального быстродействия коммутатор может начинать передачу кадра сразу, как только получит MAC-адрес узла назначения. Такой режим получил название **сквозной коммутации** или коммутации “на лету” (**cut-through switching**), он обеспечивает наименьшую задержку при прохождении кадров через коммутатор. Однако в этом режиме невозможен контроль ошибок, поскольку поле контрольной суммы находится в конце кадра. Следовательно, этот режим характеризуется низкой надежностью.

Во втором режиме коммутатор получает кадр целиком, помещает его в буфер, проверяет поле контрольной суммы (FCS) и затем пересылает адресату. Если получен кадр с ошибками, то он отбрасывается (discarded) коммутатором. Поскольку кадр перед отправкой адресату назначения запоминается в буферной памяти, то такой режим коммутации получил название коммутации с **промежуточным хранением или буферизацией** (**store-and-forward switching**). Таким образом, в этом режиме обеспечивается высокая надежность, но низкая скорость коммутации.

Промежуточное положение между сквозной коммутацией на лету и буферизацией занимает режим *коммутации свободного фрагмента* (fragment-free mode). В этом режиме читаются первые 64 байта, которые включают заголовок кадра и поле данных минимальной длины. После этого начинается передача кадра до того, как будет получен и прочитан весь кадр целиком. При этом производится верификация адресации и информации LLC

протокола, чтобы убедиться, что данные будут правильно обработаны и доставлены адресату.

Когда используется режим сквозной коммутации на лету, порты устройств источника и назначения должны иметь одинаковую скорость передачи. Такой режим называется симметричной коммутацией. Если скорости не одинаковы, то кадр должен запоминаться (буферизироваться) перед тем, как будет передаваться с другой скоростью. Такой режим называется асимметричной коммутацией, при этом должен использоваться режим с буферизацией.

Асимметричная коммутация обеспечивает связь между портами с разной полосой пропускания. Данный режим является характерным, например, для потока данных между многими клиентами и сервером, при котором многие клиенты могут одновременно соединяться с сервером. Поэтому на это соединение должна быть выделена широкая полоса пропускания.

Протокол STP

Когда сеть строится с использованием топологии иерархического дерева, то коммутационные петли отсутствуют. Однако сети часто проектируются с избыточными путями, чтобы обеспечить надежность и устойчивость сети (рис.4.7). Избыточные пути могут приводить к образованию коммутационных петель, что, в свою очередь, может привести к широковещательному шторму и обрушению сети.

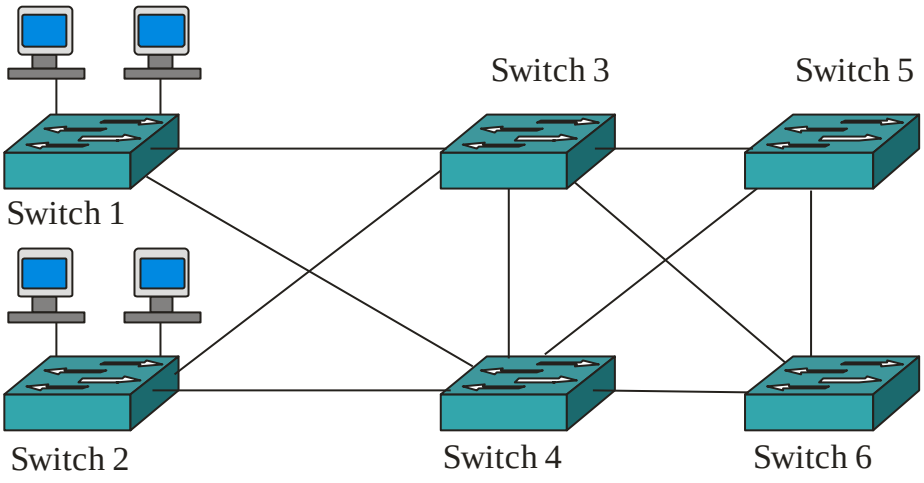


Рис.4.7. Образование маршрутных петель в сетях на коммутаторах

Протокол для предотвращения петель в коммутируемых сетях (Spanning-Tree Protocol – **STP)** используется в сетях с избыточными путями. Коммутаторы используют алгоритм STA, чтобы перевести в резервное состояние избыточные пути, которые не соответствуют иерархической топологии. Запасные избыточные пути задействуются, если основные выходят из строя.

Таким образом, протокол STP используется для создания логической иерархии без петель, т.е. даже при наличии физических петель, логические петли отсутствуют. Каждый коммутатор в локальной сети рассылает уведомления STP во все свои порты, чтобы позволять другим коммутаторам знать о их существовании. Эта информация используется, чтобы выбрать *корневой коммутатор* для сети.

Каждый порт коммутатора, который используя STP, находится в одном из следующих 5 состояний:

- Блокировка (Blocking)
- Прослушивание (Listening)
- Обучение (Learning)
- Продвижение (Forwarding)
- Выключен (Disabled)

При инициализации коммутатора все порты, за исключением находящихся в выключенном состоянии Disabled, переводятся в состояние блокировки Blocking. В этом состоянии порты передают, принимают и обрабатывают уведомления STP, т.е. участвуют в процессе управления, но не передают информационные данные.

В начальный момент работы алгоритма STA порты устанавливаются в состояние прослушивания Listening на время, определяемое таймером. Если за время работы таймера порт получит уведомление STP с лучшей чем его метрикой, то он перейдет в состояние блокировки Blocking. Если принятая метрика хуже его собственной, порт перейдет в состояние обучения Learning, чтобы принимать, но еще не продвигать пакеты данных и создавать адресную таблицу коммутации. Длительность состояния Learning также задается таймером.

После окончания заданного таймером времени порт переходит в состояние продвижения Forwarding, т.е. начинает полноценную обработку и продвижение пакетов. Переход порта в состояние выключения Disabled и

выход из него может быть реализован только по командам конфигурирования.

Существенным недостатком протокола STP является слишком долгое время формирования новой конфигурации сети, которое может составлять значение порядка минут.

Краткие итоги лекции 4

1. Канальный уровень (Data Link) обеспечивает обмен данными через общую локальную среду. Он разделен на два подуровня (LLC и MAC).
2. Подуровень LLC реализует связь с протоколами сетевого уровня.
3. Формат кадра протокола LLC является общим для всех технологий канального уровня.
4. Подуровень MAC определяет особенности доступа к физической среде при использовании различных технологий локальных сетей.
5. Каждой технологии MAC-уровня соответствует несколько вариантов (спецификаций) протоколов физического уровня, которые определяют скорость передачи, вид среды.
6. На MAC подуровне современных сетей используется ряд технологий: Ethernet, Fast Ethernet, Gigabit Ethernet и 10Gigabit Ethernet.
7. В локальных сетях адресация узлов производится на основе MAC-адресов, содержащих 48 двоичных разрядов. MAC-адреса представлены в шестнадцатеричной системе.
8. В сетях технологии Ethernet, построенных на основе логической топологии “общая шина”, разделяемая среда передачи данных является общей для всех пользователей. При этом реализуется метод множественного доступа к среде с контролем несущей и обнаружением коллизий (CSMA/CD).
9. Для предотвращения коллизий современные локальные сети строятся на базе коммутаторов, которые делят сеть на сегменты коллизий.
10. Продвижение кадров с входного интерфейса коммутатора на выходной происходит на основании записей в адресной таблице коммутации.
11. Различные режимы коммутации позволяют изменять производительность коммутатора.
12. Протокол для предотвращения петель в коммутируемых сетях (STP) используется в сетях с избыточными путями.

Вопросы по лекции 4

1. Какие функции выполняет верхний подуровень канального уровня?
2. Какие функции выполняет нижний подуровень канального уровня?
3. Что определяют спецификации технологии MAC-уровня?
4. Сколько двоичных разрядов содержит MAC-адрес и в какой системе он представлен?
5. Каким типом адреса является FFFFFFFFFFFF?
6. Какой метод доступа к среде отображается аббревиатурой CSMA/CD?
7. Что такое коллизия?
8. Какое устройство ограничивает коллизию пределами одного сегмента?
9. Что такое микросегмент?
10. На базе каких адресов происходит адресация узлов в локальных сетях?
11. Чем различаются продвижение и фильтрация кадров?
12. Какое устройство делит сеть на широковещательные домены?
13. Какими параметрами определяется производительность коммутатора?
14. Чем отличается сквозная коммутация или коммутация “на лету” от коммутации с промежуточным хранением или буферизацией?
15. Для чего используется протокол STP?

Упражнения

1. Перечислите спецификации технологий Ethernet, Fast Ethernet. Приведите их основные характеристики.
2. Изобразите формат кадра LLC.
3. Изобразите формат кадра MAC.
4. Укажите размер и назначение полей кадра стандарта 802.3.
5. Объясните, почему задается минимальная длина поля данных.
6. Изобразите схему локальной сети на коммутаторе с пятью конечными узлами, укажите номера портов и MAC-адреса узлов. Создайте таблицу коммутации для случая, когда все узлы активно обмениваются данными.

Лекция 5. ETHERNET-СОВМЕСТИМЫЕ ТЕХНОЛОГИИ

Краткая аннотация лекции: приведено краткое описание технологий Fast Ethernet, Gigabit Ethernet, 10 Gigabit Ethernet; даны основные технические характеристики и особенности функционирования указанных сетевых технологий.
Цель лекции: провести сравнительный анализ технологий Fast Ethernet, Gigabit Ethernet, 10 Gigabit Ethernet.

5.1. Технология Fast Ethernet

Создание технологии **Fast Ethernet** было обусловлено необходимостью увеличения скорости передачи данных до 100 Мбит/с. Технология Fast Ethernet выиграла в конкурентной борьбе с другими новыми высокоскоростными технологиями, поскольку обеспечила преемственность и согласованность с широко распространенными сетями Ethernet. То есть, в существующей сети Ethernet можно было постепенно отдельные сегменты переводить на технологию Fast Ethernet. При этом вся сеть оставалась работоспособной, в старых сегментах сети Ethernet скорость передачи данных была 10 Мбит/с, в новых (Fast Ethernet) – скорость 100 Мбит/с, между старыми и новыми сегментами – 10 Мбит/с.

Преемственность и согласованность с сетями Ethernet обусловили ряд принципов построения новых сетей Fast Ethernet (**стандарт 802.3u**). Так в технологии Fast Ethernet сохранился принцип использования общей разделяемой среды. Поскольку скорость передачи по сравнению с Ethernet увеличилась на порядок, то на порядок уменьшилась удвоенная задержка распространения сигнала PDV. Поэтому, чтобы не потерять кадры при возникновении коллизий, диаметр сети уменьшился также на порядок – до 200 м. Однако при использовании коммутаторов в полнодуплексном режиме возникновение коллизий исключено, поэтому существуют ограничения только на длину физических сегментов, которые соединяют два соседних устройства: сетевой адаптер с коммутатором или два соседних коммутатора.

В сетях передачи данных передатчик и приемник могут иметь несколько отличающиеся тактовые частоты. Это обусловлено различными причинами. Например, в технологии PDH узлы сети имеют разные тактовые генераторы. В сетях SDH тактовый генератор единый, однако каналы передачи информации могут иметь различную задержку. Поэтому передаваемые по линии связи данные должны отвечать принципу

самосинхронизации, т.е. тактовый генератор приемника должен подстраивать свою частоту и фазу под частоту и фазу передатчика, используя принимаемые биты данных. Для этого кодированный сигнал должен иметь достаточно частые изменения состояния: 0 и 1.

Спектр сигналов при использовании манчестерского кодирования значительно шире спектра потенциальных избыточных кодов. Поэтому, несмотря на то, что применяемый в Ethernet манчестерский код обладает очень хорошими свойствами самосинхронизации, разработчики технологии Fast Ethernet и других новых технологий отказались от него. На уровне **логического кодирования** в Fast Ethernet используются избыточные коды **4B/5B** или 8B/6T, а на **физическом уровне коды NRZI** или **MLT-3.**

На рис.5.1 приведены временные диаграммы информационных сигналов с использованием различных кодов.

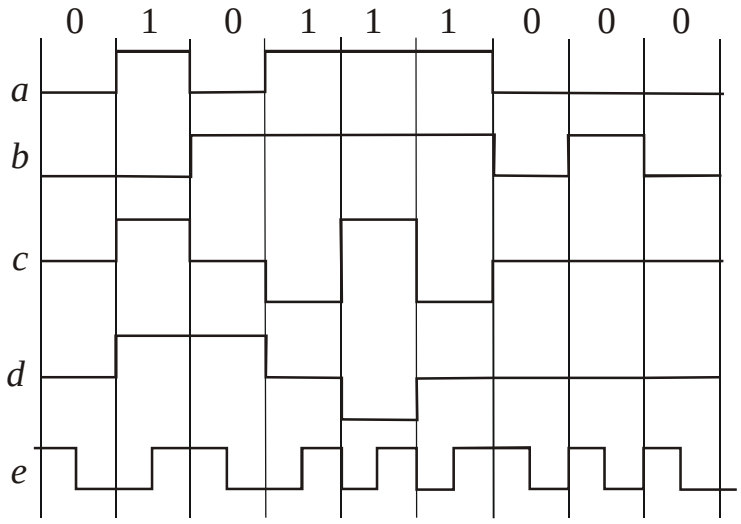


Рис.5.1. Коды передачи данных

Потенциальный код без возврата к нулю (NRZ – Non-Return to Zero) является наиболее простым, нулю соответствует низкий уровень сигнала, единице – высокий (рис.5.1а). Однако при длинных последовательностях нулей или единиц его свойства самосинхронизации очень плохие, поскольку нет переходов сигнала из одного состояния в другое. Поэтому данный код в чистом виде в сетях телекоммуникаций применяется редко.

Модифицированный потенциальный код (NRZI – Non-Return to Zero Inverted) изменяет свое состояние на противоположное при передаче нуля и

не меняет состояние – при передаче единицы (рис.5.1b). Его свойства самосинхронизации несколько лучше, чем кода NRZ, поэтому он применяется в технологии Fast Ethernet спецификации 100 Base-FX.

Существенно лучшими свойствами самосинхронизации обладают биполярные коды: AMI – Alternate Mark Inversion (рис.5.1c) и MLT-3 – Multi Level Transmission (рис.5.1d). Нулевые биты кода AMI представлены нулевым уровнем сигнала, а единичные биты – чередующимися значениями +V, -V. При передаче нулевого бита кода MLT-3 значение сигнала не изменяется, оставаясь таким, каким оно было к этому моменту. При передаче единичных бит данных значение сигнала изменяется в следующей последовательности: +V, 0, -V, 0, +V и т.д. Сигналы кода MLT-3 характеризуются более узкой полосой частот по сравнению с кодом NRZI, модификацией которого он является. Код MLT-3 используется в технологии Fast Ethernet спецификации 100 Base-TX.

Манчестерский код (рис.5.1e) обладает наилучшими свойствами самосинхронизации. Однако у него более широкая полоса частот по сравнению с потенциальными кодами NRZ, NRZI и, особенно, по сравнению с биполярными кодами AMI, MLT-3.

Для устранения плохой самосинхронизации кодов NRZ, AMI, MLT-3 используется либо избыточный блочный код 4B/5B, либо специальное устройство – скремблер. В случае применения избыточного блочного кода 4B/5B последовательность битов разбивается на блоки по 4 бита и к каждому блоку добавляется один избыточный бит. При этом из 32 кодовых комбинаций для кодирования данных используются только 16 комбинаций, содержащих чередующиеся значения нулей и единиц (табл.5.1). В последовательности передаваемых бит число нулей не может быть больше трех. Остальные кодовые комбинации считаются запрещенными.

Таблица 5.1

Код 4B/5B

4B	5B	4B	5B	4B	5B	4B	5B
0000	11110	0100	01010	1000	10010	1100	11010
0001	01001	0101	01011	1001	10011	1101	11011
0010	10100	0110	01110	1010	10110	1110	11100
0011	10101	0111	01111	1011	10111	1111	11101

Спектр потенциального избыточного кода 4B/5B уже спектра манчестерского кода, поэтому избыточный код применяется в новых высокоскоростных технологиях, например, в Fast Ethernet.

Другим способом исключения в передаваемых данных длинных последовательностей нулей является **скрэмблирование**. Результирующий код вычисляется на основании исходного кода по определенному алгоритму. Например, в качестве такого алгоритма может быть использовано следующее соотношение

$$B_i = A_i \oplus B_{i-3} \oplus B_{i-5},$$

где $\oplus$ - символ сложения по модулю 2,

B_i – значение двоичного кода на выходе скремблера на i –ом такте,

A_i – значение двоичного кода на входе скремблера на i –ом такте,

B_{i-3} – значение двоичного кода на выходе скремблера на 3 такта ранее текущего i –ого такта,

B_{i-5} – значение двоичного кода на выходе скремблера на 5 тактов ранее текущего i –ого такта.

Временные параметры Fast Ethernet, указанные в битовых интервалах, остались неизменными по сравнению с технологией Ethernet, но сам битовый интервал уменьшился на порядок и стал равен 0,01 мкс. Технология Fast Ethernet ориентирована на использование в качестве физической среды:

- витой пары 5 категории (спецификация 100Base-TX);
- витой пары 3 категории (100Base-T4) ;
- многомодового волоконно-оптического кабеля (100Base-FX).

Поскольку технология Fast Ethernet должна: во-первых – обеспечивать согласованность с сетями Ethernet, во-вторых – работать с разной физической средой, то физический уровень семиуровневой модели усложнен по сравнению с Ethernet и включает три подуровня:

- подуровень согласования (reconciliation sublayer);
- подуровень независимого от среды интерфейса (media independent interface, MII);
- устройство физического уровня (physical layer device, PHY).

Подуровень согласования необходим, чтобы MAC уровень, который был связан в Ethernet с физическим уровнем интерфейсом AUI, мог работать с

новым интерфейсом MII. Кроме того, устройство физического уровня также разделено на три подуровня:

- подуровень логического кодирования данных, на котором используются избыточные коды 4B/5B или 8B/6T;
- подуровень физического присоединения в зависимости от физической среды формирует сигналы в соответствие с кодами NRZI или MLT-3;
- подуровень автопереговоров, позволяющий определить режим работы (полудуплексный или полнодуплексный), скорость передачи данных (10Мбит/с или 100Мбит/с) и тип среды передачи в зависимости от спецификации.

В **спецификации 100Base-TX** для соединения сетевого адаптера и коммутатора (или коммутаторов между собой) используются две витых пары UTP категории 5 или STP Type 1. Максимальная длина сегмента – 100 м. Логическое кодирование – 4B/5B, физическое кодирование – MLT-3. В данной спецификации используется функция автопереговоров для возможности соединения с сетью Ethernet или с устройствами спецификации 100Base-T4.

Спецификация 100Base-T4 была создана для того, чтобы использовать в новой технологии Fast Ethernet уже существующие во многих зданиях витые пары UTP категории 3. Полоса пропускания витой пары UTP категории 3 составляет 16 МГц. Для того чтобы пропустить трафик со скоростью 100Мбит/с, в данной спецификации используется три витых пары (рис.5.2). Четвертая витая пара используется при прослушивании несущей для определения занятости среды.

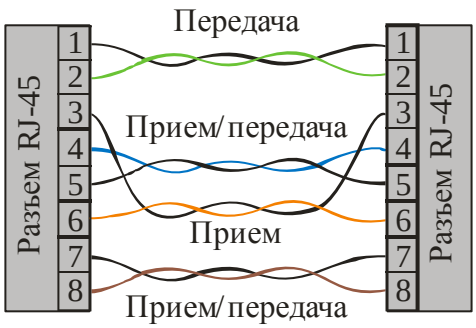


Рис.5.2. Четыре витых пары спецификации 100Base-T4

Таким образом, по каждой витой паре необходимо передавать данные со скоростью 33,3 Мбит/с, что также превышает возможности UTP

категории 3. Поэтому в этой спецификации используется метод кодирования 8B/6T, обладающий более узким спектром сигналов по сравнению с 4B/5B. Каждые 8 бит информации кодируются шестью троичными цифрами (триадами). Указанные меры позволили передавать данные со скоростью 100 Мбит/с по трем витым парам UTP категории 3.

Витые пары являются самой распространенной средой передачи данных в локальных сетях. Поэтому для них определено 5 режимов обмена данными, которые могут быть реализованы устройствами совместимых технологий Ethernet и Fast Ethernet:

- 10Base-T – 2 пары UTP 3 категории;
- 10Base-T full duplex – 2 пары UTP 3 категории;
- 100Base-TX – 2 пары UTP 5 категории;
- 100Base-T4 – 4 пары UTP 3 категории;
- 100Base-TX full duplex – 2 пары UTP 5 категории.

Fast Ethernet **спецификация 100Base-FX** предусматривает работу по двум волокнам оптического многомодового кабеля 62,5/125 мкм в полудуплексном или полнодуплексном режиме. Максимальная длина сегмента в полудуплексном режиме составляет 412 м, а в полнодуплексном – 2000 м. Метод логического кодирования – 4B/5B, физического кодирования – NRZI.

В Ethernet – совместимых технологиях скорость передачи возрастала с 10 Мбит/с до 100 Мбит/с в Fast Ethernet, затем до 1000 Мбит/с в Gigabit Ethernet и, наконец, до 10000 Мбит/с в 10 Gigabit Ethernet. При этом требование преемственности и совместимости было одним из основных, что позволило этим технологиям победить в конкурентной борьбе. Требование совместимости было удовлетворено за счет реализации процесса *автопереговоров* (Auto-Negotiation) о скорости обмена данными. Этот процесс определяет, как два узла связи автоматически договариваются о режиме и скорости обмена данными.

В процессе обмена информацией о допустимой скорости и режиме работы, оба коммутатора согласовывают и устанавливают связь с максимальной скоростью, общей для обоих коммутаторов.

Таким образом, до начала обмена данными два устройства должны в процессе автопереговоров установить, в каком режиме они будут работать. Устройство, которое инициирует начало обмена данными, посылает адресату сведения о своем наиболее приоритетном режиме. Низшим приоритетом обладает спецификация 10Base-T. Если адресат поддерживает предложенную технологию, то он подтверждает данный режим, и автопереговоры на этом завершаются. Если адресат не поддерживает предложенную технологию, то он указывает свой режим, в котором и будет производиться обмен данными.

Узлы спецификации 10Base-T не воспринимают запросы узлов с высокоприоритетными спецификациями 100Base-TX и другими. Поэтому, если узел технологии Fast Ethernet не получает ответ на свой запрос, то он устанавливает для себя низкоприоритетный режим 10Base-T.

Автопереговоры были первоначально определены для UTP реализаций Ethernet, но были расширены для работы с волоконно-оптическими линиями.

Для обеспечения совместимости и преемственности формат кадра Fast Ethernet спецификаций 100Base-FX, 100Base-TX в основном совпадает с форматом Ethernet (рис.5.3).

Рис.5.3. Формат кадра Fast Ethernet

Основное отличие заключается в том, что в технологии Ethernet признаком свободного состояния среды служило отсутствие несущей, а в технологии Fast Ethernet признаком свободного состояния служит передача по физической среде специального символа Idle. Начало кадра протокола Fast Ethernet отделяется от символов Idle парой символов J и K (11000 и 10001) кода 4B/5B, а конец – символом T.

Таким образом, технология Fast Ethernet обладает достаточно высокой скоростью 100 Мбит/с, она является совместимой с существующей широко распространенной технологией Ethernet. Ограничения диаметра сети до 200 м снимаются при использовании коммутаторов. Технология характеризуется разнообразием используемой физической среды (оптоволокно, UTP категории 5, UTP категории 3). Перечисленные свойства предопределили

широкое распространение технологии Fast Ethernet, которая в настоящее время практически заменила технологию Ethernet.

5.2. Технология Gigabit Ethernet

Внедрение услуг передачи голоса, данных и видеоинформации по единой мультисервисной сети (*Triple Play*) привело к необходимости повышения пропускной способности линий связи. Поэтому была разработана технология **Gigabit Ethernet**, предусматривающая передачу данных со скоростью 1 Гбит/с. В данной технологии, также как в Fast Ethernet, была сохранена преемственность с технологией Ethernet: практически не изменились форматы кадров, сохранился метод доступа CSMA/CD в полудуплексном режиме. На **логическом уровне** используется кодирование 8B/10B.

Поскольку скорость передачи увеличилась в 10 раз по сравнению с Fast Ethernet, то было необходимо либо уменьшить диаметр сети до 20 – 25 м, либо увеличить минимальную длину кадра. В технологии Gigabit Ethernet пошли по второму пути, увеличив минимальную длину кадра до 512 байт, вместо 64 байт в технологии Ethernet и Fast Ethernet. Диаметр сети остался равным 200 м, так же как в Fast Ethernet. Поскольку на практике часто передаются короткие кадры, то для снижения непроизводительной загрузки сети разрешается передавать несколько коротких кадров подряд с общей длиной до 8192 байт.

Современные сети Gigabit Ethernet, как правило, строятся на основе коммутаторов и работают в полнодуплексном режиме. В этом случае говорят не о диаметре сети, а о длине сегмента, которая определяется физической средой передачи данных. Gigabit Ethernet предусматривает использование:

- одномодового оптоволоконного кабеля; **802.3z**
- многомодового оптоволоконного кабеля; **802.3z**
- симметричного кабеля UTP категории 5; **802.3ab**
- коаксиального кабеля.

При передаче данных по оптоволоконному кабелю в качестве излучателей используются либо светодиоды, работающие на длине волны

830 нм, либо лазеры – на длине волны 1300 нм. В соответствие с этим стандарт **802.3z** определил две **спецификации 1000Base-SX** и **1000Base-LX.** Максимальная длина сегмента, реализованного на многомодовом кабеле 62,5/125 спецификации 1000Base-SX, составляет 220 м, а на кабеле 50/125 – не более 500 м. Максимальная длина сегмента, реализованного на одномодовом волокне спецификации 1000Base-LX, составляет 5000 м. Длина сегмента на коаксиальном кабеле не превышает 25 м.

Для использования уже имеющихся симметричных кабелей UTP категории 5 был разработан стандарт 802.3ab. Поскольку в технологии Gigabit Ethernet данные должны передаваться со скоростью 1000 Мбит/с, а витая пара 5 категории имеет полосу пропускания 100 МГц, то было решено передавать данные параллельно по 4 витым парам и использовать UTP категории 5 или 5е с шириной полосы более 125 МГц. Таким образом, по каждой витой паре необходимо передавать данные со скоростью 250 Мбит/с, что в 2 раза превышает возможности UTP категории 5е. Для устранения этого противоречия используется код 4D-PAM5 с пятью уровнями потенциала (-2, -1, 0, +1, +2). По каждой паре проводов одновременно производится передача и прием данных со скоростью 125 Мбит/с в каждую сторону. При этом происходит постоянная коллизия, при которой формируются сигналы сложной формы пяти уровней. Разделение входного и выходного потоков производится за счет использования схем гибридной развязки Н (рис.5.4). В качестве таких схем используются сигнальные процессоры. Для выделения принимаемого сигнала приемник вычитает из суммарного (передаваемого и принимаемого) сигнала собственный передаваемый сигнал.

Таким образом, технология Gigabit Ethernet обеспечивает высокоскоростной обмен данными и применяется, главным образом, для передачи данных между подсетями, а также для обмена мультимедийной информацией. Стандарт IEEE 802.3 рекомендует, что технология Gigabit Ethernet с передачей данных по волокну должна быть магистральной (backbone).

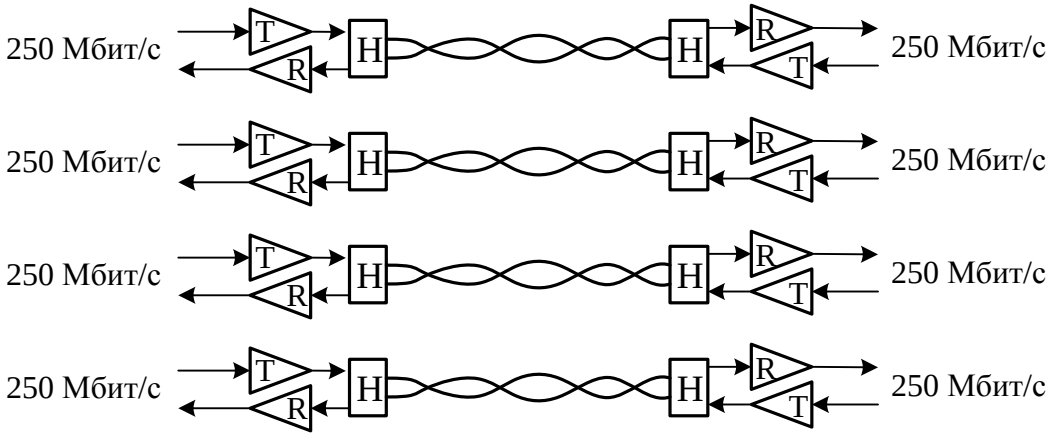


Рис. 5.4. Передача данных по 4 парам UTP категории 5

Временные интервалы, формат кадра и передача являются общими для всех версий 1000 Мбит/с (рис.5.5). Физический уровень определяют две схемы кодирования сигнала. Схема 8B/10B используется для оптического волокна и медных экранированных кабелей. Для симметричных кабелей UTP используется модуляция амплитуды импульсов (код PAM5). В волоконно-оптических линиях используют логическое кодирование 8B/10B и линейное кодирование (NRZ).

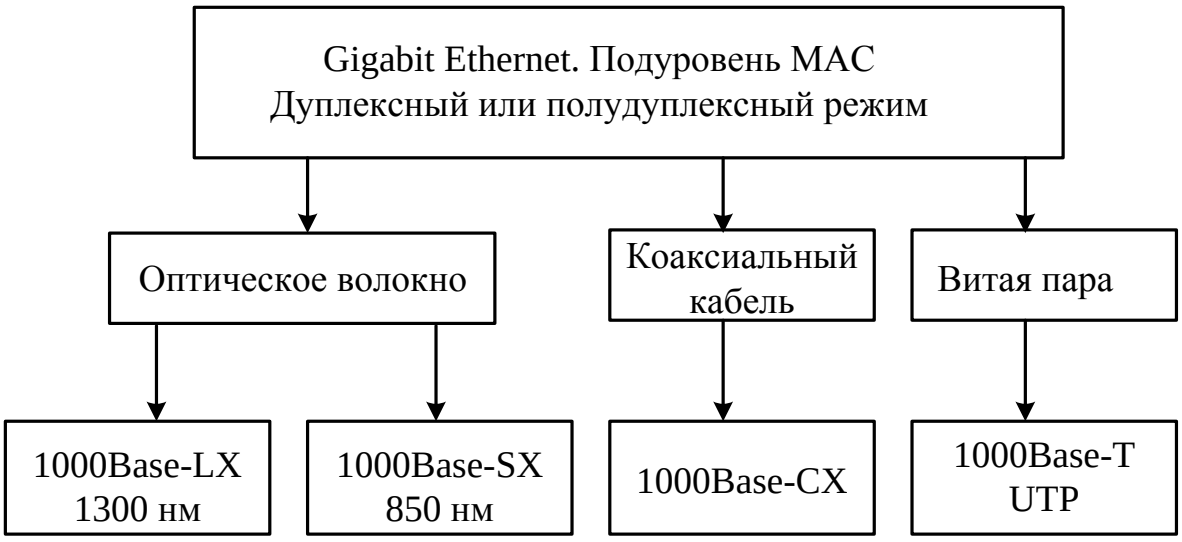


Рис.5.5. Спецификации технологии Gigabit Ethernet

Сигналы NRZ передаются по волокну, используя либо коротковолновые (short-wavelength), либо длинноволновые (long-wavelength) источники света. В качестве коротковолновых источников используются светодиоды с длиной волны 850 нм для передачи по многомодовому

оптическому волокну (1000BASE-SX). Этот менее дорогостоящий вариант используется для передачи на короткие расстояния в 200 – 300 м. Длинноволновые лазерные источники (1310 нм) используют одномодовое или многомодовое оптическое волокно (спецификация 1000BASE-LX). Лазерные источники в совокупности с одномодовым волокном способны передавать информацию на расстояние до 5000 м.

В соединениях точка – точка (point-to-point) для передачи (Tx) и приема (Rx) используются раздельные волокна, поэтому реализуется полнодуплексная связь. Технология Gigabit Ethernet позволяет устанавливать только единственный ретранслятор между двумя станциями. Ниже приведены параметры технологий 1000BASE (табл. 5.2).

Таблица 5.2

Сравнительные характеристики спецификаций Gigabit Ethernet

	Спецификация	Среда	Расстояние
1	1000Base-LX	Волокно 10 мкм	5000 м
2		Волокно 50 мкм	500 м
3		Волокно 62,5 мкм	500 м
4	1000Base-SX	Волокно 50 мкм	500 м
5		Волокно 62,5 мкм	300 м
6	1000Base-T	Витая пара UTP, 5e	100 м
7	1000Base-CX	Коаксиальн. кабель	25 м

Сети технологии Gigabit Ethernet, как правило, строятся на основе коммутаторов, когда расстояние полнодуплексных соединений ограничено только средой, а не временем двойного оборота. При этом используются топология «звезда» или «расширенная звезда».

Стандарт 1000BASE-T предусматривает использование кабеля UTP. категории 5e, 6 или 7. Предельная длина кабеля аппаратуры 1000BASE-T не превышает 100 м.

5.3. Технология 10-Gigabit Ethernet

Технология 10-Gigabit Ethernet (10GbE) описывается стандартом IEEE **802.3ae**, который определяет полнодуплексную передачу данных со скоростью 10 Гбит/с по волоконно-оптическому кабелю. Максимальные расстояния передачи зависят от типа используемого волокна. Используя одномодовое волокно как среду передачи, максимальное расстояние передачи – 40 километров. В настоящее время разрабатываются стандарты и создается аппаратура для технологий Ethernet со скоростью передачи 40 Гбит/с, 80 Гбит/с, 160- Гбит/с.

Стандарт 10GbE на физическом уровне позволяет увеличить расстояние связи до 40 км по одномодовому волокну и обеспечить совместимость с сетями синхронной цифровой иерархии (SDH) и фотонными сетями, использующими **плотное спектральное уплотнение по длине волны** (Dense Wave-length Division Multiplexing – **DWDM**).

Функционирование на 40-километровом расстоянии, скорость передачи до 10 Gbps и совместимость с системами SDH делает технологию 10GbE не только технологией локальных, но и технологией глобальных сетей. Специфические требования глобальных сетей обеспечивает технология операторского класса Carrier Ethernet. Таким образом, стандарт совместимых с Ethernet технологий развивается не только для LAN, но также для MAN и WAN. Поскольку в технологии 10GbE используется только полнодуплексная связь, в режиме CSMA/CD нет необходимости. Следовательно, в сетях исключается использование концентраторов hub.

Стандарт 802.3ae управляет семейством технологий 10GbE, которое включает:

- **10GBASE- SR** –для коротких расстояний по уже установленному многомодовому волокну, поддерживает связь на расстоянии от 26 м до 82 м.
- **10GBASE- LX4** – использует технологию уплотнения по длины волне (**WDM**), поддерживает связь на расстоянии от 240 м до 300 м по уже установленному многомодовому волокну и до 10 км по одномодовому волокну.
- **10GBASE- LR и 10GBASE- ER** – обеспечивает связь от 10 км до 40 км по одномодовому волокну.

- **10GBASE- SW, 10GBASE- LW и 10GBASE- EW** – технологии с общим названием **10GBASE-W**, предназначены, чтобы обеспечить работу оборудования глобальных сетей с модулями SONET/SDH.

Для 10-Gigabit Ethernet не предусмотрены повторители, поскольку полудуплексный режим не поддерживается.
Ниже приведены некоторые параметры спецификаций технологии 10GbE.

Таблица 5.3

Параметры спецификаций технологии 10GbE

Спецификация	Длина волны	Волокно	Расстояние
10GBase-LX4	1310 нм	62,5 мкм	2 – 300 м
		50 мкм	2 – 300 м
		10 мкм	2 – 10 км
		62,5 мкм	2 – 33 м
		50 мкм	2 – 300 м
10GBase-L	1310 нм	10 мкм	2 – 10 км
10GBase-E	1550 нм	10 мкм	2 – 40 км

В заключение следует отметить, что в настоящее время технологии Ethernet является стандартом для различных соединений: горизонтальных (внутри аудиторий, нескольких комнат на этаже), вертикальных (между этажами), соединений между зданиями. Новые версии Ethernet стирают различие между локальными и глобальными сетями. Трудно назвать сеть локальной, когда в сегменте, использующим технологию 10GbE, передаются данные на расстояние в 40 км.

Специально разработанной технологией Ethernet для глобальных сетей является технология операторского класса Carrier Ethernet. Технология Carrier Ethernet предоставляет услуги характерные для глобальных сетей: разделяет и изолирует адресные пространства локальной сети пользователя и глобальной сети провайдера, обеспечивая безопасность, гарантирует требуемое качество QoS, выделяя необходимую полосу пропускания, обеспечивает значения задержки и джиттера, не превышающие заданные.

В сетях Ethernet передача информации производится по трем составляющим сетевой среды:

1. По медным кабелям со скоростью примерно до 1000 Мбит/с, и возможно больше.
2. По беспроводной среде (радиоканалы) – примерно 100 Мбит/с и больше.
3. По оптическим кабелям со скоростью примерно 10000 Мбит/с, новые разработки – до 100 Гбит/с и выше.

Медная и беспроводная среда имеют определенные физические и практические ограничения на высокочастотные сигналы. В волоконно-оптических системах ограничивающим фактором является электронная технология и параметры оптического волокна.

В ранних версиях технологии Ethernet, использующих концентраторы в полудуплексном режиме, с возможностью возникновения коллизий (CSMA/CD), не рассматривался вопрос качества обслуживания (QoS). Однако на современном этапе при передаче определенных видов трафика, например, IP телефония и видео этот вопрос стал очень важным. Полнодуплексные быстродействующие технологии (Gigabit Ethernet, 10GbE) обеспечивают достаточную поддержку разнообразных приложений. Это расширяет потенциальные приложения Ethernet-совместимых технологий.

Краткие итоги лекции 5

1. В существующей сети Ethernet отдельные сегменты можно постепенно переводить на технологию Fast Ethernet.
2. Спецификация100Base-T4 представляет переходную технологию от Ethernet к Fast Ethernet. В данной спецификации для передачи данных используется три витых пары кабеля UTP 3 категории.
3. Основными спецификациями технологии Fast Ethernet являются 100Base-TX и 100Base-FX.
4. В технологии Fast Ethernet сохранился принцип использования общей разделяемой среды. При этом диаметр сети уменьшился до 200 м.
5. Спектр сигналов при использовании манчестерского кодирования значительно шире спектра потенциальных избыточных кодов.
6. При применении избыточного блочного кода 4B/5B из 32 кодовых комбинаций для кодирования символа используются только 16 комбинаций, содержащих чередующиеся значения нулей и единиц.
7. Скрэмблирование является одним из способов исключения в передаваемых данных длинных последовательностей нулей.
8. В процессе автопереговоров два узла связи автоматически договариваются о режиме и скорости обмена данными.
9. Начало кадра протокола Fast Ethernet отделяется от символов свободной среды Idle парой символов J и K (11000 и 10001) кода 4B/5B, а конец – символом T.
10. В технологии Gigabit Ethernet минимальная длина кадра увеличена до 512 байт, вместо 64 байт в технологии Ethernet и Fast Ethernet. Разрешается передавать несколько коротких кадров подряд с общей длиной до 8192 байт.
11. Стандарт 802.3z технологии Gigabit Ethernet определил две спецификации 1000Base-SX и 1000Base-LX. Для использования уже имеющихся симметричных кабелей UTP категории 5 был разработан стандарт 802.3ab.
12. Сети технологии Gigabit Ethernet, как правило, строятся на основе коммутаторов, когда расстояние полнодуплексных соединений ограничено только средой сегмента.
13. Технология 10-Gigabit Ethernet (10GbE) описывается стандартом IEEE 802.3ae, который определяет полнодуплексную передачу данных со скоростью 10 Гбит/с по волоконно-оптическому кабелю.
14. Стандарт 10GbE на физическом уровне позволяет увеличить расстояние связи до 40 км по одномодовому волокну и обеспечить совместимость с сетями синхронной цифровой иерархии (SDH) и фотонными сетями, использующими спектральное уплотнение по длине волны DWDM.

Вопросы по лекции 5

1. Чему равен диаметр сети Fast Ethernet при использовании концентраторов?
2. Чем определяется максимальное расстояние между узлами сети Fast Ethernet при использовании коммутаторов?
3. В чем достоинства и недостатки манчестерского кода?
4. Для чего используется скрэмблирование?
5. Какие коды используются на уровне логического кодирования в сетях технологий Fast Ethernet, Gigabit Ethernet?
6. Для чего в сетях используются блочные избыточные коды 4B/5B или 8B/10B?
7. Для чего в сетях технологий Fast Ethernet введены автопереговоры?
8. Какой кабель используется в сетях Fast Ethernet спецификации 100Base-FX?
9. Какова максимальная длина сегмента спецификации 100Base-FX в полудуплексном и в полнодуплексном режиме?
10. Как отмечаются начало и конец кадра технологий Fast Ethernet?
11. Почему в технологии Gigabit Ethernet увеличили минимальную длину кадра до 512 байт?
12. Чему равна максимальная длина сегмента, реализованного на одномодовом волокне спецификации 1000Base-LX?
13. Можно ли использовать в технологии 10GbE режим CSMA/CD ?
14. Какие спецификации технологии 10GbE обеспечивают максимальную дальность связи?

Упражнения

1. Приведите временные диаграммы информационных сигналов с использованием различных кодов (NRZ, NRZI, AMI, Манчестерский код).
2. Изобразите формат кадра технологии Fast Ethernet. Объясните, в чем его отличие от кадра Ethernet.
3. Изобразите схему кабеля спецификации 100Base-T4.
4. Объясните, почему в технологии Gigabit Ethernet увеличена минимальная длина кадра до 512 байт.
5. Изобразите схему передачи данных по кабелю UTP 5 категории в сетях технологии Gigabit Ethernet.

Контрольный тест по разделу 2

Задача 2.1
Вариант 1 Задачи 2.1

37. Что происходит в сети Ethernet после возникновения коллизии? (выбрать три ответа)
    Передача данных останавливается и запускается алгоритм обработки коллизии
    Вовлеченные в коллизию устройства затем имеют приоритет для передачи данных
    Вовлеченные в коллизию устройства затем не имеют приоритет для передачи данных
    Вовлеченное в коллизию устройство перед повторной передачей должно прослушивать среду передачи
    Повторно передается только слово кадра, поврежденное в результате коллизии

Вариант 2 Задачи 2.1

38. Какие утверждения относительно технологии Ethernet являются верными? (выбрать два ответа)
    Используются адреса уровней Layer 2 и Layer 3 модели OSI
    Функционирование определяется стандартом 802.3
    Функционирование определяется стандартом 802.5
    Обеспечивается преемственность при переходе к более высокоскоростной технологии
    При переходе к более высокоскоростной технологии необходима замена всего оборудования

Вариант 3 Задачи 2.1

39. Что означает метод доступа CSMA/CD?
    Детерминированный множественный доступ к среде с определением коллизий
    Не детерминированный множественный доступ к среде с определением коллизий
    Детерминированный множественный доступ к среде с устранением коллизий
    Не детерминированный множественный доступ к среде с устранением коллизий

Задача 2.2
Вариант 1 Задачи 2.2

40. Какова минимальная длина поля данных кадра 802.3?
    1500 байт
    512 байт
    46 байт
    72 байта

Вариант 2 Задачи 2.2

41. Какова максимальная длина поля данных кадра стандарта 802.3?
    46 байт
    64 байт
    48 бит
    1500 бит
    1500 байт

Вариант 3 Задачи 2.2

42. Какова длина поля адреса кадра стандарта 802.3?
    46 байт
    64 байт
    48 бит
    1500 бит
    1500 байт

Задача 2.3
Вариант 1 Задачи 2.3

43. Какой тип среды может использоваться в оборудовании спецификации 10Base-T? (выбрать три ответа)
    UTP категории 5
    Толстый коаксиальный кабель
    Тонкий коаксиальный кабель
    Многомодовый волоконно-оптический кабель
    UTP категории 3
    UTP категории 5e

Вариант 2 Задачи 2.3

44. Какой тип среды может использоваться в оборудовании спецификации 100Base-TX? (выбрать два ответа)
    UTP категории 5
    Толстый коаксиальный кабель
    Тонкий коаксиальный кабель
    Многомодовый волоконно-оптический кабель
    Одномодовый волоконно-оптический кабель
    UTP категории 3
    UTP категории 5e

Вариант 3 Задачи 2.3

45. Какой тип среды может использоваться в оборудовании спецификации 1000Base-T?
    Толстый коаксиальный кабель
    Тонкий коаксиальный кабель
    Многомодовый волоконно-оптический кабель
    Одномодовый волоконно-оптический кабель
    UTP категории 3
    UTP категории 5e

Задача 2.4
Вариант 1 Задачи 2.4

46. Какое устройство реализует деление сети на широковещательные домены?
    Маршрутизатор
    Коммутатор
    Концентратор
    Мост
    Повторитель

Вариант 2 Задачи 2.4

47. Какое устройство реализует деление сети на домены коллизий? (выбрать два ответа)
    Маршрутизатор
    Коммутатор
    Концентратор
    Мост
    Повторитель

Вариант 3 Задачи 2.4

48. Какое устройство не может делить сети на домены коллизий? (выбрать два ответа)
    Маршрутизатор
    Коммутатор
    Концентратор
    Мост
    Повторитель

Задача 2.5
Вариант 1 Задачи 2.5

49. Какой режим коммутации обеспечивается высокую надежность, но низкую скорость?
    Коммутации с буферизацией (store-and-forward)
    Сквозной коммутации или коммутации “на лету” (cut-through switching)
    Симметричной коммутацией (symmetric switching)
    Асимметричной коммутацией (asymmetric switching)
    Коммутации свободного фрагмента (fragment-free mode)

Вариант 2 Задачи 2.5

50. Какой режим коммутации реализует наименьшую задержку при прохождении кадров через коммутатор?
    Коммутации с буферизацией (store-and-forward)
    Сквозной коммутации или коммутации “на лету” (cut-through switching)
    Симметричной коммутацией (symmetric switching)
    Асимметричной коммутацией (asymmetric switching)
    Коммутации свободного фрагмента (fragment-free mode)

Вариант 3 Задачи 2.5

51. Для борьбы с петлями в сети с коммутаторами используется протокол
    RIP
    IP
    STP
    ARP
    RARP

Задача 2.6
Вариант 1 Задачи 2.6

52. Какая спецификация Ethernet рекомендована в качестве магистральной (backbone) технологии в настоящее время?
    10BASE-T
    100BASE-TX

100BASE-FX
1000BASE-LX

Вариант 2 Задачи 2.6

53. Что описывает технологию Gigabit Ethernet? (выберите два ответа)
Передает данные со скоростью 100 Мбит/с
Обычно используется в качестве магистральной (backbone) среды
Требуется экранированная витая пара
Передает данные со скоростью 1000 Мбит/с
Обычно используется в качестве среды между рабочими станциями

Вариант 3 Задачи 6

54. Как 1000BASE-T использует пары кабеля UTP для обмена данными?
Две пары использует для передачи и две пары для приема
Одна пара – для передачи, одна для приема, и две пары – двунаправленные
+ Все четыре пары используются для передачи и приема одновременно
Две пары используют спецификацию 10BASE-T и две пары – 100BASE-TX

Задача 2.7
Вариант 1 Задачи 2.7

55. Какая спецификация использует UTP? (выберите два ответа)
10Base-T
10Base-5
100Base-FX
100Base-TX
10Base-2T
10Base-FB

Вариант 2 Задачи 2.7

56. Какая спецификация использует одномодовое оптическое волокно?
10Base-T
10Base-5
100Base-FX
100Base-TX
10Base-2T
1000Base-LX

Вариант 3 Задачи 2.7

57. В какой технологии не используется метод доступа CSMA/CD в полудуплексном режиме?
Ethernet
Fast Ethernet
Gigabit Ethernet
10 Gigabit Ethernet
Используется во всех

Задача 2.8
Вариант 1 Задачи 2.8

58. Технология 10GbE регламентируется стандартом:
    802.3
    802.3u
    802.3z
    802.3ab
    802.3ae

Вариант 2 Задачи 2.8

59. Технология Gigabit Ethernet регламентируется стандартом: (дать 2 ответа)
    802.3
    802.3u
    802.3z
    802.3ab
    802.3ae

Вариант 3 Задачи 2.8

60. Технология Fast Ethernet регламентируется стандартом:
    802.3
    802.3u
    802.3z
    802.3ab
    802.3ae

Раздел 3. ПРИНЦИПЫ И СРЕДСТВА МЕЖСЕТЕВОГО ВЗАИМОДЕЙСТВИЯ

Лекция 6. АДРЕСАЦИЯ В IP - СЕТЯХ

Краткая аннотация лекции: Рассмотрены вопросы функционирования маршрутизаторов в составных сетях, логические адреса версии IPv4 на основе классов и бесклассовая адресация с масками переменной длины, а также принципы суммирования адресов. Рассмотрены частные адреса. Приведены параметры адресации IPv6. Механизмы назначения IP-адресов.
Цель лекции: изучить систему логических IP-адресов, методы формирования подсетей.

6.1. Адресация и маршрутизация

Объединение нескольких локальных сетей, узлов и отдельных пользователей в глобальную (**распределенную, составную**) сеть происходит с помощью устройств (**маршрутизаторов**) и протоколов сетевого Уровня 3 семиуровневой эталонной модели или уровня межсетевого взаимодействия четырехуровневой модели TCP/IP. **Маршрутизатор выбирает наилучший (оптимальный) путь к адресату, анализируя логический адрес назначения** передаваемого пакета данных. Процесс **выбора оптимального пути** получил название **маршрутизация**. Логические адреса сетевого интернет протокола (**Internet Protocol – IP**), получившие название **IP-адреса**, позволяют адресовать любую сеть, любого пользователя, любой узел или сайт в пределах всемирной сети Интернет.

Наиболее распространенными устройствами межсетевого взаимодействия сетей, подсетей и устройств являются **маршрутизаторы.** Они представляют собой специализированные компьютеры для выполнения специфических функций сетевых устройств. В лекции 4 (см. рис. 4.6) было показано, что маршрутизаторы используются, чтобы сегментировать сеть на широковещательные домены, т.е. являются устройствами локальных сетей **LAN**, но они используются и как устройства формирования глобальных сетей **WAN**. Поэтому маршрутизаторы имеют как **LAN, так и WAN интерфейсы**. Маршрутизаторы используют WAN интерфейсы, чтобы связываться друг с другом и всемирной сетью Интернет, и LAN интерфейсы для связи с узлами (компьютерами), например, через коммутаторы. Поэтому

маршрутизаторы являются устройствами как локальных, так и глобальных сетей. Маршрутизаторы являются также основными устройствами больших корпоративных сетей.

На рис.6.1 приведен пример того, как маршрутизаторы A, B и C объединяет нескольких локальных сетей (Локальные сети №1, №2, №3) в распределенную (составную) сеть. Поэтому **маршрутизаторы имеют интерфейсы как локальных, так и глобальных соединений**. К локальным сетям, созданным на коммутаторах, маршрутизатор присоединен через интерфейсы, которые на рис. 6.1 обозначены через F0/1, что означает: интерфейс Fast Ethernet, слот 0, номер 1. Глобальные соединения на рис.6.1 представлены последовательными или серийными (**serial**) интерфейсами S0/1, S0/2. Через такой же последовательный интерфейс реализовано соединение составной сети с сетью Интернет (Internet). Подобная структурная схема, включающая несколько последовательно соединенных маршрутизаторов, характерна для многих корпоративных сетей.

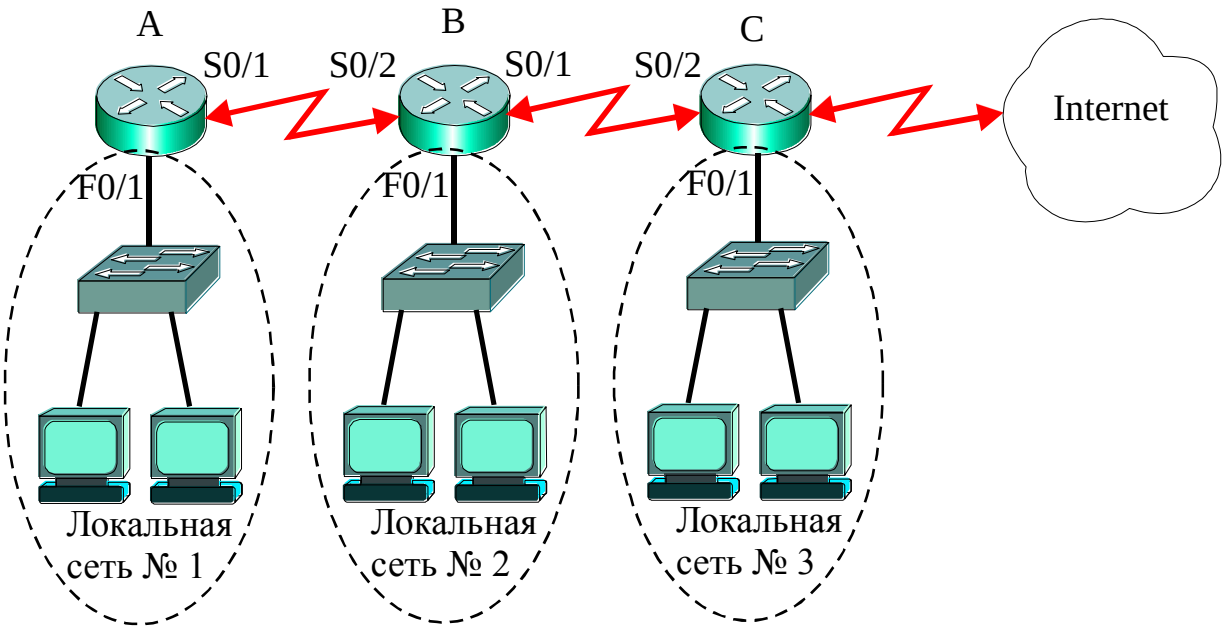


Рис.6.1. Составная сеть на маршрутизаторах

Интернет представляет собой совокупность сетей операторов и провайдеров (Internet Service Provider – **ISP**), соединенных с локальными сетями, сетями доступа, отдельными пользователями (рис.6.2).

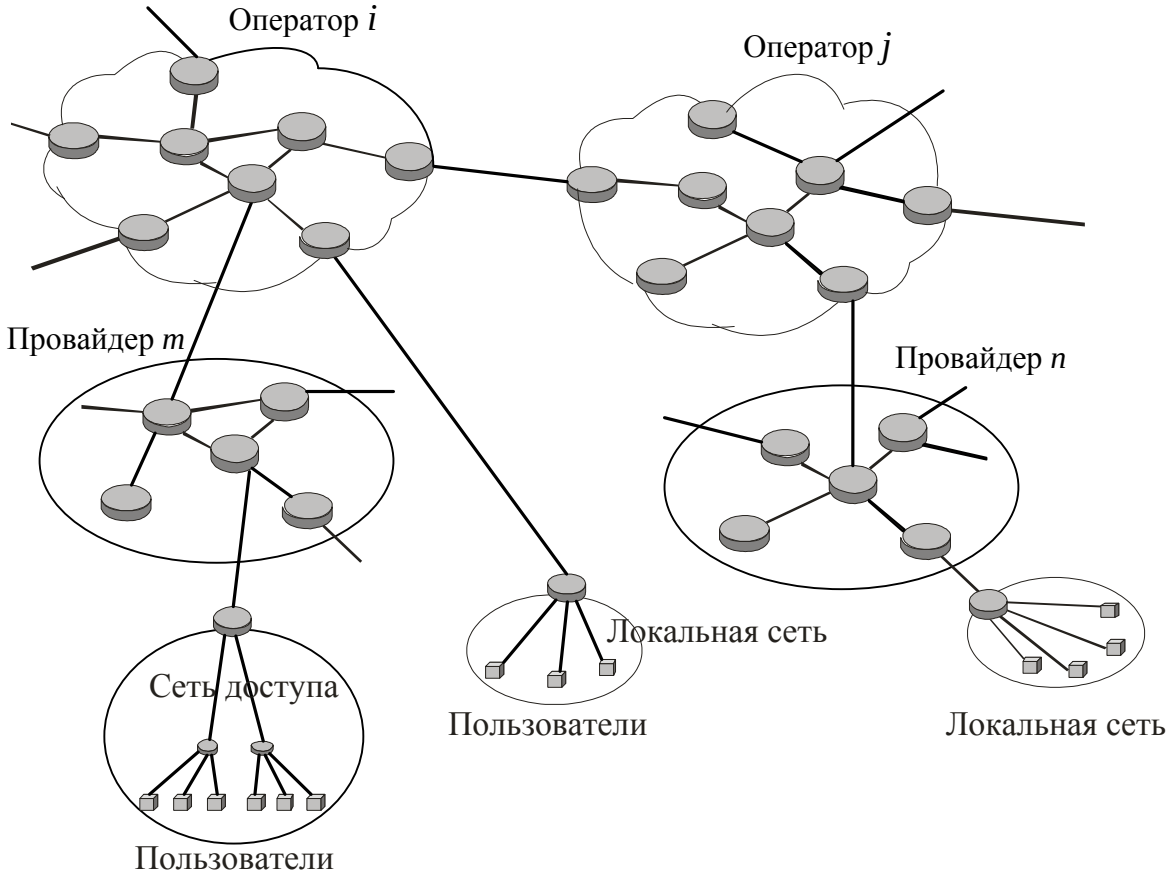


Рис.6.2. Схематичное изображение сети Интернет

Таким образом, маршрутизаторы обеспечивают связь между сетями и определяют наилучший (оптимальный) путь пакета данных к сети адресата назначения, причем, **технологии объединяемых локальных сетей могут быть различными**. Например, в локальной сети №1 (рис.6.1) может использоваться технология Fast Ethernet, в сети №2 – Token Ring, а в сети №3 – Gigabit Ethernet.

Устройства распределенной IP-сети должны иметь уникальные физические и логические адреса. Физический адрес устанавливается изготовителем аппаратных средств, например, MAC-адрес сетевой карты NIC, который «прошивается» в ПЗУ. Логический адрес устанавливается пользователем (администратором) или назначается динамически протоколом DHCP из диапазона выделенных провайдером адресов.

6.2. Логические адреса версии IPv4

Логические адреса узлов в IP-сетях версии **IPv4**, используемой в настоящее время, содержат 32 двоичных разряда, т.е. 4 байта. Каждый из 4 байт адреса в технической документации отображается десятичным числом (от 0 до 255), а байты разделяются точкой, например, 172.100.220.14. Часть этого адреса (**старшие разряды) является адресом сети, а другая часть (младшие разряды) – номером узла в сети**. Таким образом, **IP-адреса** являются **иерархическими**, в отличие от плоских MAC-адресов.

Если граница между сетевой частью адреса и номером узла в сети проходит в произвольной части IP-адреса, то такая **адресация** называется **бесклассовой** (**classless**). Если же сетевой части адреса отводится строго 1, 2 или 3 байта, такая **адресация** называется адресацией на основе **полного класса** (**classfull**). Деление адреса на классы производится в соответствии с тем, сколько байт адреса относится к номеру сети, а сколько к номеру узла. Для создания уникальных адресов узлов используются три класса.

В адресе класса A старший байт задает адрес сети, а три младших байта – адрес узла (host).

0	×	×	×	×	×	×	×	2-ой байт	3-ий байт	4-ый байт
№ сети – 1 байт								№ узла – 3 байта		

В адресе класса B два старших байта задают адрес сети, а два младших байта – адрес узла (host).

1	0	×	×	×	×	×	×	2-ой байт	3-ий байт	4-ый байт
№ сети – 2 байта								№ узла – 2 байта		

В адресе класса C три старших байта задают адрес сети, а младший байт – адрес узла.

1	1	0	×	×	×	×	×	2-ой байт	3-ий байт	4-ый байт
№ сети – 3 байта										№ узла – 1 байт

Существует также **многоадресный** (**multicast**) класс D и резервный класс E. Дополнительная информация по классам и адресам приведена в табл.6.1.

Таблица 6.1

Классы IP адресов

Класс	Первый байт адреса	Наименьший адрес сети	Наибольший адрес сети	Максимальное число узлов
A	0×××××××	1.0.0.0	126.0.0.0	2^{24} - 2
B	10××××××	128.0.0.0	191.255.0.0	2^{16} - 2
C	110×××××	192.0.0.0	223.255.255.0	2^{8} - 2
D	1110××××	224.0.0.0	239.255.255.255	multicast
E	11110×××	240.0.0.0	247.255.255.255	Резерв

Номер узла (адрес хоста – host) не может состоять только из одних единиц или нулей. Если в поле адреса узла все нули, то это значит, что задается номер (адрес) сети или подсети. Если же в этом поле все двоичные разряды равны единице, то это означает **широковещательный (broadcast) адрес**, когда пакет предназначен всем узлам сети, в которой находится узел, сформировавший данный пакет, т.е. источник передаваемой информации. Этим объясняется уменьшение максимального числа узлов в сети на 2 (см. табл.6.1). Таким образом, максимальное число узлов в сети класса С будет равно $2^{8} – 2 = 254$.

Старший разряд адреса класса А всегда равен 0, поэтому адреса сетей могут находиться в диапазоне от 1 до 127. Однако **адрес 127.0.0.1** предназначен для **самотестирования**, по этому адресу узел обращается к самому себе, проверяя, установлен ли протокол TCP/IP на этом хосте. Поэтому адрес сети 127.0.0.0 не входит в состав адресов таблицы 6.1.

С целью сокращения количества адресов, которыми оперирует маршрутизатор, в его таблице маршрутизации хранятся адреса сетей, а не узлов. В то же время, в адресной части заголовка пакета задаются адреса узлов. Поэтому маршрутизатор, получив пакет, должен из адреса назначения получить адрес сети. Эту операцию маршрутизатор реализует путем **логического умножения сетевого адреса узла на маску**. Число разрядов маски равно числу разрядов IP-адреса. Непрерывная последовательность единиц в старших разрядах маски задает число разрядов адреса, относящихся к номеру сети. **Младшие разряды маски, равные нулю, соответствуют разрядам адреса узла в сети**. При логическом умножении адреса узла на маску получается адрес сети. Например, при умножении IP-адреса

192.100.12.67 на стандартную маску класса С, равную 255.255.255.0, получается следующий результат:

11000000.01100100.00001100.01000011
11111111.11111111.11111111.00000000
11000000.01100100.00001100.00000000

т.е. получен номер сети 192.100.12.0.

Аналогичная запись предыдущего адреса с той же маской класса С может также иметь следующий вид: 192.100.12.67/24, означающий, что маска содержит единицы в 24 старших разрядах. При этом 24 старших разряда будут одинаковы для всех узлов сети, т.е. образуют общую часть адреса, называемую **префиксом**. Именно префикс имеет обозначение /24.

Стандартная маска адреса класса В имеет 16 единиц в старших разрядах и 16 нулей в младших. Поэтому, если адрес узла будет равен 172.16.37.103/16, то адрес сети будет равен 172.16.0.0. Маска адреса класса А имеет 8 единиц в старших разрядах и 24 нуля в младших. Поэтому, например, адресу узла 10.116.37.103/8 соответствует адрес сети 10.0.0.0.

Жесткому разбиению адресов на классы соответствуют протоколы маршрутизации типа **Classful**, которые требуют, чтобы использовалась стандартная (единая) маска сети. Например, в сети с адресом 192.168.187.0 может использоваться стандартная маска 255.255.255.0, а в сети 172.16.0.0 используется стандартная маска 255.255.0.0.

6.3. Формирование подсетей

В ряде случаев для удобства управления администратор может самостоятельно формировать подсети внутри выделенного ему адресного пространства. Например, администратору выделен адрес сети 198.11.163.0 класса С, и ему необходимо создать 10 подсетей по 14 компьютеров. Для адресации 10 подсетей потребуется 4 двоичных разряда адреса ($2^4 = 16$), и для адресации 14 узлов также требуется 4 двоичных разряда ($2^4 = 16$). Таким образом, сетевая часть адреса будет содержать 28 двоичных разрядов (24 + 4 = 28), а хостовая часть – 4 младших разряда. При этом маска должна иметь

единицы в 28 старших двоичных разрядах и 4 нуля в младших – 11111111.11111111.11111111.11110000, т.е. маска будет 255.255.255.240.

В этом случае максимально может быть задано 16 подсетей по 14 узлов в каждой. Из 16 подсетей администратор использует 10, а оставшиеся 6 использоваться не будут. Граница между сетевой частью адреса и номером узла (хоста) проходит посредине четвертого байта (октета), т.е. адресация будет **бесклассовой** (**classless**). Следовательно, если задан адрес 198.11.163.83 с маской 255.255.255.240, то после логического умножения адреса на маску будет получен следующий адрес подсети:

11000110.00001011.10100011.01010011
11111111.11111111.11111111.11110000
11000110.00001011.10100011.01010000 ,

т.е. подсеть имеет адрес 198.11.163.80, входящий в сеть полного класса 198.11.163.0, и номер узла в подсети равен 3 (0011).

Адреса всех подсетей и узлов, которые могут быть сформированы из выделенного адресного пространства 198.11.163.0/28, приведены в (табл.6.2).

Таблица 6.2

Адреса узлов и подсетей

№ подсети	Адрес подсети	Адреса узлов
1	198.11.163.0	198.11.163.1 - 198.11.163.14
2	198.11.163.16	198.11.163.17 - 198.11.163.30
3	198.11.163.32	198.11.163.33 - 198.11.163.46
…	…	…
10	198.11.163.144	198.11.163.145 - 198.11.163.158
…	…	…
16	198.11.163.240	198.11.163.241 - 198.11.163.254

При использовании других масок можно формировать другие комбинации подсетей и узлов. Например, с помощью маски 255.255.255.224 в адресном пространстве 198.11.163.0/24 можно сформировать 8 подсетей по

30 узлов в каждой, а с помощью маски 255.255.255.248 можно задать 32 подсети по 6 узлов. Используя маски разной (переменной) длины для создания подсетей, администратор может формировать подсети разного размера в пределах одной автономной системы. Таким образом, **маски переменной длины** (Variable-length subnet mask - **VLSM**) позволяют создавать подсети разного размера, гибко задавая границы между полем адреса сети и полем адреса узла. VLSM позволяют использовать больше чем одну маску подсети в пределах выделенного адресного пространства сети.

Например, для формирования сетей по 30 узлов в каждой требуется 27 разрядов маски (255.255.255.224), содержащих единицы, а для создания сети, соединяющей пару маршрутизаторов (точка – точка), требуется всего два адреса, т.е. маска должна иметь 30 единиц (255.255.255.252). При использовании маски в 30 двоичных разрядов два младших разряда адреса позволяют сформировать 4 адреса, из которых первый используется для адресации сети, второй и третий – для адресации узлов, а четвертый – в качестве широковещательного адреса.

В нижеприведенном примере (рис. 6.3, табл. 6.3), адресное пространство 192.168.100.0/24 использовано для создания 8 подсетей по 32 адреса в каждой, т.е. маска имеет единицы в 27 старших двоичных разрядах (255.255.255.224). Одна из последних подсетей (подсеть 6) разделена на субподсети, при этом используется маска (255.255.255.252). Каждая из субподсетей служит для связей «точка-точка».

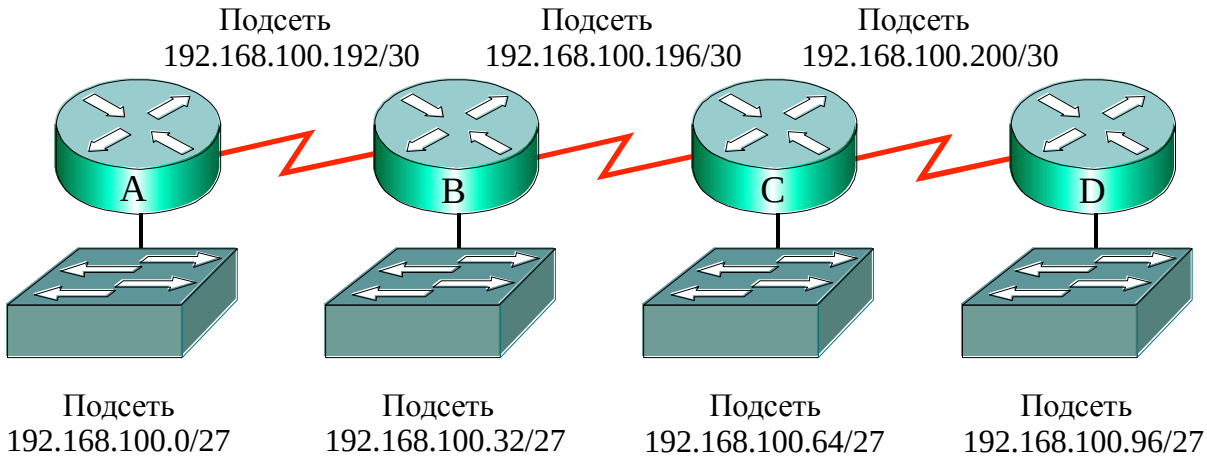


Рис.6.3. Пример использования масок переменной длины

Таблица 6.3

Формирование подсетей и субподсетей

Номер подсети	Адрес подсети	Число разрядов маски	Число узлов подсети
Подсеть 0	192.168.100.0	27	30
Подсеть 1	192.168.100.32	27	30
Подсеть 2	192.168.100.64	27	30
Подсеть 3	192.168.100.96	27	30
Подсеть 4	192.168.100.128	27	30
Подсеть 5	192.168.100.160	27	30
Подсеть 6	192.168.100.192	27	Используется для формирования субподсетей
Субподсеть 0	192.168.100.192	30	2
Субподсеть 1	192.168.100.196	30	2
Субподсеть 2	192.168.100.200	30	2
Субподсеть 3	192.168.100.204	30	2
Субподсеть 4	192.168.100.208	30	2
Субподсеть 5	192.168.100.212	30	2
Субподсеть 6	192.168.100.216	30	2
Субподсеть 7	192.168.100.220	30	2
Подсеть 7	192.168.100.224	27	30

Таким образом, за счет использования VLSM может быть сформировано 7 подсетей с числом узлов до 30 и восемь субподсетей с числом узлов 2. В распределенной составной сети (рис.6.3) четыре локальных сети (192.168.100.0/27, 192.168.100.32/27, 192.168.100.64/27, 192.168.100.96/27) и три сети «точка-точка».

Маски переменной длины VLSM позволяют создавать подсети разного размера. Например, сеть 198.11.163.0/24 может быть разбита на десять подсетей: две подсети по 62 узла в каждой, две подсети по 30 узлов, 2 подсети по 14 узлов и 4 подсети по 6 узлов в каждой (табл.6.4). Соответственно маски будут иметь размер: 26 – для первых двух подсетей, 27 – для третьей и четвертой подсети, 28 – для пятой и шестой, 29 – для четырех последних подсетей. Естественно, что могут быть реализованы и другие варианты деления сети на подсети и субподсети.

Важно помнить, что только неиспользованные подсети могут далее делиться на субподсети. Если какой-то адрес подсети уже используется, то подсеть на субподсети далее делиться не может.

Таблица 6.4

Формирование подсетей с использованием масок переменной длины

№ подсети	Маска	Адрес подсети	Число узлов	Адреса узлов
1	255.255.255.192	198.11.163.0	62	198.11.163.1 - 198.11.163.62
2	255.255.255.192	198.11.163.64	62	198.11.163.65 - 198.11.163.126
3	255.255.255.224	198.11.163.128	30	198.11.163.129 - 198.11.163.158
4	255.255.255.224	198.11.163.160	30	198.11.163.161 - 198.11.163.190
5	255.255.255.240	198.11.163.192	14	198.11.163.193 - 198.11.163.206
6	255.255.255.240	198.11.163.208	14	198.11.163.209 - 198.11.163.222
7	255.255.255.248	198.11.163.224	6	198.11.163.225 - 198.11.163.230
8	255.255.255.248	198.11.163.232	6	198.11.163.233 - 198.11.163.238
9	255.255.255.248	198.11.163.240	6	198.11.163.241 - 198.11.163.246
10	255.255.255.248	198.11.163.248	6	198.11.163.249 - 198.11.163.254

На рис.6.4 представлен еще один пример (в десятичной и двоичной системе) формирования пяти подсетей с маской длиной 26 единиц.

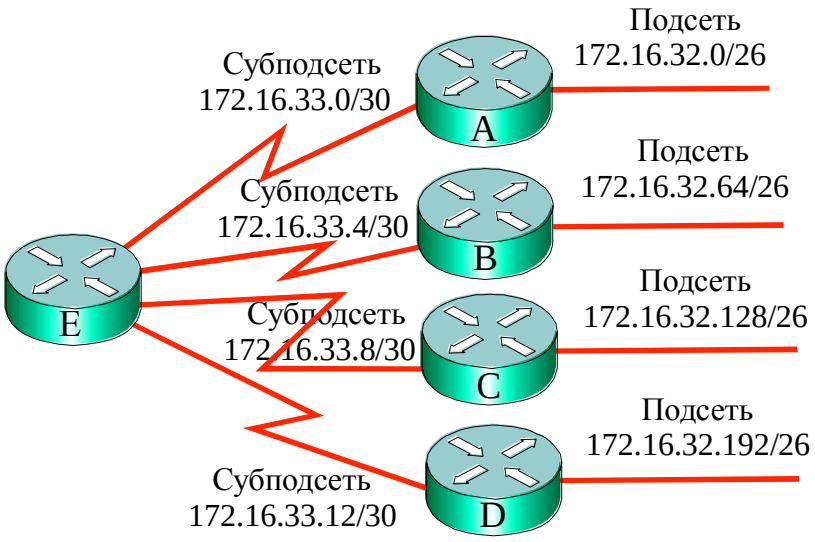


Рис.6.4. Использование подсетей и субподсетей

Подсети занимают адресное пространство от 172.16.32.0 до 172.16.33.63:

1) 172.16.32.0/26; – 10101100.00010000.00100000.00000000
2) 172.16.32.64/26; – 10101100.00010000.00100000.01000000
3) 172.16.32.128/26; – 10101100.00010000.00100000.10000000
4) 172.16.32.192/26; – 10101100.00010000.00100000.11000000
5) 172.16.33.0/26; – 10101100.00010000.00100001.00000000

Подсеть 172.16.33.0/26, далее подразделили на субподсети с маской длиной 30 разрядов (255.255.255.252).

При проектировании сетей может быть поставлена и обратная задача, когда несколько отдельных адресов необходимо объединить в один общий (**агрегированный**) адрес. Общую часть адреса, представленную старшими разрядами, называют **префиксом**. В ряде случаев это сокращает число записей в таблице маршрутизации. Например, сети

172.16.14.0 – 10101100.00010000.00001110.00000000 и
172.16.15.0 – 10101100.00010000.00001111.00000000

могут быть агрегированы (объединены) так, чтобы маршрутизаторы использовали только один маршрут для объединенной (**агрегированной**) сети 172.16.14.0/23, поскольку 23 разряда адреса обеих сетей одинаковы.

Тип маршрутизации, использующий агрегированные адреса, получил название **бесклассовой междоменной маршрутизации** (classless interdomain routing – **CIDR**), когда маршрутизация реализуется на основе префикса. Агрегирование маршрутов уменьшает нагрузку на маршрутизаторы.

Ниже рассмотрен следующий пример агрегирования адресов. Группа из четырех подсетей:

192.168.16.0/24 – 11000000.10101000.00010000.00000000
192.168.17.0/24 – 11000000.10101000.00010001.00000000
192.168.18.0/24 – 11000000.10101000.00010010.00000000
192.168.19.0/24 – 11000000.10101000.00010011.00000000

может быть представлена суммарным (агрегированным) адресом

192.168.16.0/22 – 11000000.10101000.00010000.00000000,

поскольку 22 разряда адреса у них одинаковы.

Аналогично группа из других четырех подсетей:

192.168.20.0/24 – 11000000.10101000.00010100.00000000
192.168.21.0/24 – 11000000.10101000.00010101.00000000
192.168.22.0/24 – 11000000.10101000.00010110.00000000

192.168.23.0/24 – 11000000.10101000.00010111.00000000

может быть представлена агрегированным адресом

192.168.20.0/22 – 11000000.10101000.00010100.00000000,

поскольку 22 разряда адреса у них также одинаковы.

Третья группа подсетей:

192.168.24.0/24 – 11000000.10101000.00011000.00000000

192.168.25.0/24 – 11000000.10101000.00011001.00000000

192.168.26.0/24 – 11000000.10101000.00011010.00000000

192.168.27.0/24 – 11000000.10101000.00011011.00000000

может быть представлена агрегированным адресом

192.168.24.0/22 – 11000000.10101000.00011000.00000000,

поскольку у них одинаковы 22 разряда адреса.

Агрегирование приведенных выше адресов иллюстрирует рис.6.5.

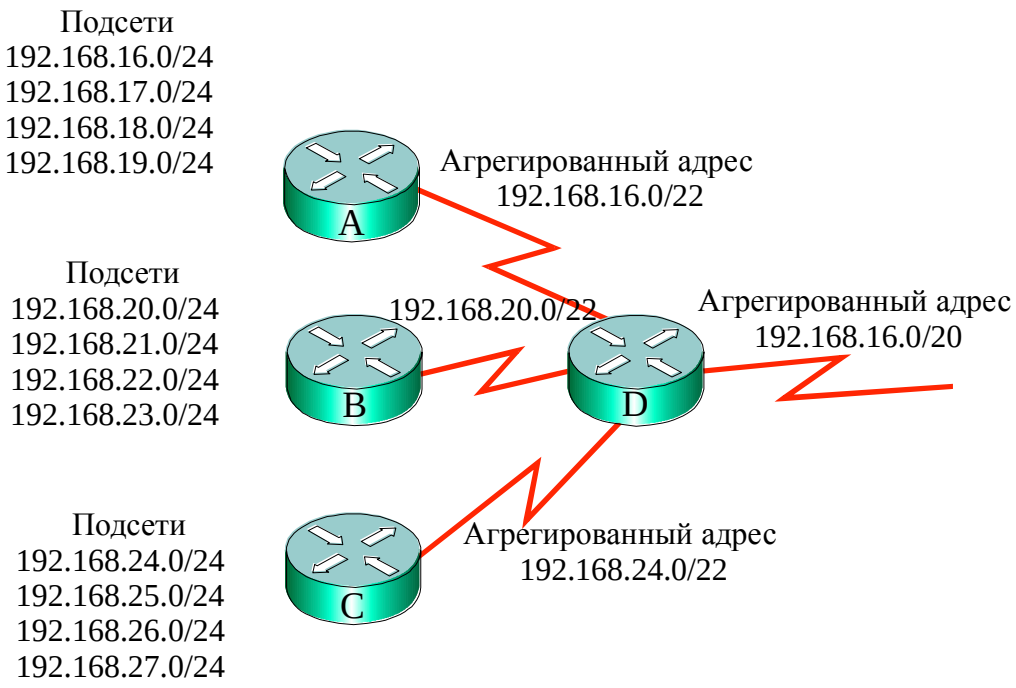


Рис.6.5. Агрегирование адресов маршрутов

Вместо адресов четырех подсетей в таблице маршрутизации каждого из маршрутизаторов A, B, C используется адрес только одного (агрегированного) маршрута с префиксом в 22 двоичных разряда. Адреса четырех указанных подсетей имеют общую часть – **префикс**, который используется как единый совокупный адрес. В маршрутизаторе D можно

сформировать агрегированный адрес всех трех групп подсетей. Он будет иметь адрес 192.168.16.0/20, т.е. маска (префикс) содержит 20 единиц в старших разрядах, поскольку все представленные на рис.6.5 адреса имеют двадцать одинаковых старших двоичных разрядов адреса.

Таким образом, итоговый суммарный маршрут трех групп подсетей (рис. 6.5) содержит префикс на 20 битов, общий для всех адресов в указанной сети – 192.168.16.0/20 - 11000000.10101000.00010000.00000000. Двадцать старших разрядов адреса (11000000.10101000.0001) используются как единый адрес организации, которая подключается к сети Интернет через маршрутизатор D.

Чтобы функционировала маршрутизация на основе префикса, адреса должны быть назначены иерархическим способом. Маршрутизатор должен знать номера всех присоединенных к нему подсетей и не должен сообщать другим маршрутизаторам о каждой подсети, если он может послать один совокупный маршрут (aggregate routes). Маршрутизатор, который использует агрегированные маршруты, реже обращается к таблице маршрутизации.

Маршрутизация на основе префикса и масок переменной длины возможна, если маршрутизаторы сети используют бесклассовый (classless) протокол маршрутизации, например, OSPF или EIGRP. **Бесклассовые протоколы маршрутизации** передают в обновлениях маршрутизации (routing updates) 32-разрядные IP-адреса и соответствующие маски.

6.4. Частные и общедоступные адреса

Адреса всех пользователей сети Internet должны быть уникальными. Первоначально уникальность адресов обеспечивал центр Internet Network Information Center (InterNIC), на смену которому пришла организация Internet Assigned Numbers Authority (IANA). **IANA управляет IP-адресами**, чтобы не произошло дублирования общедоступных адресов, распределяя их между пятью Региональными регистраторами адресов: ARIN (Северная Америка), RIPE (Россия и Европа), APNIC (Азия и Австралия), LACNIC (Латинская и Южная Америка), AfriNIC (Африка). Таким образом, все общественные (общедоступные) адреса должны быть зарегистрированы Региональным Интернет Регистратором (Regional Internet Regiestry – RIR), который

выделяет адреса сетевым операторам и провайдерам, а те, в свою очередь, выделяет адреса сетевым администраторам и отдельным пользователям.

В связи с быстрым ростом сети Internet, наблюдается дефицит общественных адресов. Радикально решить проблему дефицита IP-адресов может созданная новая шестая версия (**IPv6**) адресации в IP-сетях. До ее широкого внедрения для смягчения проблемы нехватки общественных адресов были разработаны новые схемы адресации, такие как адресация на основе масок переменной длины (VLSM) и бесклассовая междоменная маршрутизация (CIDR).

Кроме того, проблему нехватки общественных адресов может в некоторой мере ослабить использование частных адресов (Private IP addresses). Сети с частными адресами, не подключенные к Internet, могут иметь любые адреса, лишь бы они были уникальны внутри частной сети. Выход в Интернет пакетов с **частными адресами** блокируется маршрутизатором. Документ RFC 1918 устанавливает три блока частных адресов для использования внутри частных сетей (табл. 6.5).

Таблица 6.5

Диапазоны частных адресов

№	Диапазон адресов	Префикс
1	10.0.0.0 – 10.255.255.255	/8
2	172.16.0.0 – 172.31.255.255	/12
3	192.168.0.0 – 192.168.255.255	/16

Таким образом, данные адреса не могут быть использованы непосредственно в сети Интернет, т.к. маршрутизаторы отбрасывают пакеты с частными адресами. Чтобы узлы с частными адресами могли при необходимости подключаться к Интернет, используются специальные трансляторы частных адресов в общественные, например, **транслятор сетевых адресов** (Network Address Translation – **NAT**). Данный транслятор переводит один частный адрес в один общественный. Поэтому экономия IP-адресов может быть достигнута только за счет того, что не всем узлам частной сети разрешается выход в Интернет.

Второй тип трансляции сетевых адресов с использованием номеров портов (Port Address Translation – **PAT**), когда один общедоступный адрес

комбинируется с набором номеров порта узла источника. При этом один IP-адрес могут использовать сразу несколько узлов частной сети. Поэтому данный метод трансляции частных адресов в общественные эффективно экономит общедоступные IP-адреса.

6.5. Адреса версии IPv6

В настоящее время наблюдается дефицит адресов в связи с ростом числа пользователей Интернета, бурным развитием сетей мобильной связи, предоставляющих услуги передачи данных, использованием сетевых технологий для управления технологическими процессами и бытовой техникой. 32 двоичных разряда адреса версии IPv4 обеспечивают примерно 4 миллиарда адресов. В Северной Америке уже использованы все общественные адреса версии IPv4. Для снижения остроты дефицита в локальных сетях используются частные адреса, разработаны трансляторы NAT и PAT, используются маски переменной длины и адресация на основе префикса. Однако эти меры лишь предоставляли отсрочку полного истощения адресов версии IPv4.

Кардинальным решением данной проблемы является разработка и внедрение адресации версии IPv6. **Версия IPv6** использует для адресации 128 двоичных разрядов, что обеспечивает адресацию **$3{,}4\ 10^{38}$** объектов, вместо 32 разрядов версии IPv4, обеспечивающей адресацию **$4{,}3\ 10^{9}$** объектов. Со временем версия IPv6 заменит IPv4 в качестве основного сетевого протокола Internet Protocol.

Адреса версии IPv6 представлены в виде 8 блоков по 16 двоичных разрядов, которые записываются в шестнадцатеричной системе, т.е. каждый блок представлен в виде четырех шестнадцатеричных чисел. Блоки разделяются двоеточием. Ниже приведен пример адреса версии IPv6:

2af9:0000:7ee5:d947:0009:01c5:6b9f:00c4.

Для облегчения чтения впереди стоящие нули могут быть пропущены. При этом вышеприведенный адрес может быть записан в виде:

2af9:0:7ee5:d947:9:1c5:6b9f:c4.

Если в адресе имеется длинная последовательность нулей, например,

2af9:0:7ee5:0:0:0:6b9f:c4,

то запись можно сократить путем использования двух двоеточий подряд

2af9:0:7ee5::6b9f:c4.

Два двоеточия подряд в адресе могут быть использованы только один раз.

Таким образом, адрес 2af9:0:0:0:0:0:0f:c4 может быть представлен 2af9::c4.

Младшие разряды адреса нижнего уровня иерархии (идентификатор интерфейса) используется для задания номера узла, а старшие разряды – для задания **префикса адреса** (номера сети), как представлено на рис.6.6.

Префикс адреса (64 бита)		Идентификатор интерфейса (64 бита)	
127	64	63	0

Рис. 6.6. Уровни иерархии адреса IPv6

Причем старшие разряды адреса образуют несколько полей. Формат адреса IPv6 приведен ниже на рис. 6.7.

Наименование поля	FP	TLA	Резерв	NLA	SLA	Идентификатор интерфейса
Длина поля (бит)	3	13	8	24	16	64

Рис. 6.7. Формат адреса IPv6

Идентификатор интерфейса задает адрес узла (интерфейса) в определенной сети. Длина идентификатора интерфейса составляет 64 младших бита адреса (четыре младших блока из четырех шестнадцатеричных чисел). Это позволяет в поле идентификатора интерфейса размещать адреса конечных узлов различных сетевых технологий, например, физический MAC-адрес длиной 48 бит. При этом идентификаторы интерфейса могут быть динамически получены из адреса Уровня 2. Поэтому отпадает необходимость в протоколе ARP, который связывает IP-адреса и соответствующие MAC-адреса, что ускоряет процесс продвижения пакета через маршрутизатор. В этом поле могут также задаваться адреса других

протоколов, например, ATM-адреса, номера телефонов международной и междугородной связи, номера мобильных телефонов, а также **адреса IPv4**.

Поле префикса формата (FP – Format Prefix) версии IPv6 имеет размер 3 бита и значение в двоичном коде 001. Поэтому адреса версии IPv6 будут начинаться либо с шестнадцатеричной цифры 2 (0010), либо 3 (0011).

Поле агрегирования верхнего уровня (TLA – Top-Level Aggregation) задает адреса сетей пяти основных регистратров Европы, Азии, Северной Америки, Южной Америки, Африки (ARIN, RIPE, APNIC, LACNIC, AfriNIC). 13 разрядов этого поля позволяет адресовать 8196 сетей. Поле префикса формата FP и поле агрегирования верхнего уровня TLA составляют 16 старших бит адреса IPv6, они выделяются и управляются организацией IANA и пятью основными регистраторами адресов. Для возможности расширения этого поля в будущем зарезервировано еще 8 разрядов. С учетом префикса формата (001) первая сеть IPv6 будет иметь номер 2001.

Поле агрегирования следующего уровня (NLA – Next-Level Aggregation) адресует сети мелких и средних провайдеров. 24 разряда этого поля позволяют адресовать примерно 16 миллионов сетей.

Поле местного уровня (SLA – Site-Level Aggregation) используется для адресации подсетей пользователя. Таким образом, в распоряжении сетевого администратора имеется 16 двоичных разрядов, что позволяет организации адресовать до 65 535 отдельных подсетей.

Кроме формата (рис.6.7) для описания адреса IPv6 используется также формат (рис.6.8), где 48 старших бита адреса образуют префикс сайта (Site Prefix), из которых 32 старших – образуют префикс провайдера (ISP Prefix).

Так как в поле идентификатора интерфейса могут задаваться адреса IPv4, то обеспечивается совместимость IPv4 и IPv6. Для преобразования адреса IPv6 в адрес IPv4 разработан подтип адреса, в котором 4 младших байта содержат адрес предыдущей версии IPv4, а старшие 12 байт – содержат нули. При преобразовании адреса IPv4 в адрес IPv6 младшие 4 байта содержат адрес версии IPv4, байты 5 и 6 содержат единицы, а старшие 10 байт содержат нули.

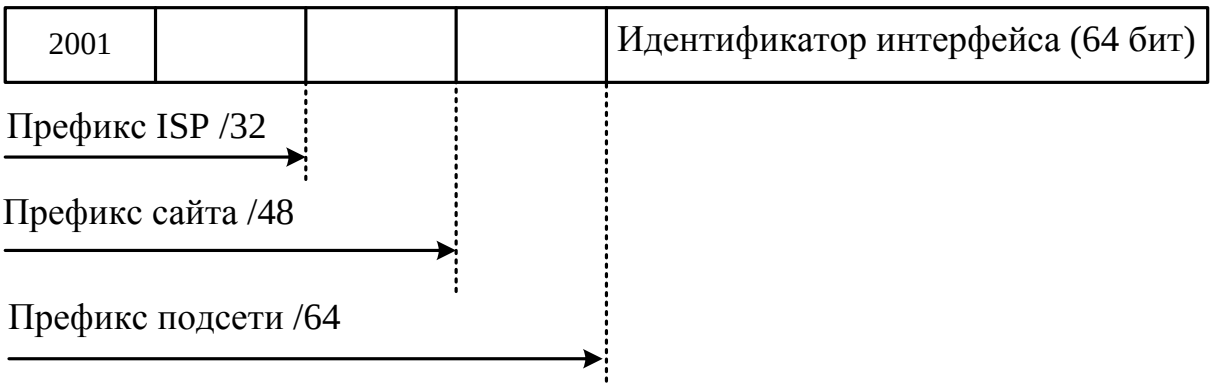


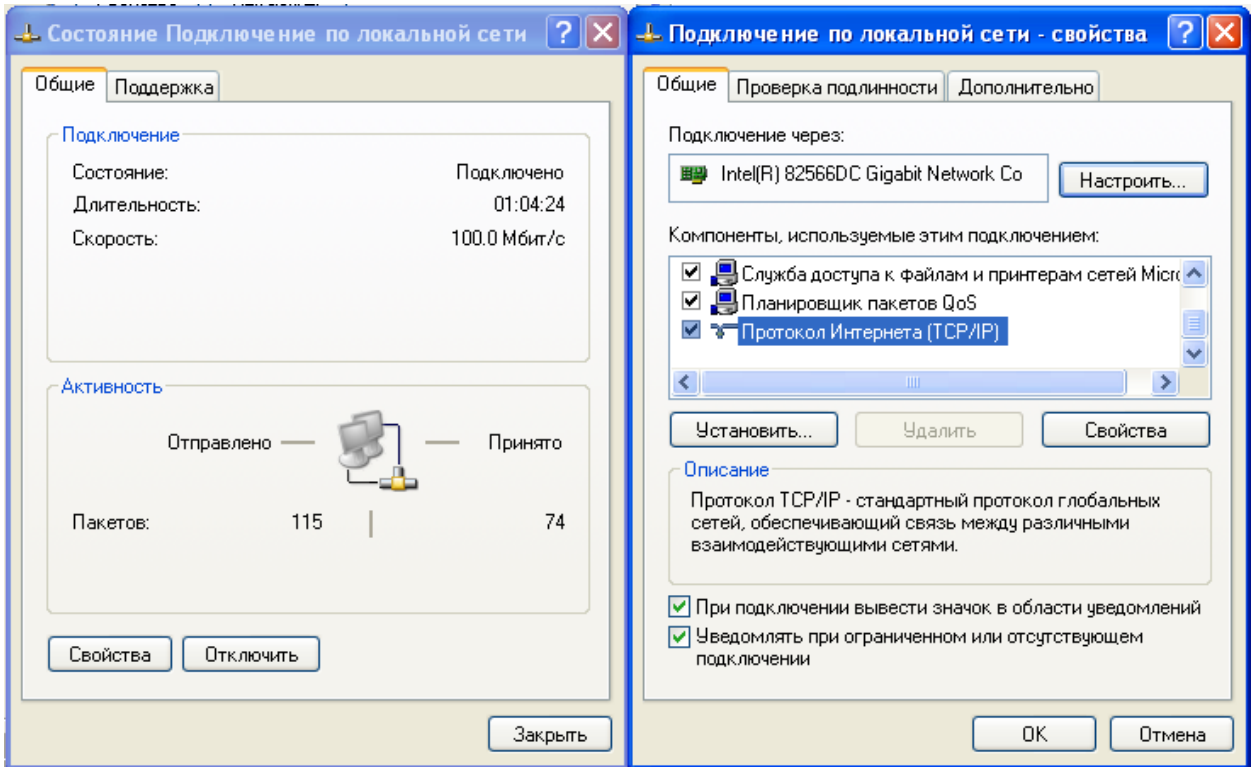
Рис. 6.8. Префиксы формата адреса IPv6

На период перехода от IPv4 к IPv6 разработано несколько механизмов. Например, механизм двойного стека, когда устройства поддерживают оба протокола, причем, IPv6, является привилегированным. То есть, на интерфейсах устройств конфигурируется **два стека протоколов**. Устройство с двойным стеком определяет, какой стек использовать, базируясь на адресе назначения пакета, отдавая предпочтение IPv6, когда это возможно.

6.6. Назначение IP-адресов

Назначение IP-адреса может производиться администратором вручную или автоматически с помощью DHCP-сервера. Для назначения адреса вручную обычно в главном меню компьютера необходимо последовательно выбрать следующие опции: “*Пуск*”, “*Настройка*”, “*Панель управления*”, “*Сетевые подключения*”, “*Подключение по локальной сети*”,

Во всплывшем окне (рис. 6.9а) выбрать “*Свойства*”. В следующем окне выбрать “*Протокол Интернета (TCP/IP)*” (рис. 6.9б), затем “*Свойства*”. Вручную назначаются адреса сетевым принтерам, серверам и интерфейсам маршрутизаторов.



а) б)

Рис. 6.9. Окна выбора протокола TCP/IP

После этого необходимо назначить IP-адрес, маску подсети и основной шлюз по умолчанию (рис. 6.10).

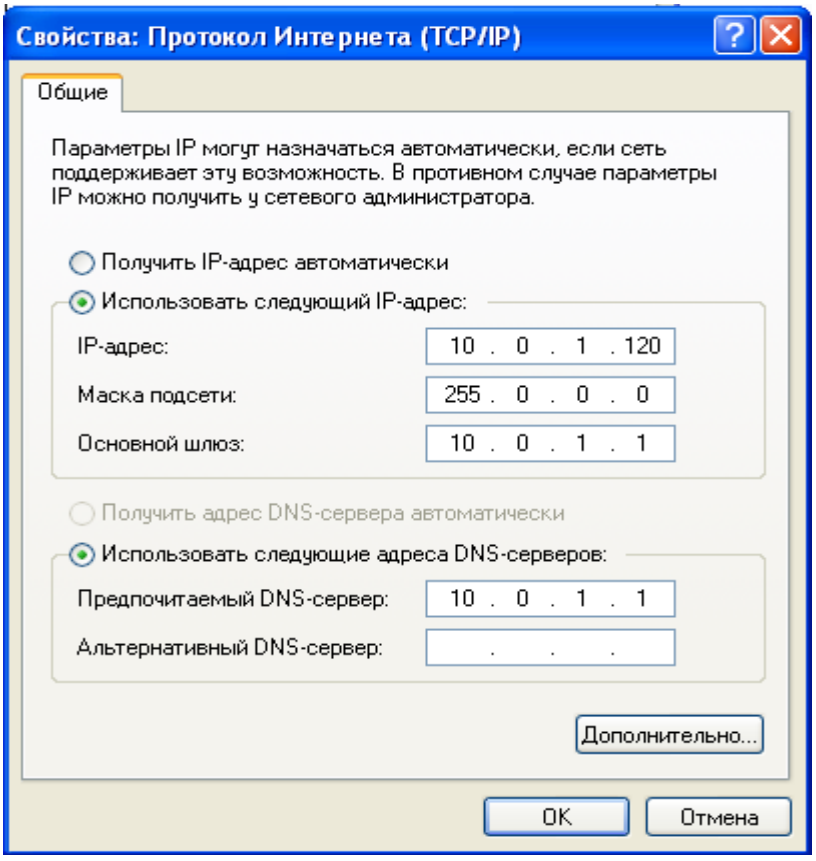


Рис. 6.10. Назначение IP-адреса администратором вручную

Из протоколов автоматического назначения IP-адреса устройств (хостов – host) в настоящее время используется **протокол динамического конфигурирования узлов** Dynamic Host Configuration Protocol (**DHCP**), который позволяет узлу динамически без участия администратора получать IP-адрес. Нужно только определить диапазон IP-адресов на DHCP-сервере.

Для запроса IP-адреса узел посылает в локальную сеть (рис.6.11) запрос с широковещательным IP-адресом назначения – 255.255.255.255 и MAC-адресом – FF:FF:FF:FF:FF:FF. В качестве MAC-адреса источника в запросе указывается адрес запрашивающего узла 01:AA:11:AA:11:AA. Такой запрос поступает на все устройства сети, в том числе на сервер DHCP. Все устройства отбрасывают пакет с запросом, за исключением сервера, который опознает адресованный ему запрос.

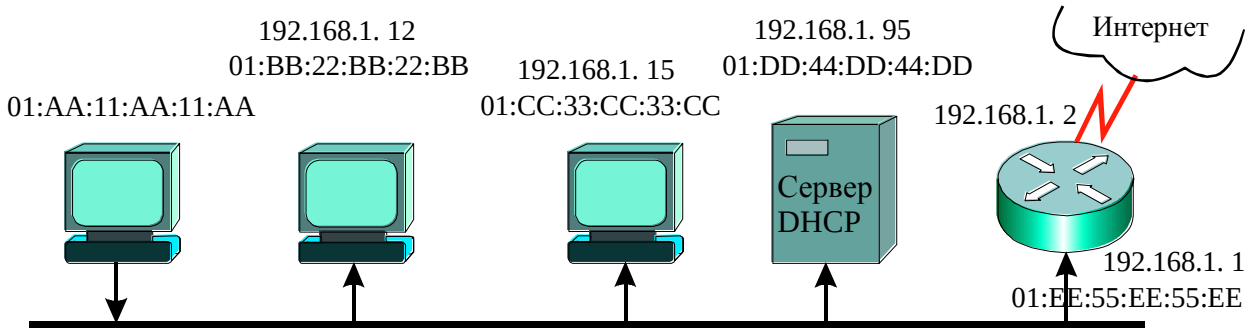


Рис. 6.11. Передача ответа сервера DHCP

При получении запроса DHCP-сервер формирует ответ, в котором указывается выделяемый в аренду узлу IP-адрес. В заголовке ответа в качестве MAC-адреса назначения указывается адрес запрашивающего узла (01:AA:11:AA:11:AA). Поэтому все устройства отбрасывают пакет с ответом, за исключением узла, пославшего запрос. Кроме выделяемого в аренду IP-адреса в ответе DHCP-сервера содержится адрес основного шлюза по умолчанию и другая информация. На рис. 6.9 основной шлюз имеет IP-адрес 192.168.1.1 и MAC-адрес 01:EE:55:EE:55:EE. Важным свойством DHCP является способность выделять IP-адрес в аренду динамически, т.е. сервер может изымать неиспользуемый адрес, а затем восстанавливать пользователю адрес, который использовался ранее.

Краткие итоги лекции 6

1. Объединение нескольких локальных сетей в глобальную (распределенную, составную) WAN сеть происходит с помощью устройств и протоколов сетевого Уровня 3 семиуровневой эталонной модели OSI.
2. Наиболее распространенными устройствами межсетевого взаимодействия сетей, подсетей и устройств являются маршрутизаторы.
3. Маршрутизаторы имеют как LAN, так и WAN интерфейсы и поэтому являются устройствами как локальных, так и глобальных сетей.
4. Логические адреса задаются администратором или назначаются динамически протоколом DHCP из диапазона выделенных адресов.
5. Логические адреса узлов в IP-сетях версии IPv4 содержат 32 двоичных разряда, версии IPv6 – 128 двоичных разряда.
6. IP-адреса являются иерархическими. Старшие разряды определяют номер сети, а младшие разряды – номер узла в сети.
7. Существует адресация на основе классов и бесклассовая адресация.
8. Адрес 127.0.0.1 предназначен для самотестирования, когда проверяют, установлен ли протокол TCP/IP на хосте.
9. В таблице маршрутизации задаются адреса сетей для сокращения записей, которыми оперирует маршрутизатор.
10. Адрес сети маршрутизатор получает путем логического умножения сетевого адреса узла на маску.
11. Общая часть адреса называется префиксом.
12. В маршрутизаторах используют как адресацию на основе стандартных масок, так и адресацию с масками переменной длины.
13. Маски переменной длины позволяют создавать подсети разного размера.
14. Агрегированный адрес получается путем объединения адресов в один общий.
15. Радикально решить проблему дефицита IP-адресов может новая шестая версия (IPv6) адресации в IP-сетях.
16. Сети с частными адресами, не подключенные к Internet, могут иметь любые адреса, лишь бы они были уникальны внутри частной сети.
17. Пакеты с частными адресами блокируются маршрутизатором.
18. Трансляторы сетевых адресов переводят частные адреса в общественные.
19. Кардинальным решением проблемы нехватки логических адресов является разработка и внедрение адресации версии IPv6, которая использует для адресации 128 двоичных разрядов.
20. Адреса версии IPv6 представлены в виде 8 блоков по четыре шестнадцатеричных числа. Блоки разделяются двоеточием.
21. Формат адреса IPv6 можно представить в виде поля идентификатора интерфейса (младшие 64 бита, которые задают адрес узла) и полей префиксов подсети, сайта и провайдера (старшие 64 бита).
22. Основным протоколом автоматического назначения IP-адресов устройств является протокол динамического конфигурирования узлов DHCP.

Вопросы по лекции 6

1. Кто назначает логические адреса интерфейсам и конечным узлам сети?
2. Сколько двоичных разрядов содержат логические адреса узлов в IP-сетях версии IPv4?
3. Что определяют старшие и младшие разряды сетевого адреса?
4. Какие классы уникальных адресов используются в сетях?
5. Какие размеры имеют стандартные маски адресов классов A, B, C?
6. Какое максимальное число узлов могут задавать адреса класса C?
7. Какой адрес используется для самотестирования?
8. Какие параметры задаются в таблицах маршрутизации?
9. Для чего нужны сетевые маски?
10. Как называется общая часть адреса нескольких устройств?
11. Для чего необходимы маски переменной длины?
12. Что позволит радикально решить проблему дефицита IP-адресов?
13. Сколько двоичных разрядов содержат логические адреса узлов в IP-сетях версии IPv6?
14. Как представлены адреса версии IPv6?
15. Для чего используются частные адреса в локальных сетях?
16. Каковы диапазоны частных адресов?
17. Можно ли использовать частные адреса в сети Интернет?
18. Что переводит частные адреса в общественные?
19. Какие протоколы автоматически назначают IP-адреса устройств?
20. Какие IP-параметры назначает администратор вручную?

Упражнения

1. Приведите примеры адресов конечных узлов классов A, B, C. Используя стандартные маски, рассчитайте адреса соответствующих сетей.
2. Переведите адреса 10.169.77.19; 172.18.190.59; 192.168.55.112 в двоичную систему.
3. Рассчитайте максимальное количество хостов в подсетях 10.169.77.16/28; 172.18.190/27; 192.168.55.112/29.
4. Для выделенного диапазона адресов 172.16.10.0/24 сформируйте 10 подсетей по 8 – 14 компьютеров в каждой. Какова будет сетевая маска?
5. Для выделенного адреса 10.1.5.0/24 сформируйте 2 подсети по 50 – 60 компьютеров, 2 подсети по 25 – 30 компьютеров, 2 подсети по 10 – 12 компьютеров, 2 подсети по 5 – 6 компьютеров, остальные адреса использовать для адресации соединений «точка -точка».
6. Каким агрегированным адресом может быть представлена группа из четырех подсетей: 172.16.16.0/24, 172.16.17.0/24, 172.16.18.0/24, 172.16.19.0/24?
7. На компьютере посмотрите и объясните, как получен IP-адрес (автоматически или назначен администратором).

Лекция 7. ФУНКЦИИ МАРШРУТИЗАТОРОВ

Краткая аннотация лекции: приведены основные устройства и методы межсетевого взаимодействия, основные элементы маршрутизаторов, принципы маршрутизации, функции протокола ARP, функционирование таблиц маршрутизации..
Цель лекции: изучить принципы и средства межсетевого взаимодействия.

7.1. Маршрутизаторы в сетевых технологиях

Устройствами, объединяющими нескольких локальных сетей в глобальную (**распределенную, составную**) WAN в составную сеть, являются: **маршрутизаторы** (routers), модемы, коммуникационные серверы. Наиболее распространенными устройствами межсетевого взаимодействия сетей, подсетей и устройств являются **маршрутизаторы**. Они представляют собой специализированные компьютеры для выполнения специфических функций сетевых устройств.

На рис.6.1 приведен пример того, как локальные сети через последовательный интерфейс маршрутизатора С соединены с сетью Интернет (Internet). В большинстве случаев соединение маршрутизатора локальной сети с сетью Интернет производится через сеть провайдера. Терминальное (оконечное) оборудование (Data Terminal Equipment - **DTE**), к которому относится и маршрутизатор, подсоединяется к глобальной сети (или к сети провайдера) через канальное телекоммуникационное оборудование (Data Communications Equipment или Data Circuit-terminating Equipment – **DCE**). Маршрутизатор обычно является оборудованием пользователя, а оборудование DCE предоставляет провайдер. Услуги, предоставляемые провайдером для терминальных устройств DTE, доступны через модем или каналообразующее оборудование, согласующее с каналом устройство (Channel Service Unit /Data Service Unit – **CSU/DSU**), которые и являются оборудованием DCE (рис. 7.1).

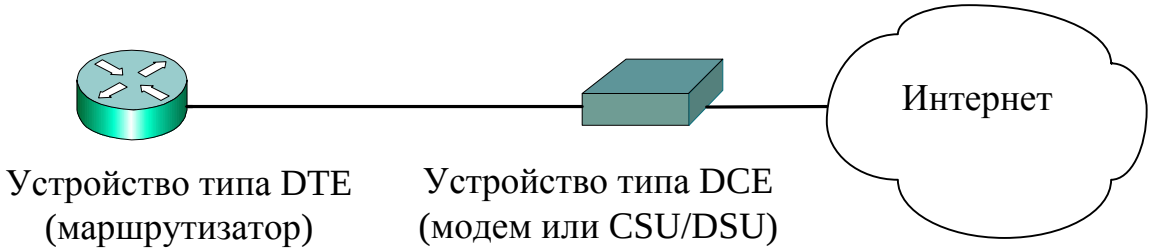


Рис.7.1. Устройства распределенных сетей

Оборудование DCE является ведущим в паре DCE – DTE, оно обеспечивает синхронизацию и задает скорость передачи данных.

Поскольку маршрутизаторы в распределенных сетях (рис. 6.1) часто соединяются последовательно, то из двух последовательно соединенных серийных интерфейсов маршрутизаторов один должен выполнять роль устройства DCE, а второй – устройства DTE (рис.7.2).

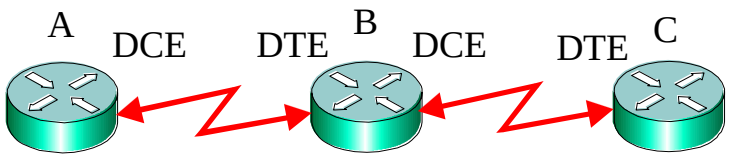


Рис. 7.2. Последовательное соединение маршрутизаторов

Главными функциями маршрутизаторов являются:

1. **Выбор наилучшего (оптимального) пути** для пакетов к адресату назначения.
2. **Продвижение** (коммутация) принятого пакета с входного интерфейса на соответствующий выходной интерфейс.

Таким образом, маршрутизаторы обеспечивают связь между сетями и определяют наилучший путь пакета данных к сети адресата, причем, **технологии объединяемых локальных сетей могут быть различными**.

Протоколы канального (data link) уровня WAN описывают, как по сети передаются кадры. Они включают протоколы, обеспечивающие функционирование через выделенные соединения точка-точка и через коммутируемые соединения. Основными WAN протоколами и стандартами канального уровня являются: High-level data link control (HDLC), Point-to-Point Protocol (PPP), Synchronous Data Link Control (SDLC), Serial Line Internet Protocol (SLIP), X.25, Frame Relay, ATM. Основными протоколами и стандартами физического уровня являются: EIA/TIA-232, EIA/TIA-449, V.24, V.35, X.21, G.703, EIA-530, xDSL, PDH, SDH, OTN и др.

Функционируя на Уровне 3 модели OSI, маршрутизаторы принимают решения, базируясь на сетевых логических адресах (IP-адресах). Для определения наилучшего пути передачи данных через связываемые сети, **маршрутизаторы строят таблицы маршрутизации** и **обмениваются сетевой маршрутной информацией** с другими маршрутизаторами.

Администратор может конфигурировать статические маршруты и поддерживать таблицы маршрутизации вручную. Однако большинство таблиц маршрутизации создается и поддерживается динамически, за счет использования **протоколов маршрутизации** (**routing protocol**), которые позволяют маршрутизаторам автоматически обмениваться друг с другом информацией о сетевой топологии.

Функционирование маршрутизаторов происходит под управлением сетевой операционной системы (*Internetwork Operation System* – **IOS**), текущая (*running*) версия которой находится в оперативной памяти RAM (рис.6.4). Помимо текущей версии IOS оперативная память хранит активный **конфигурационный файл** (Active Configuration File), таблицы протоколов динамической маршрутизации, выполняет буферизацию пакетов и поддерживает их очередь, обеспечивает временную память для конфигурационного файла маршрутизатора пока включено питание.

Загрузка операционной системы IOS в оперативную память обычно производится из энергонезависимой флэш-памяти (**Flash**), которая является перепрограммируемым запоминающим устройством (**ППЗУ**). После модернизации IOS она перезаписывается во флэш-память, где может храниться несколько версий. Версию операционной системы можно также сохранять на TFTP-сервере (рис.7.3).

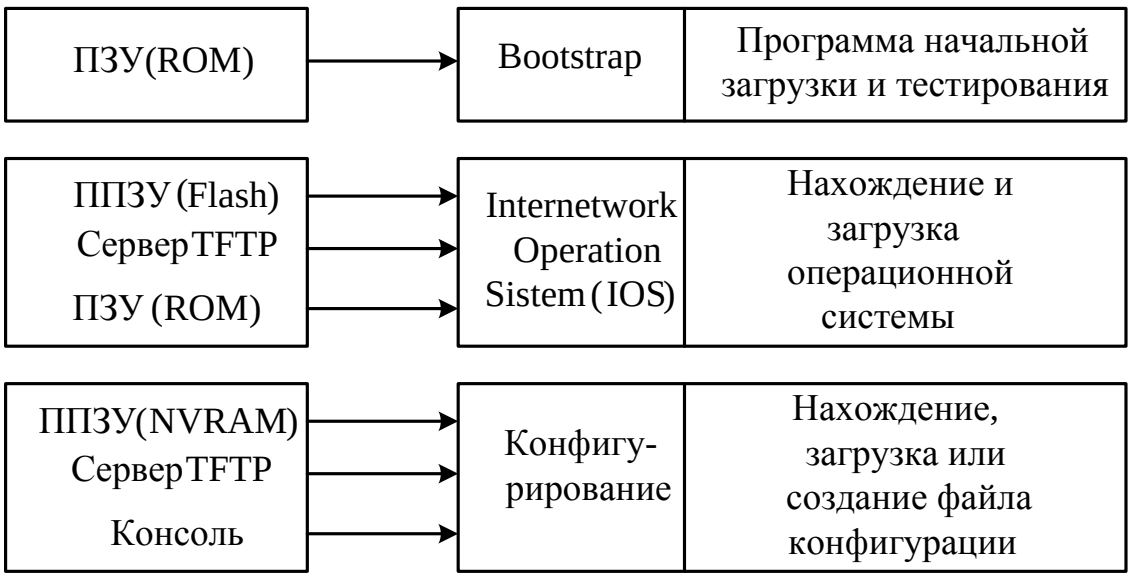


Рис.7.3. Элементы памяти и программы маршрутизатора

Постоянное запоминающее устройство (ПЗУ – ROM) содержит программу начальной загрузки (bootstrap) и сокращенную версию операционной системы, установленную при изготовлении маршрутизатора. Обычно эта версия IOS используется только при выходе из строя Flash памяти. Память ROM также поддерживает команды для теста диагностики аппаратных средств (power-on self test - POST).

Энергонезависимая (non-volatile) оперативная память **NVRAM** маршрутизатора является перепрограммируемым запоминающим устройством (ППЗУ). NVRAM хранит стартовый (*startup*) конфигурационный файл, который после изменения конфигурации перезаписывается в ППЗУ, где создается резервная копия (*backup*). **Конфигурационные файлы содержат команды и параметры** управления потоком трафика, проходящим через маршрутизатор. Конфигурационный файл используется для выбора сетевых протоколов и протоколов маршрутизации, которые определяют наилучший путь для пакетов к адресуемой сети. Первоначально конфигурационный файл обычно создается с консольной линии (*console*) и помимо памяти NVRAM может сохраняться на TFTP-сервере (рис. 7.3). Временное хранение входящих и исходящих пакетов обеспечивается в памяти интерфейсов, которые могут быть выполнены на материнской плате или в виде отдельных модулей.

При включении маршрутизатора начинает функционировать программа начальной загрузки *bootstrap*, которая тестирует оборудование и загружает операционную систему IOS в оперативную память RAM. В оперативную память загружается также конфигурационный файл, хранящийся в NVRAM. В процессе конфигурирования маршрутизатора задаются адреса интерфейсов, пароли, создаются таблицы маршрутизации, устанавливаются протоколы, проводится проверка параметров. Процесс коммутации и продвижения данных проходит под управлением операционной системы.

7.2. Принципы маршрутизации

Информационный поток данных, созданный на прикладном уровне, на транспортном уровне “нарезается” на **сегменты**, которые на сетевом уровне снабжаются заголовками и образуют **пакеты**. Заголовок пакета содержит **сетевые IP-адреса** узла назначения и узла источника. На основе этой информации устройства сетевого уровня (маршрутизаторы) осуществляют передачу пакетов между узлами составной сети по определенному маршруту.

Маршрутизатор оценивает доступные пути к адресату назначения и выбирает наиболее рациональный маршрут на основе некоторого критерия – **метрики**. При оценке возможных путей маршрутизаторы используют информацию о топологии сети. Эта информация может быть сконфигурирована сетевым администратором или собрана в ходе динамического процесса обмена информацией между маршрутизаторами, который выполняется в сети протоколами маршрутизации.

Пакет, принятый на одном (*входном*) интерфейсе, маршрутизатор должен отправить (продвинуть) на другой (*выходной*) интерфейс (порт), который соответствует наилучшему пути к адресату. Чтобы передать пакеты от исходной сети (от источника) до сети адресата (назначения), на сетевом Уровне 3 маршрутизаторы используют таблицы маршрутизации для определения наиболее рационального пути.

Процесс прокладывания маршрута происходит последовательно от маршрутизатора к маршрутизатору. При прокладывании пути каждый маршрутизатор анализирует сетевую часть адреса узла назначения, заданного в заголовке поступившего пакета, т.е. вычленяет адрес сети назначения из адреса узла. Затем маршрутизатор обращается к таблице маршрутизации, где хранятся адреса всех доступных сетей, и определяет свой выходной интерфейс, на который необходимо передать (продвинуть) пакет. Итак, **маршрутизатор ретранслирует пакет**, продвигая его с входного интерфейса на выходной, при этом используя адрес назначения и таблицу маршрутизации.

Выходной интерфейс связан с наиболее рациональным маршрутом к адресату. Конечный маршрутизатор на пути пакета непосредственно (прямо) связан с сетью назначения. Он использует логический (IP) и физический (MAC) адрес узла назначения, чтобы доставить пакет получателю данных.

Процесс ретрансляции пакетов маршрутизаторами рассмотрен на примере сети, приведенной на рис. 7.4. Маршрутизаторы в целом сетевого адреса не имеют, но поскольку они связывают между собой несколько сетей, то **каждый интерфейс** (порт) маршрутизатора **имеет уникальный адрес,** сетевая часть которого совпадает с номером сети, соединенной с данным интерфейсом. Последовательные (*serial*) порты, соединяющие между собой маршрутизаторы, на рисунке обозначены молниевидной линией.

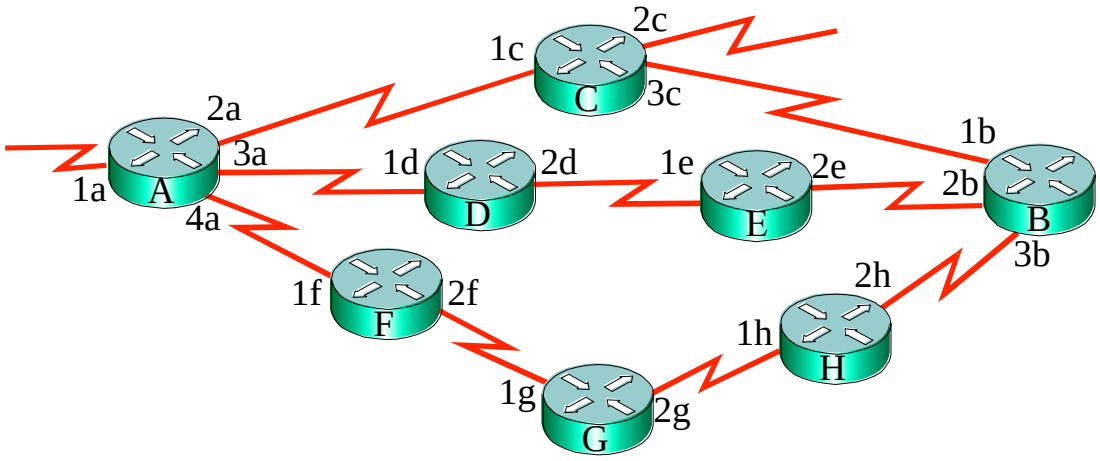


Рис. 7.4. Определения пути пакета

Путь от маршрутизатора A к маршрутизатору B может быть выбран:

1. Через маршрутизатор C;
2. Через маршрутизаторы D и E;
3. Через маршрутизаторы F, G и H.

Оценка *наилучшего пути* производится на основе *метрики*. Например, если метрика учитывает только количество маршрутизаторов на пути к адресату, то будет выбран первый маршрут. Если же метрика учитывает полосу пропускания линий связи, соединяющих маршрутизаторы, то может быть выбран второй или третий маршрут, если на этом пути иболее широкополосные линии связи.

При выборе первого пути, функция коммутации реализуется за счет продвижения поступившего на интерфейс 1a маршрутизатора A пакета на интерфейс 2a. Таким образом, пакет попадает на интерфейс 1c маршрутизатора C, который продвинет полученный пакет на свой выходной интерфейс 3c, и затем передаст полученный пакет маршрутизатору B.

В процессе передачи пакета по сети используются как сетевые логические адреса (IP-адреса), так и физические адреса устройств (MAC-адреса в сетях Ethernet). Например, при передаче информации с компьютера Host X локальной сети Сеть 1, (рис.7.5) на компьютер Host Y, находящийся в удаленной Сети 2, определен маршрут через маршрутизаторы A, B, C.

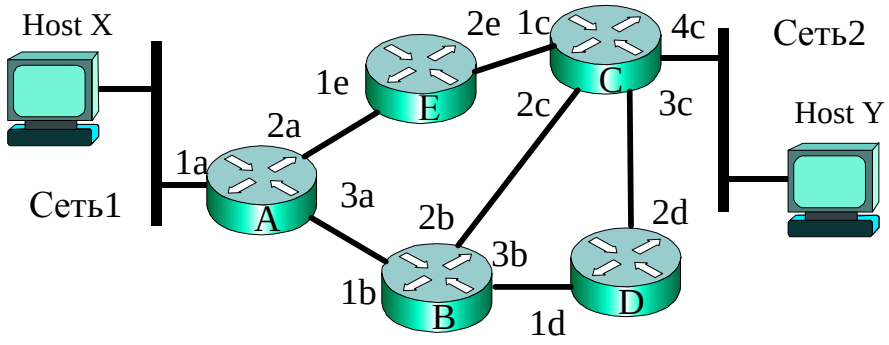


Рис. 7.5. Маршрутизаторы в сети передачи данных Ethernet

Когда узел Host X Сети 1 передает пакет адресату Host Y из другой Сети 2, ему известен сетевой IP-адрес получателя, который записывается в заголовке пакета, т.е. известен адрес 3-го уровня. При инкапсуляции пакета в кадр источник информации Host X должен задать в заголовке кадра адреса назначения и источника канального уровня, т.е. адрес 2-го уровня (рис.7.6).

Заголовок кадра		Заголовок пакета		Поле данных	Концевик (трейлер)
MAC-адрес назначения	MAC-адрес источника	IP-адрес назначения	IP-адрес источника	Данные	Контрольная сумма

Рис. 7.6. Основные поля кадра

У передающего узла нет информации об адресе канального уровня (MAC-адресе) узла назначения Host Y, поэтому Host X в заголовке кадра задаст MAC-адрес входного интерфейса 1a маршрутизатора A. Именно через этот интерфейс, называемый **шлюзом по умолчанию** (**Default Gateway**), все пакеты из локальной Сети 1 будут передаваться в удаленные сети. Однако и этот адрес источнику информации Host X не известен. Процесс нахождения MAC-адреса по известному сетевому адресу реализуется с помощью **протокола разрешения адресов** (Address Resolution Protocol – **ARP),** который входит в стек протоколов TCP/IP.

7.3. Протокол ARP

В локальных сетях телекоммуникаций на основе дейтаграмм устройствам необходимы как MAC-адрес, так и IP-адрес, которые для каждого узла образуют соответствующую пару. Протоколы и устройства Уровня 2 и Уровня 3 модели OSI постоянно взаимодействуют при передаче данных по сети (рис. 7.7).

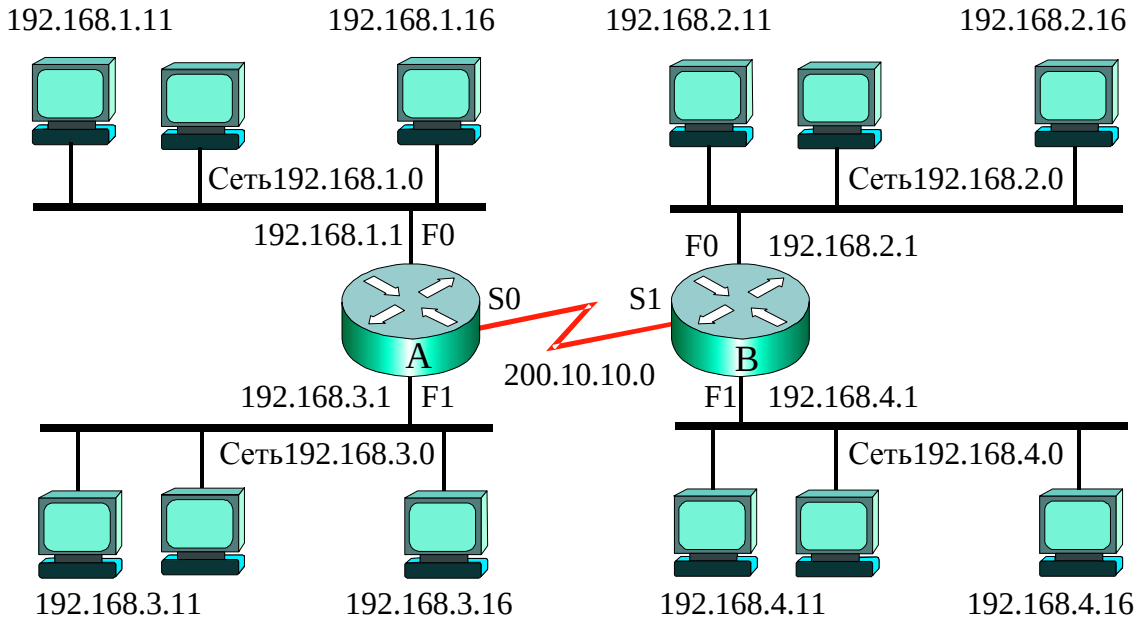


Рис. 7.7. Взаимодействие протоколов и устройств

Это проявляется в виде взаимодействия таблиц протокола ARP (табл. 7.1), функционирующих на Уровне 2, и таблиц маршрутизации протоколов Уровня 3 модели OSI. Каждый компьютер и порт маршрутизатора поддерживает таблицы ARP, каждая строка которых содержит пару соответствующих IP- и MAC-адресов и функционируют только в пределах широковещательного домена, т.е. в пределах сети или подсети.

Таблица 7.1

Таблица ARP маршрутизатора A

IP адрес	MAC адрес
192.168.1.11	0001AAAA1111
…	…
192.168.3.11	0003AAAA3333

На каждом конечном узле можно посмотреть его физический адрес и IP-адрес по команде **ipconfig /all** (рис.7.8). Из распечатки следует, что физическим MAC-адресом конечного узла является 00-19-D1-93-7E-BE, а логическим IP-адресом – 10.0.118.52.

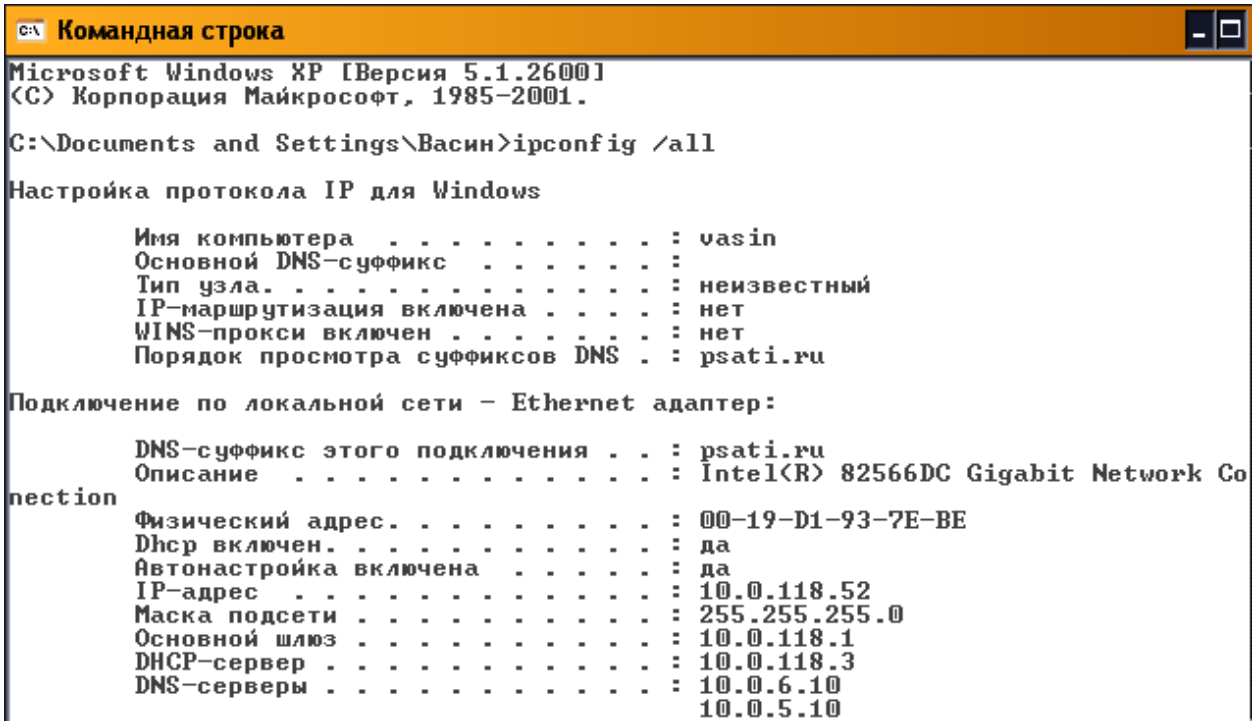


Рис. 7.8. Результат выполнения команды ipconfig /all

Протокол ARP может по IP-адресу автоматически определить MAC-адрес устройства. Каждое устройство в сети поддерживает таблицу **ARP table**, которая содержит соответствующие пары MAC и IP адреса других устройств той же локальной сети. Таблица ARP любого узла может быть просмотрена по команде **arp –a** (рис. 7.9). Записи таблицы хранятся в памяти RAM, где динамически поддерживаются.

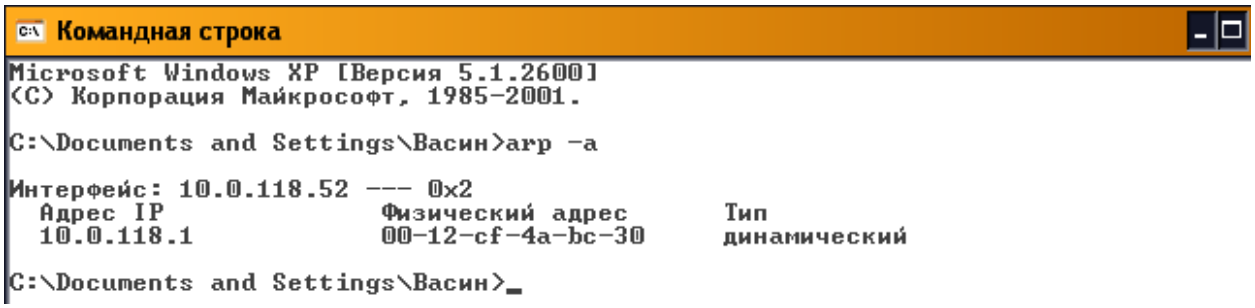


Рис. 7.9. Таблица ARP

Если узлы долго не передают данные, то соответствующие записи из таблицы удаляются, что отображает рис. 7.9, где таблица содержит только одну пару IP и MAC адресов.

Таблица ARP пополняется динамически путем контроля трафика локального сегмента сети. Все станции локальной сети Ethernet анализируют трафик, чтобы определить, предназначены ли данные для них. При этом IP и MAC-адреса источников дейтаграмм записываются в таблице ARP. Например, после общения с узлом 10.0.118.65 в таблице ARP (рис. 7.10) появляется вторая запись (сравните с рис.7.9).

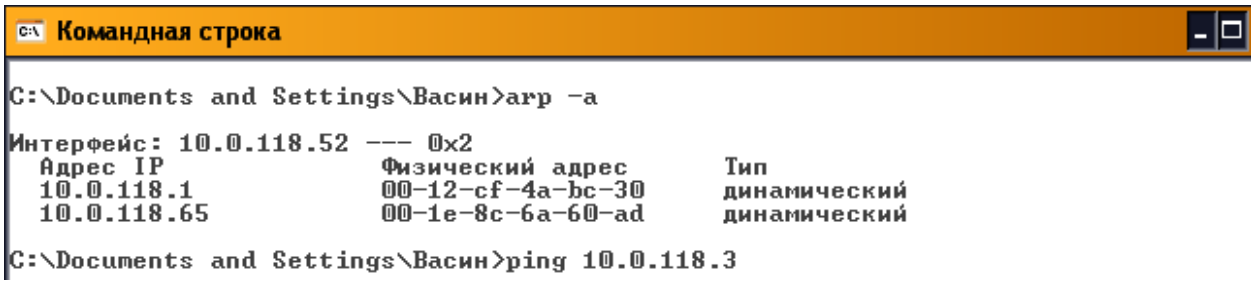


Рис. 7.10. Изменения в таблице ARP

Когда устройство передает пакет по IP-адресу назначения, оно проверяет, имеется ли в ARP-таблице соответствующий MAC-адрес назначения. Если соответствующая запись имеется, то она используется при инкапсуляции пакета в кадр данных. Данные передаются по сетевой среде, устройство назначения принимает их.

Если узел не находит соответствующей записи в таблице ARP, то он для получения MAC-адреса назначения посылает в локальную сеть *широковещательный ARP-запрос*, в котором задается сетевой логический IP-адрес устройства назначения. Все другие устройства сети анализируют его. Если у одного из локальных устройств IP-адрес совпадает с запрашиваемым, то устройство посылает ARP-ответ, который содержит пару IP и MAC адресов. Эта пара IP и MAC адресов записывается в ARP-таблице. Если в локальной сети нет запрашиваемого IP-адреса, то устройство источник сообщает об ошибке.

Когда данные передаются за пределы локальной сети, то для передачи сообщения необходимы IP и MAC-адреса как устройства назначения, так и промежуточных маршрутизирующих устройств. Поскольку маршрутизаторы не транслируют широковещательные запросы в другие сегменты сети, то в

этом случае маршрутизатор в ответ на запрос посылает ARP-ответ с *MAC-адресом своего входного интерфейса*, на который поступил запрос. Таким образом, сформированный конечным устройством кадр поступит на интерфейс маршрутизатора, который по адресу сети назначения и таблице маршрутизации продвинет пакет на выходной интерфейс.

Передать данные по адресу устройства, которое находится в другом сегменте сети, можно также за счет установки в таблице маршрутизации шлюза по умолчанию. **Шлюз по умолчанию имеет IP-адрес входного интерфейса маршрутизатора на пути к устройству назначения**. Этот адрес хранится в конфигурационном файле конечного узла (хоста). Источник сообщения сравнивает IP-адрес назначения со своим IP-адресом и определяет, находятся ли эти адреса в одном сегменте сети или в разных сегментах. Если они находятся в разных сегментах, то данные будут переданы только при условии, что установлен шлюз по умолчанию.

Таким образом, при передаче данных по сети (рис. 7.5) Host X для нахождения MAC-адреса назначения посылает в сеть широковещательный ARP запрос, в котором задается IP-адрес устройства назначения, на который Router A в ответ посылает MAC-адрес своего входного интерфейса, и передаваемый пакет поступает в маршрутизатор.

7.4. Таблицы маршрутизации

При получении кадра маршрутизатор A (рис. 7.5) извлекает из кадра пакет, обрабатывает заголовок поступившего пакета, чтобы определить сеть адресата, затем использует таблицу маршрутизации и продвигает пакет на выходной интерфейс. Пакет вновь инкапсулируется в новый кадр данных и направляется следующему маршрутизатору B, при этом в заголовке кадра указывается новый MAC-адрес входного интерфейса этого маршрутизатора. Этот процесс происходит каждый раз, когда пакет проходит через очередной маршрутизатор. В конечном маршрутизаторе (в данном примере – маршрутизатор C, рис. 7.5), который связан с сетью узла назначения Сеть 2, пакет инкапсулируется в кадр локальной сети адресата с MAC-адресом устройства назначения и доставляется адресату Host Y.

Для продвижения пакета к узлу назначения маршрутизатор использует **таблицу маршрутизации**, основными параметрами которой являются номер (**адрес**) **сети назначения** и сетевой адрес входного интерфейса следующего маршрутизатора на пути к адресату назначения. Этот **адрес** интерфейса получил название **следующего перехода (next hop address)**.

Таким образом, в таблице задаются:

- адрес сети назначения;
- адрес следующего перехода;
- другие дополнительные параметры, которые различаются для разных протоколов маршрутизации и маршрутизаторов разных фирм, производящих оборудование.

Из дополнительных параметров в таблицы маршрутизации включается информация:

- о маршрутизации (статической или динамической),
- об используемых протоколах маршрутизации,
- о метрике, используемой при выборе возможного пути.

Принцип построения таблиц маршрутизации рассмотрен на примере сети, построенной на маршрутизаторах и коммутаторах (рис. 7.11).

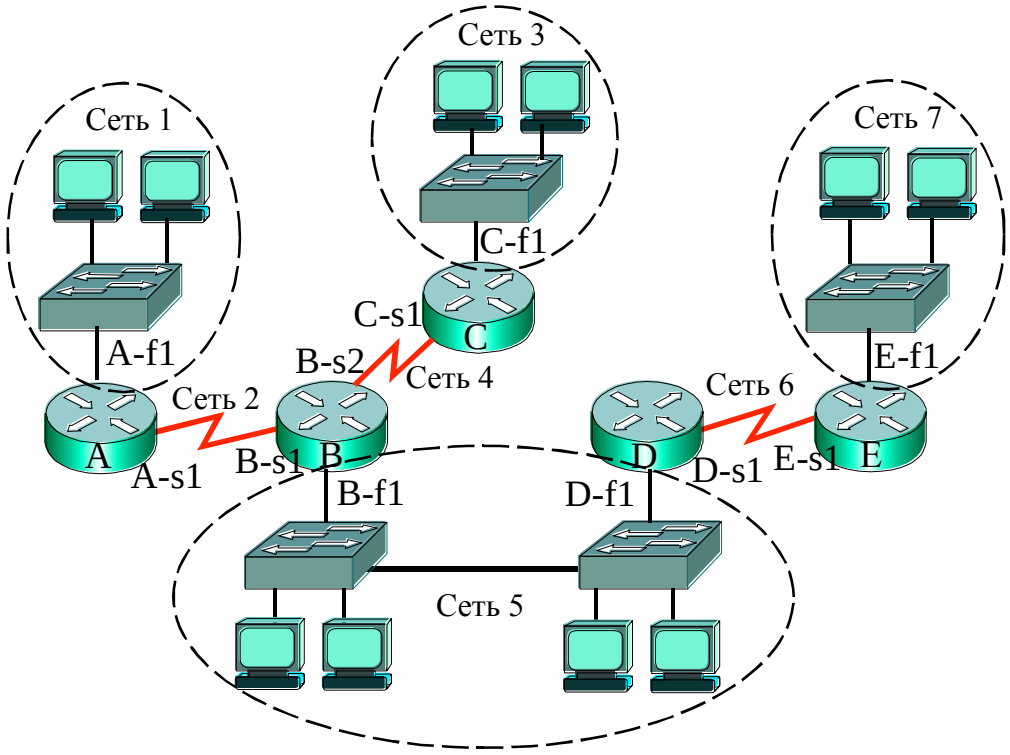


Рис. 7.11. Принцип маршрутизации в сети

Последовательные (serial) интерфейсы маршрутизаторов на рис. 7.11 соединены между собой молниевидной линией, а интерфейсы FastEthernet – прямой линией. В приведенной схеме, например, D-f1 означает – первый FastEthernet интерфейс маршрутизатора **D**, B-s2 – второй последовательный интерфейс маршрутизатора **B**.

Таблица маршрутизации, например, маршрутизатора **B** (табл. 7.2), содержит информацию о маршрутах ко всем сетям (рис. 7.11). Маршрут к Сети 1 лежит через последовательный интерфейс A-s1 маршрутизатора **A**, к Сети 3 – через последовательный интерфейс C-s1 маршрутизатора **C**, а к сетям Сеть 6, Сеть 7 – через интерфейс D-e1 маршрутизатора **D**. Адреса входных интерфейсов маршрутизаторов на пути следования пакета к адресату назначения называются **адресами следующего перехода (**next hop**).**

Таблица 7.2

Основные параметры таблицы маршрутизации

Адрес сети назначения	Адрес следующего перехода
Сеть 1	A-s1
Сеть 3	C-s1
Сеть 6	D-f1
Сеть 7	D-f1

Вместо адреса следующего перехода часто указывают обозначение выходного интерфейса маршрутизатора, отправляющего пакет. Поскольку выходной интерфейс маршрутизатора, отправляющего пакет, и входной интерфейс следующего маршрутизатора на пути к адресату назначения соединены между собой, то противоречий при этом никаких нет.

Кроме удаленных сетей назначения в таблице маршрутизации указываются непосредственно (прямо) присоединенные сети с указанием выходного интерфейса. Например, таблица маршрутизации B (табл. 7.3) будет содержать три прямо присоединенных сети.

Таблица 7.3

Прямо присоединенные сети таблицы маршрутизации

Адрес присоединенной сети	Выходной интерфейс
Сеть 2	s1
Сеть 4	S2
Сеть 5	f1

Таким образом, пакет, предназначенный одному из узлов сети, например Сети 7, попав в маршрутизатор **B**, будет направлен на входной интерфейс D-f1 маршрутизатора **D** (следующий переход). В свою очередь, в таблице маршрутизации **D** будет задан адрес входного интерфейса E-s1 следующего маршрутизатора **E**, для которого Сеть 7 является непосредственно присоединенной. Поэтому маршрутизатор **E** направит пакет узлу назначения.

7.5. Передача данных в сетях с маршрутизаторами

Процесс взаимодействия IP и MAC-адресов при передачи данных от узла Host X до узла Host Y через маршрутизаторы A, B, C рассмотрен на примере сети (рис. 7.12). Адреса конечных узлов и интерфейсов маршрутизаторов, задействованных в этом процессе передачи, приведены в табл. 7.4. Сетевая маска во всех сетях – 255.255.255.0.

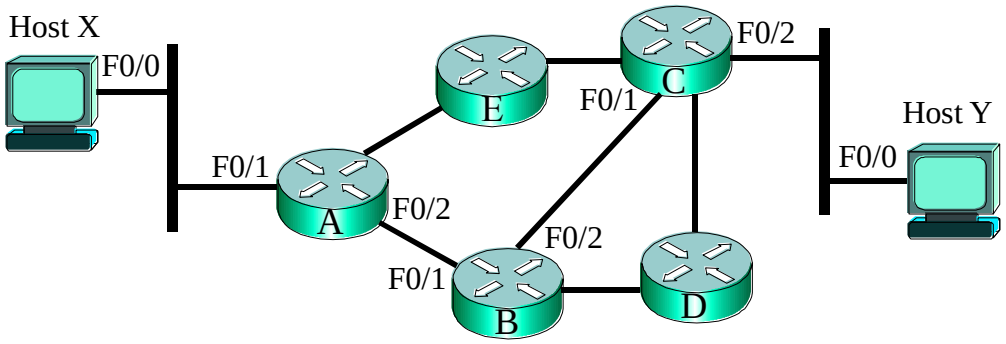


Рис. 7.12. Передача данных по сети

Таблица 7.4

Адреса узлов и интерфейсов маршрутизаторов

Устройство	Интерфейс	IP-адрес	MAC-адрес
Host X	F0/0	172.16.10.11	011ABC123456
Router_A	F0/1	172.16.10.1	0001AAAA1111
	F0/2	198.20.20.5	0002AAAA2222
Router_B	F0/1	198.20.20.6	0001BBBB1111
	F0/2	199.30.30.9	0002BBBB2222
Router_C	F0/1	199.30.30.10	0001CCCC1111
	F0/2	200.40.40.1	0002CCCC2222
Host Y	F0/0	200.40.40.7	022DEF123456

Маршрутизаторы соединены между собой через порты FastEthernet, номера которых также приведены на рис. 7.12. Интерфейсы FastEthernet характеризуются физическими MAC-адресами и логическими IP-адресами. Сетевая маска во всех сетях задана одинаковой и равной 255.255.255.0.

Сообщение, сформированное протоколами верхних уровней компьютера Host X, поступает на сетевой Уровень 3, где IP-протокол формирует пакет данных. Поскольку адрес назначения 200.40.40.7 не относится к сети 172.16.10.0, в которой находится Host X, то необходима маршрутизация.

<table>
<tr><td colspan="3">Заголовок пакета</td><td>Поле данных</td></tr>
<tr><td>Первые поля заголовка пакета</td><td>IP адрес узла назначения 200.40.40.7</td><td>IP адрес узла источника 172.16.10.11</td><td>Data</td></tr>
<tr><td colspan="4">Пакет данных</td></tr>
</table>

На канальном уровне узел Host X инкапсулирует сформированный пакет в кадр соответствующей технологии, например, FastEthernet. В заголовке кадра, наряду с другой информацией, указываются MAC-адреса источника и назначения. MAC-адрес источника в данном примере будет 011ABC123456. Поскольку MAC-адрес узла-получателя Host Y компьютеру Host X не известен, то узел Host X обращается к таблице ARP. Узел не находит соответствующей записи в таблице ARP, поэтому он посылает в локальную сеть широковещательный ARP-запрос, в котором задает сетевой логический IP-адрес устройства назначения – 200.40.40.7. Адресат назначения находится за пределами локальной сети 172.16.10.0. Поскольку маршрутизаторы не транслируют широковещательные запросы в другие сегменты сети, то в этом случае маршрутизатор Router_A в ответ на запрос посылает ARP-ответ с *MAC-адресом своего входного интерфейса*, на который поступил запрос. Входной интерфейс играет роль основного шлюза по умолчанию. ARP-протокол обращается к соответствующей строке таблицы

IP адрес	MAC адрес
172.16.10.1	0001AAAA1111

и посылает узлу Host X ответ с MAC-адресом 0001AAAA1111.

В соответствие с полученным MAC-адресом 0001AAAA1111 узел Host X формирует кадр, который по физической среде передается в маршрутизатор Router_A:

Заголовок кадра		Заголовок пакета		Поле данных
MAC-адрес узла назначения 0001AAAA1111	MAC-адрес узла источника 011ABC123456	IP- адрес узла назначения 200.40.40.7	IP- адрес узла источника 172.16.10.11	Data
Кадр данных				

В маршрутизаторе Router_A из кадра извлекается (декапсулируется) пакет данных. Производится логическое умножение IP-адреса назначения на маску и определяется сеть назначения. Затем происходит обращение к таблице маршрутизации, в соответствие с которой определяется адрес входного порта следующего маршрутизатора Router_B (адрес следующего перехода) и выходной интерфейс маршрутизатора Router_A. При этом формируется новый заголовок пакета, который продвигается к выходному FastEthernet интерфейса F0/2 маршрутизатора Router_A. В новом пакете изменяются некоторые поля заголовка (TTL, контрольная сумма заголовка), но IP-адреса источника и узла назначения остаются неизменными:

Заголовок пакета			Поле данных
Первые поля заголовка пакета	IP-адрес узла назначения 200.40.40.7	IP-адрес узла источника 172.16.10.11	Data
Пакет данных			

Затем пакет инкапсулируется в новый кадр, в качестве MAC-адреса узла источника будет использоваться физический адрес выходного интерфейса F0/2 – 0002AAAA2222 маршрутизатора Router_A. MAC-адрес узла назначения определяется с помощью ARP-протокола, как было описано выше. MAC-адресом узла назначения будет физический адрес входного интерфейса маршрутизатора Router_B – 0001BBBB1111.

Сформированный кадр по сетевой среде передается на входной интерфейс маршрутизатора Router_B:

Заголовок кадра		Заголовок пакета		Данные
MAC-адрес узла назначения 0001BBBB1111	MAC-адрес узла источника 0002AAAA2222	IP- адрес узла назначения 200.40.40.7	IP- адрес узла источника 172.16.10.11	Data
Кадр данных				

Приняв кадр, маршрутизатор Router_B извлекает из него пакет данных и с использованием маски по таблице маршрутизации определяет выходной интерфейс. Пакет инкапсулируется в новый кадр, который передается с новыми MAC-адресами источника и назначения в маршрутизатор Router_C:

Заголовок кадра		Заголовок пакета		Данные
MAC-адрес узла назначения 0001CCCC1111	MAC-адрес узла источника 0002BBBB2222	IP-адрес узла назначения 200.40.40.7	IP- адрес узла источника 172.16.10.11	Data
Кадр данных				

В маршрутизаторе Router_C, также как в Router_A и Router_B, формируются новый пакет и кадр. Поскольку адресат назначения находится в сети, которая непосредственно присоединена к интерфейсу F0/2 маршрутизатора Router_C, то кадр передается узлу назначения Host Y:

Заголовок кадра		Заголовок пакета		Данные
MAC-адрес узла назначения 022DEF123456	MAC-адрес узла источника 0002CCCC2222	IP-адрес узла назначения 200.40.40.7	IP- адрес узла источника 172.16.10.11	Data
Кадр данных				

Протокол сетевого уровня узла Host Y извлекает из кадра пакет данных. Если пакет при передаче был фрагментирован, то из фрагментов формируется целый пакет и через соответствующий интерфейс направляется на транспортный уровень, где из пакетов извлекаются сегменты данных, а из сегментов формируется сообщение.

При передаче данных через соединения «точка-точка» (см. рис. 7.2) заголовок кадра может быть существенно упрощен, т.к. интерфейсы непосредственно связаны между собой, поэтому отпадает необходимость задания MAC-адресов узла источника и узла назначения. Примером может служить **протокол «точка-точка»** (Point-to-Point Protocol – **PPP**) .

На пути кадра к устройству назначения его заголовок и трейлер, в котором размещается контрольная сумма кадра (см. рис. 4.3), изменяются при прохождении через каждое устройство 3-го уровня составной сети, например, через маршрутизатор. Это происходит вследствие того, что в кадре используется локальная адресация 2-го уровня, а пакеты адресуются с использованием логического адреса 3-го уровня и в пакете задается конечный адрес узла назначения. Таким образом, при передаче данных через составную сеть ***IP-адреса узла назначения и узла источника остаются неизменными, MAC-адреса назначения и источника меняются при прохождении каждого маршрутизатора.***

Всякий раз при формировании кадра вычисляется **контрольная сумма,** которая записывается в поле FCS трейлера кадра (рис.4.3). При приеме кадра на каждом входном интерфейсе всех устройств на пути к адресату назначения вновь вычисляется контрольная сумма, которая сравнивается с принятой в трейлере. Правильность принятых данных проверяется с использованием циклического кода CRC. Если расчетный результат и контрольная сумма не совпадают, то кадр отбрасывается. При положительном результате сравнения из кадра извлекается пакет, который проверяется, предназначен ли пакет сетям, прямо присоединенным к данному маршрутизатору, или его надо передать другому устройству составной сети, т.е. маршрутизировать.

Если пакет необходимо маршрутизировать, IP-адрес сети назначения сравнивается с таблицей маршрутизации. При нахождении соответствующей записи в таблице пакет будет переслан на интерфейс, определенный в строке таблицы маршрутизации. Когда пакет коммутируется на выходной интерфейс, формируется новый кадр с новым заголовком и новым значением CRC в трейлере. Кадр затем передается в новый домен на пути к адресату назначения.

Краткие итоги лекции 7

1. Главными функциями маршрутизаторов являются: выбор наилучшего пути для пакетов к адресату назначения и продвижение принятого пакета с входного интерфейса на соответствующий выходной интерфейс.
2. Конфигурационный файл хранится в памяти NVRAM. Он содержит команды и параметры для управления потоком трафика. Конфигурационный файл задает сетевые протоколы и протоколы маршрутизации, которые определяют наилучший путь для пакетов к адресуемой сети.
3. Маршрутизатор оценивает доступные пути к адресату назначения и выбирает наиболее рациональный маршрут на основе некоторого критерия – метрики.
4. Администратор может конфигурировать статические маршруты и поддерживать таблицы маршрутизации вручную. Однако большинство таблиц маршрутизации создается и поддерживается динамически, за счет использования протоколов маршрутизации, которые позволяют маршрутизаторам автоматически обмениваться информацией о сетевой топологии друг с другом.
5. Маршрутизатор ретранслирует пакет, продвигая его с входного интерфейса на выходной, для чего использует сетевую часть адреса назначения и обращается к таблице маршрутизации.
6. Основными параметрами таблицы маршрутизации являются адрес сети назначения и сетевой адрес входного интерфейса следующего маршрутизатора на пути к адресату назначения (следующий переход – next hop) или собственный выходной интерфейс маршрутизатора.
7. Протокол разрешения адресов (ARP) – реализует процесс нахождения MAC-адреса по известному сетевому адресу (IP-адресу). Таблица ARP содержит MAC и IP адреса устройств локальной сети.
8. Шлюз по умолчанию (Gateway Default) – это интерфейс, через который все пакеты из локальной сети будут передаваться в удаленные сети.
9. При передаче данных через составную сеть IP-адреса узла назначения и узла источника остаются неизменными.
10. При передаче данных через составную сеть MAC-адреса назначения и источника меняются при прохождении каждого маршрутизатора.
11. При формировании кадра вычисляется контрольная сумма, которая записывается в поле FCS трейлера кадра. При приеме кадра на каждом входном интерфейсе вновь вычисляется контрольная сумма, которая сравнивается с принятой.
12. При передаче данных через соединения «точка-точка» заголовок кадра может быть существенно упрощен.

Вопросы по лекции 7

1. Какие устройства объединяют LAN в распределенную составную сеть?
2. Какого типа интерфейсы имеют маршрутизаторы ?
3. Что означают термины DTE, DCE?
4. Для чего служит устройство CSU/DSU?
5. Могут ли маршрутизаторы объединять локальные сети различных технологий?
6. На основании чего маршрутизатор ретранслирует пакет, продвигая его с входного интерфейса на выходной?
7. Что служит оценкой наилучшего пути к адресату назначения?
8. Какой протокол позволяет находить MAC-адреса по известному сетевому адресу?
9. По какой команде может быть просмотрена таблица ARP узла?
10. В каком случае маршрутизатор в ответ на запрос посылает ARP-ответ с MAC-адресом своего входного интерфейса, на который поступил запрос?
11. Как формируются таблицы маршрутизации?
12. Что означает термин адрес следующего перехода (next hop)?
13. Что означает термин Шлюз по умолчанию?
14. Какие параметры содержит таблица марщрутизации?
15. При передаче данных через составную сеть, какие адреса остаются неизменными, а какие меняются при прохождении каждого маршрутизатора?

Упражнения

1. Поясните, с использованием какой линии создается конфигурационный файл, и где он может сохраняться.
2. Изобразите схему составной сети из четырех маршрутизаторов, последовательно соединенных через FastEthernet интерфейсы. Обозначьте интерфейсы. Укажите, MAC-адреса каких интерфейсов будут использоваться в качестве адресов источников и адресов назначения передаваемых кадрах при их прохождении через каждый маршрутизатор.
3. Укажите основные параметры таблицы маршрутизации маршрутизатора B (рис.7.11).
4. Для схемы рис.7.12 рассмотрите процесс передачи данных от узла Host Y до узла Host X через маршрутизаторы C, B, A. Какие MAC-адреса и каких интерфейсов будут использоваться в качестве адресов источников и адресов назначения передаваемых кадров при их прохождении через каждый маршрутизатор.
5. Поясните, какие параметры можно посмотреть на каждом конечном узле по команде **ipconfig /all**.
6. Поясните, почему из двух последовательно соединенных серийных интерфейсов маршрутизаторов один должен выполнять роль устройства DCE, а второй – устройства DTE.

Лекция 8. ПРОТОКОЛЫ СЕТЕВОГО УРОВНЯ

Краткая аннотация лекции: Рассмотрены принципы функционирования протоколов сетевого уровня: сетевых и протоколов маршрутизации. Рассмотрен формат заголовка IP-пакета. Проведен сравнительный анализ протоколов вектора расстояния и состояния канала. Приведены основные характеристики протокола RIP.
Цель лекции: изучить принципы функционирования протоколов IP-сетей.

8.1. Сетевые протоколы

Основным **сетевым** (routed) протоколом всемирной сети Интернет является Internet Protocol (**IP**). Формат сообщения сетевого уровня представляет собой **пакет**, известный также как **дейтаграмма** (datagram). В дейтаграммных сетях доставка данных производится **без предварительного соединения** отправителя и получателя сообщения (**connectionless**). В процессе организации связи не используются схемы коммутации цепей, поскольку все соединения выполнены заранее и нужно лишь выбрать наилучший путь к адресату назначения на основе метрики протокола маршрутизации. В IP-сетях с коммутацией пакетов отправитель информации не знает, получено ли его сообщение и получено ли оно без ошибок. Поэтому для повышения надежности и достоверности доставки данных дополнительно используется протокол TCP, а сети и стек протоколов передачи данных получили название **TCP/IP** (см. раздел 2.2).

Дейтаграммные сети характеризуются терминами «*ненадежный*» (**unreliable**) и «*доставка по возможности*» или доставка с наибольшими возможными усилиями (**best-effort delivery**). Это означают, что проверка (верификация) правильности полученных данных на сетевом уровне не производится. Для такой проверки **на конечных узлах используется** протокол транспортного уровня **TCP**.

В **сетях с предварительным соединением** отправителя и получателя (**connection-oriented**) отправитель и получатель перед обменом данными предварительно устанавливают соединение. Кроме того, при использовании таких технологий проводится подтверждение принятых данных. Примером сетей с предварительным соединением являются телефонные сети с коммутацией каналов, а также сети на основе виртуальных каналов.

Правила передачи сообщений по дейтаграммным IP-сетям, их формат и другие параметры устанавливают **сетевые маршрутизируемые протоколы** (**Routed protocol**) и **протоколы маршрутизации** ил маршрутизирующие протоколы (**Routing protocol**). **Сетевые протоколы** определяют формат пакета, логические адреса узла источника и назначения (IP-адреса), заключающиеся в заголовке пакета, и прокладывают маршрут пакета на основе имеющихся таблиц маршрутизации.

М**аршрутизирующие протоколы** (не путать с протоколами маршрутизации!) также являются протоколами сетевого уровня, они создают и поддерживают таблицы маршрутизации. **Обновления (update) таблиц** протоколами маршрутизации реализуется путем обмена маршрутными данными между маршрутизаторами. Таким образом, **протоколы маршрутизации создают и поддерживают таблицы маршрутизации, а сетевые протоколы используют эти таблицы для продвижения пакетов**.

Протоколы сетевого уровня (IP, IPX/SPX, AppleTalk) должны обеспечивать номера (адреса) сетей и номера (адреса) хостов. Некоторым протоколам, например Novell Internetwork Packet Exchange (**IPX**), требуются только сетевой адрес, поскольку они используют MAC-адрес устройства в качестве адреса хоста. Протоколу IP требуется адрес, содержащий как сетевую, так и узловую (хостовую) части. Для того чтобы можно было выделить адрес сети и адрес хоста необходима маска сети или подсети. Сетевые протоколы обеспечивают поддержку Уровня 3 модели OSI.

Формат пакета сетевого протокола IP (рис. 8.1) включает заголовок, состоящий из 12 полей общей длиной в 160 бит (5 слов по 4 байта, т.е. 20 байт), поле опций переменной длины и поле данных.

<table>
<tr><td>1 4</td><td>5 8</td><td>9 16</td><td>17 19</td><td>20 32</td></tr>
<tr><td colspan="2">1.Vers</td><td>2.HLEN</td><td>3. Type of Service</td><td colspan="2">4. Total Length</td></tr>
<tr><td colspan="3">5. Identification</td><td>6.Flags</td><td>7. Fragment Offset</td></tr>
<tr><td colspan="2">8. Time to Live</td><td>9. Protocol</td><td colspan="2">10. Header Checksum</td></tr>
<tr><td colspan="5">11. Source IP address</td></tr>
<tr><td colspan="5">12. Destination IP address</td></tr>
<tr><td colspan="5">13. IP option</td></tr>
<tr><td colspan="5">14. Data</td></tr>
</table>

Рис.8.1. Формат заголовка IP-пакета

1. Первое 4-х разрядное поле (Vers) задает номер версии протокола. В настоящее время действует версия 4 – IPv4, согласно которой длина адреса источника (Source IP address) и адреса назначения (Destination IP address) равна 32 разрядам (4 байтам). В распечатках поля заголовка обычно представляются в десятичной и шестнадцатеричной системе. Например, действующая в настоящее время версия 4 выглядит следующим образом: Version = 4 (0x4), в двоичной системе – 0100.
2. Длина заголовка – количество 32-разрядных слов в заголовке, задается вторым полем HLEN. Например, двоичный код в этом поле – 0101 и запись Header Length = 20 (0x14) означает, что заголовок содержит 5 слов по 32 разряда или 20 байт.
3. Поле типа сервиса (Type of Service – ToS) длиной 8 бит включает четыре идентификатора: трехразрядный идентификатор PR и одноразрядные D, T, R. Идентификаторы определяют требования к метрике при прокладке маршрута. Идентификатор PR определяет тип пакета (нормальный, управляющий и др.) и в соответствие с этим задает приоритет. Установка 1 в разряде D означает требование минимизации задержки при передаче пакета; единица в разряде T означает требование максимальной пропускной способности; установка 1 в разряде R требует максимальную надежность. **Поле типа сервиса** позволяет в мультисервисных сетях при передаче разных типов трафика организовать систему приоритетов, т.е. организовать **систему качества обслуживания** (Quality of Service – **QoS**), когда чувствительный к задержкам трафик пропускается в первую очередь.
4. Поле Total Length задает общую длину пакета, включая заголовок и поле данных. 16 разрядов поля позволяют задавать максимальную длину 64 Кбайт. Поскольку максимальная длина кадра в большинстве технологий локальных сетей меньше 64 Кбайт, например, в Ethernet она составляет 1500 байт, то большие пакеты разбивают на фрагменты. При **фрагментации** пакета используется информация 5, 6 и 7 полей, все фрагменты должны иметь: одинаковый идентификационный номер пакета; номер, определяющий порядок следования фрагмента при сборке пакета; дополнительную информацию.
5. Пятое поле заголовка содержит **идентификационный номер пакета.**

При фрагментации пакета идентификационный номер будет единым для всех фрагментов.

6. Трехразрядное поле Flags содержит два одноразрядных флага фрагментации. Установка 1 в разряде DF запрещает маршрутизатору производить фрагментацию данного пакета. Единичка в разряде MF указывает, что данный пакет не является последним из числа фрагментированных.
7. 13-разрядное **поле смещения данных** Fragment Offset помогает собрать фрагменты в единый пакет. Оно задает смещение в байтах поля данных этого пакета от начала общего поля данных исходного не фрагментированного пакета.
8. **Время жизни** (Time to Live – **TTL**) уменьшается на 1 при прохождении каждого маршрутизатора или каждую секунду. Оно задается при формировании пакета и может иметь значение от 1 до 255. При обнулении значения TTL пакет уничтожается. Таким образом, число узлов, через которые может пройти пакет, ограничено.
9. Поле Protocol указывает протокол верхнего уровня (TCP, UDP, и др.), которому будет передан принятый пакет после завершения IP процесса.
10. Поле контрольной суммы заголовка Header Checksum. Поскольку при прохождении маршрутизатора значения некоторых полей заголовка изменяются, например время жизни TTL, то расчет контрольной суммы производится в каждом маршрутизаторе заново.
11. **Адрес источника информации** (**Source IP address**) длиной 4 байта (32 двоичных разряда).
12. **Адрес назначения** (**Destination IP address**) или адрес приемника информации – длина 4 байта (32 разряда).
13. Поле IP option позволяет поддерживать различные опции, например, опцию защиты информации. Это поле может иметь разную длину, поэтому оно дополняется нулями до 32 разрядов.
14. Поле данных Data имеет длину более 64 двоичных разрядов.

8.2. Основные параметры протоколов маршрутизации

Совокупность сетей, представленных набором маршрутизаторов под общим административным управлением, образует **автономную систему** (рис. 8.2). Примерами автономных систем являются сети провайдеров. Автономные системы нумеруются и в некоторых протоколах (IGRP, EIGRP) эти номера используются. В настоящем курсе лекций рассматривается маршрутизация только внутри автономной системы. Протокол BGP, обеспечивающий маршрутизацию между автономными системами изучается в курсе CCNP Международной сетевой академии Cisco.

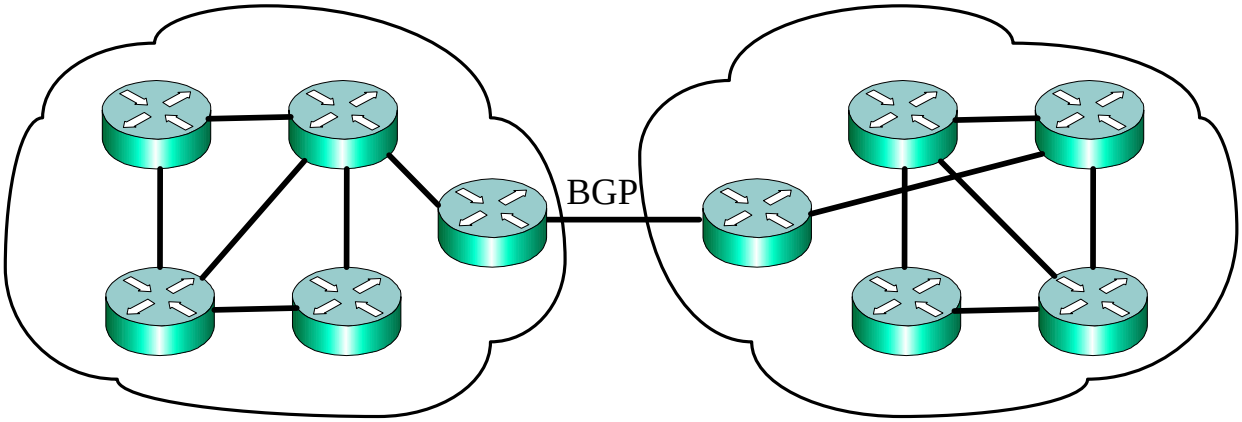


Рис. 8.2. Взаимодействие автономных систем

Маршрутизаторы функционируют в дейтаграммных сетях с коммутацией пакетов, где все возможные маршруты уже существуют. Поэтому пакету нужно лишь выбрать наилучший путь на основе метрики протокола маршрутизации. Процесс прокладывания пути производится последовательно от одного маршрутизатора к другому. Этот процесс маршрутизации (routing) является функцией Уровня 3 модели OSI. При прокладывании пути пакета маршрутизатор анализирует сетевой адрес узла назначения, заданный в заголовке пакета, и вычленяет из него адрес сети. **Адреса всех доступных сетей** назначения хранятся **в таблице маршрутизации**. Поэтому маршрутизатор должен создавать и поддерживать таблицы маршрутизации, а также извещать другие маршрутизаторы о всех известных ему изменениях в топологии сети.

Маршрутизацию, т.е. прокладывание маршрута внутри автономных систем, осуществляют протоколы внутренней маршрутизации (Interior Gateway Protocols - **IGP**s), к которым относятся RIP, RIPv2, IGRP, EIGRP, OSPF, Intermediate System-to-Intermediate System (IS-IS). Маршрутизацию между автономными системами производят протоколы внешней маршрутизации (Exterior Gateway Protocols - **EGP**s). Примером протокола внешней маршрутизации является протокол BGP, который работает на граничных маршрутизаторах автономных систем (рис. 8.2).

Маршрутизирующие протоколы, работающие внутри автономных систем, в свою очередь, подразделяются на **протоколы вектора расстояния** (**distance-vector**) и **протоколы состояния канала** (**link-state**). Протоколы вектора расстояния определяют расстояние и направление, т.е. вектор соединения в составной сети на пути к адресату. Расстояние может быть выражено в **количестве переходов** (**hop count**) или маршрутизаторов в соединении на пути от узла источника к адресату назначения, а также других значениях метрики.

При использовании протокола **вектора расстояния** маршрутизаторы посылают всю или часть таблицы маршрутизации соседним (смежным) маршрутизаторам через определенные интервалы времени. В таких протоколах как **RIP**, *обмен обновлениями (update) или модификациями происходит периодически, даже если в сети нет никаких изменений*, на что затрачивается довольно большая часть полосы пропускания. Получив обновление маршрутной информации, маршрутизатор может заново вычислить все известные пути и произвести изменения в таблице маршрутизации.

Протоколы **состояния канала** создают полную картину топологии сети и вычисляют кратчайшие пути ко всем сетям назначения. Если путей несколько, то выбирают первый из вычисленных. Протоколы состояния канала (или соединения) быстрее реагируют на изменения в сети по сравнению с протоколами вектора расстояния, но при этом требуют больших вычислительных ресурсов.

Когда инкапсулированный в кадр пакет прибывает на входной интерфейс, маршрутизатор декапсулирует его, затем использует таблицу маршрутизации, чтобы определить, по какому маршруту направить пакет, т.е. **на какой свой выходной интерфейс передать поступивший пакет.**

Выходной интерфейс связан с наиболее рациональным маршрутом к адресату назначения. Этот процесс называется **коммутацией** или **продвижением** пакета. На выходном интерфейсе пакет инкапсулируется в новый кадр, при этом маршрутизатор добавляет информацию для формирования кадра (см. материалы лекции 7).

Определение наиболее рационального (или оптимального) пути производится маршрутизатором на основе некоторого критерия – **метрики.** Значение метрики используется при оценке возможных путей к адресату назначения. Метрика может включать разные параметры, например: полосу пропускания, задержку, надежность, загрузку, обобщенную стоимость и другие параметры сетевого соединения.

Маршрутизаторы могут использовать один какой-то параметр или комбинацию параметров метрики при выборе оптимального маршрута.

Маршрутная информация может быть сконфигурирована сетевым администратором – при этом реализуется **статическая маршрутизация. Динамическая маршрутизация** реализуется протоколами маршрутизации, когда маршрутная информация собирается в ходе динамического процесса обмена обновлениями (модификациями) между маршрутизаторами, который по определенным правилам выполняется в сети.

Таким образом, протоколы маршрутизации (routing protocol) позволяют выбирать маршрутизаторам наилучший путь для передаваемых сообщений от источника да устройства назначения. Для этого маршрутизирующие протоколы создают и поддерживают (модифицируют) таблицы маршрутизации путем обмена маршрутной информацией с другими маршрутизаторами в сети. В настоящем курсе лекций рассматривается функционирование и конфигурирование следующих протоколов маршрутизации:

RIP (**Routing Information Protocol**) – протокол маршрутизации на основе вектора расстояния;

EIGRP (**Enhanced Interior Gateway Routing Protocol**) – расширенный протокол внутренней маршрутизации;

OSPF (**Open Shortest Path First**) – открытый протокол маршрутизации по состоянию канала.

Маршрутизаторы способны поддерживать много независимых протоколов и таблиц маршрутизации для нескольких сетевых протоколов. Эта способность позволяет маршрутизатору передавать пакеты различных сетевых протоколов по тем же самым каналам связи.

Таблицы маршрутизации позволяют передавать пакеты за пределы широковещательного домена. Например, строки таблицы маршрутизации (табл. 8.1) с меткой C отображают непосредственно присоединенные сети, а с меткой R – сети, путь к которым проложен с помощью протокола RIP. В каждой строке также представлены: расстояние до сети назначения, выраженное в количестве переходов между маршрутизаторами (hop); выходной интерфейс маршрутизатора на пути к сети назначения.

Таблица 8.1

Таблица маршрутизации маршрутизатора A

Метка	Адрес сети назначения	Число переходов (hop)	Выходной интерфейс
C	192.168.1.0	0	F0
C	192.168.3.0	0	F1
C	200.10.10.0	0	S0
R	192.168.2.0	1	S0
R	192.168.4.0	1	S0

На Уровне 2 модели OSI функционируют коммутаторы, которые соединяют сегменты одной локальной сети или подсети, используя MAC-адреса. Для соединения с хостами вне локальной сети коммутатор продвигает кадр на маршрутизатор. Хост использует MAC-адрес входного интерфейса маршрутизатора как адрес назначения. Неизвестный MAC-адрес хост узнает из таблицы ARP. Маршрутизатор сверяет IP-адрес сети назначения с таблицей маршрутизации и продвигает пакет на выходной интерфейс в соответствие с найденной строкой таблицы маршрутизации.

Поскольку коммутаторы не блокируют широковещательные передачи, то сети на коммутаторах могут быть затоплены широковещательными штормами. *Маршрутизаторы блокируют широковещательные передачи*, поэтому широковещательный шторм может быть только в пределах широковещательного домена (broadcast domain), т.е. в пределах сети.

Поэтому *маршрутизаторы по сравнению с коммутаторами обеспечивают большую безопасность* и контроль полосы пропускания.

Маршрутизаторы используют протоколы маршрутизации, чтобы создавать и поддерживать таблицы маршрутизации для определения маршрута. При этом таблицы маршрутизаторов разных фирм производителей и разных протоколов маршрутизации могут иметь несколько различающуюся маршрутную информацию. В большинстве случаев таблицы маршрутизации содержат:

- *Тип протокола*, который идентифицирует протокол маршрутизации, который создавал каждый вход (строку) таблицы.
- *Следующий переход* (Next-hop) – указывает адрес входного интерфейса следующего маршрутизатора на пути к адресату назначения.
- *Метрику*, которая различается для разных протоколов.
- *Выходной интерфейс*, через который данные должны быть отправлены к устройству назначения.

Маршрутизаторы поддерживают таблицы маршрутизации через обмен *обновлениями* или *модификациями* (update). Некоторые протоколы передают обновления периодически, например, протоколы RIP. Другие протоколы посылают модификации только когда происходят изменения в сетевой топологии, например, OSPF, EIGRP.

Маршрутизаторы, зная информацию о пути к некоторым сетям, обмениваются этой информацией с другими маршрутизаторами. Следовательно, после таких обновлений или модификаций все маршрутизаторы в сети будут иметь согласованную информацию о маршрутах к доступным сетям. Таким образом, ***маршрутизирующие протоколы разделяют сетевую информацию между маршрутизаторами***.

Различные протоколы маршрутизации используют разные алгоритмы при выборе маршрута, т.е. выходного интерфейса, на который должен быть передан пакет. Алгоритм и метрика определяются целым рядом решаемых задач, таких как простота, устойчивость, гибкость, быстрая **сходимость или конвергенция** (convergence). Сходимость это процесс согласования между всеми маршрутизаторами сети информации о доступных маршрутах. При изменениях состояния сети необходимо, чтобы обмен модификациями восстановил согласованную сетевую информацию.

Каждый алгоритм по своему интерпретирует выбор наиболее рационального пути на основе **метрики**. Обычно **меньшее значение метрики соответствует лучшему маршруту**. Метрика может базироваться на одном или на нескольких параметрах пути. В протоколах маршрутизации наиболее часто используются следующие метрики:

- **Полоса пропускания** (Bandwidth) – способность соединения передавать данные с некоторой скоростью. Например, соединения сети Fast Ethernet передающие данные со скоростью 100 Мбит/с, предпочтительней сети E1 со скоростью 2,048 Мбит/с.
- **Задержка** (Delay) – это длительность времени прохождения пакета от источника до адресата назначения. Задержка зависит от количества промежуточных соединений и их типов, объема буферных устройств маршрутизаторов, сходимости сети и расстояния между узлами.
  Загрузка (Load) – загрузка определяется количеством информации, загружающей сетевые ресурсы (маршрутизаторы и каналы). Чем больше загрузка, тем дольше пакет будет в пути.
- **Надежность** (Reliability) – надежность определяется интенсивностью ошибок на каждом сетевом соединении.
- **Количество переходов** (Hop count) – это количество маршрутизаторов, через которые пакет должен пройти на пути к адресату назначения (число переходов от маршрутизатора к маршрутизатору).
- **Стоимость** (Cost) –это обобщенный параметр затрат на передачу пакета к адресату назначения. Обычно стоимость имеет произвольное значение, назначенное администратором.

8.3. Протоколы вектора расстояния и состояния канала

Протоколы вектора расстояния периодически рассылают обновления маршрутной информации или **модификации** (updates). У протокола RIP этот период равен 30 сек. При этом обновляются таблицы маршрутизации, которые и хранят всю информацию о маршрутах в сети. При изменении в сети маршрутизатор, обнаруживший такое изменение, сразу начинает обмен маршрутной информацией с соседними маршрутизаторами. Этот обмен идет последовательно от маршрутизатора к маршрутизатору с

некоторой задержкой, определяемой временем модификации таблиц в каждом маршрутизаторе, а также специальным таймером. Поэтому **сходимость** (**конвергенция**) сети, когда все маршрутизаторы будут иметь согласованную информацию о сетевых соединениях, **происходит медленно,** что является главным недостатком протоколов вектора расстояния.

Протоколы состояния соединения или канала (Link-state) быстро реагируют на изменения в сети, **рассылая модификации при изменениях в сетевой топологии**, всем маршрутизаторам в пределах некоторой области сети. Протоколы состояния канала создают таблицы маршрутизации на основе информации, хранящейся в *специальной базе данных* (*link-state database*). В базе данных хранится один или несколько путей к адресату назначения, из которых выбирается **первый кратчайший путь** (shortest path first), который и помещается в таблицу маршрутизации. Если первый путь становится недоступным, то протокол из базы данных может выбрать другой оперативно без дополнительных вычислений.

Когда происходят изменения в маршрутах или каналах (пропадают ранее существовавшие или появляются новые), маршрутизатор, первым заметивший изменение в сети, создает **извещение о состоянии** этого **соединения** (Link-State Advertisement - **LSA**). Сообщение LSA затем передается всем смежным маршрутизаторам. Каждый маршрутизатор, получив копию LSA, транслирует LSA всем соседним устройствам и модифицирует свою базу данных. Такое волновое распространение пакетов (flooding) предопределяет, что все устройства маршрутизации создадут базы данных, которые согласованно будут отражать сетевую топологию перед модификацией таблиц маршрутизации.

Наиболее известным в сети Internet протоколом типа distance-vector является **Routing Information Protocol** (**RIP**), который использует в качестве метрики *число переходов* (*hop count*) на пути к адресату назначения.

Другим простым протоколом вектора расстояния является Interior Gateway Routing Protocol (**IGRP**), который был разработан в корпорации Cisco. Для работы в больших сложных сетях на смену ему пришел протокол **Enhanced IGRP** (**EIGRP**), который включает много особенностей протоколов как типа link-state, так и distance-vector. Поэтому он был назван гибридным протоколом (hybrid). Разработчики корпорации Cisco относят его к протоколам distance-vector.

Протокол вектора расстояния RIP Version 1 (**RIPv1**), или просто RIP, использует счетчик переходов (hop count) в качестве метрики, чтобы определить направление и расстояние до определенного соединения в составной сети. Если существует несколько путей, то RIP выберет путь с наименьшим числом маршрутизаторов или переходов (hops) к адресату назначения. Однако выбранный маршрут не всегда является лучшим путем к адресату, поскольку выбранный маршрут с наименьшим числом устройств может характеризоваться меньшей скоростью передачи (меньшей полосой пропускания) по сравнению с альтернативными маршрутами. Кроме того, RIP не может направлять пакеты далее 15 переходов (15 hops), поэтому он рекомендован для работы в малых и средних сетях. Протокол RIPv1 требует, чтобы все устройства в сети использовали одинаковую маску подсети, поскольку RIP не включает информацию о маске подсети в модификацию (update) маршрутизации. Такой метод получил название **маршрутизации на основе классов** (classful routing).

Протокол вектора расстояния RIP Version 2 (**RIPv2**) обеспечивает **бесклассовую маршрутизацию CIDR**, (classless routing) поскольку в модификацию маршрутизации включена информация о маске подсети (о префиксе). При этом внутри одной сети могут существовать подсети с масками переменной длины (variable-length subnet masking - **VLSM**).

Протокол EIGRP обеспечивает быструю сходимость и малое количество служебной информации, передаваемой в обновлениях, что экономит полосу пропускания. EIGRP использует ряд функций протоколов link-state. Протоколы EIGRP работают с оборудованием CISCO и не всегда поддерживаются программным обеспечением аппаратуры других фирм.

Наиболее известными в сети Internet протоколами типа Link-state являются протокол **Open Shortest Path First** (**OSPF**), а также протокол Intermediate System-to-Intermediate System (IS-IS).

OSPF является маршрутизирующим протоколом состояния канала, разработанным фирмой Engineering Task Force (IETF). Он предназначен для работы в больших гибких составных сетях, может работать с оборудованием разных фирм производителей, поэтому получил широкое распространение.

Протокол граничного шлюза (Border Gateway Protocol - **BGP**) относится к внешним протоколам External Gateway Protocol (EGP). Протокол обеспечивает обмен маршрутизирующей информацией между автономными

системами, гарантирует выбор пути, свободный от маршрутных петель (loop-free). Протокол BGP используется основными сетевыми компаниями, в том числе провайдерами Интернет. Протокол BGP принимает решение о выборе маршрута на основе сетевой политики.

8.4. Протокол RIP

Протокол RIP для своей работы использует алгоритм Беллмана-Форда. Функционирование алгоритма рассмотрено на примере сети из четырех последовательно соединенных маршрутизаторов (рис. 8.3), где Сеть 1 непосредственно присоединена к маршрутизатору **A**, поэтому метрика пути к Сети 1 из **A** равна 0. Протокол RIP каждые 30 сек. рассылает обновления.

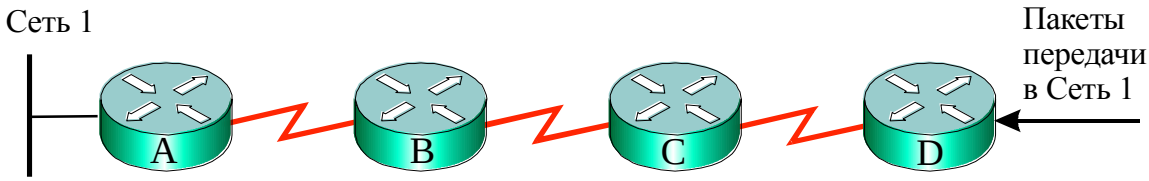


Рис. 8.3. Сеть из последовательно соединенных маршрутизаторов

Согласно алгоритма Беллмана-Форда маршрутизатор **A** посылает маршрутизатору **B** информацию о пути в Сеть 1, при этом добавляет 1 к значению вектора расстояния, т.е. увеличивает метрику (hop count) до единицы. Таким образом, в таблице маршрутизации **B** будет информация, что расстояние до Сети 1 равно одному переходу. Затем **B** посылает копию таблицы маршрутизации маршрутизатору **C**, увеличив метрику до 2. В свою очередь маршрутизатор **C** повышает значение метрики до 3 и обменивается маршрутной информацией с маршрутизатором **D**. То есть, результирующий вектор или расстояние поэтапно увеличивается.

Эта особенность алгоритма может приводить к появлению маршрутных петель в случае медленной конвергенции после изменений в сети, пример чего иллюстрирует рис. 8.4.

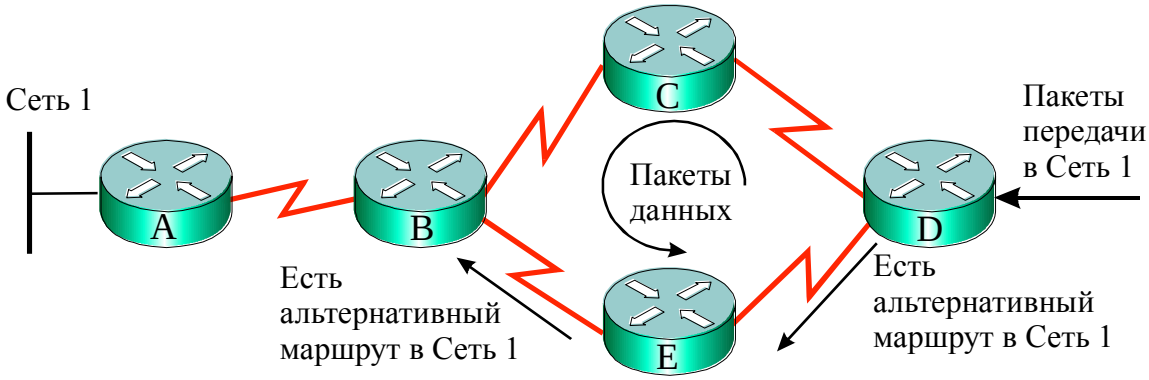


Рис. 8.4. Образование маршрутных петель в сети

Предположим, что до изменений в представленной сети наилучшим путем к Сети 1 для маршрутизатора **D** был путь через маршрутизаторы **C** и **B**. Метрика пути из маршрутизатора D в Сеть 1 была равна 3 переходам. Если, например, Сеть 1 (рис. 8.4) вышла из строя, то начинается обновление маршрутной информации. При этом может возникнуть маршрутная петля:

1. Маршрутизатор **A** посылает обновление об изменении маршрутов маршрутизатору **B** и он прекращает передачу пакетов данных в Сеть 1. Но поскольку маршрутизаторы **C**, **E** и **D**, еще не получили обновления, то они продолжают передачу.
2. Маршрутизатор **B** отправляет обновления маршрутизаторам **C** и **E**, они прекращают отправлять пакеты в Сеть 1, но маршрутизатор **D** – продолжает. Он пока еще считает, что имеется путь в Сеть 1 через маршрутизатор **C** и метрика равна 3 переходам.
3. Если маршрутизатор **D** отправит обновление маршрутизатору **E**, то в нем он укажет, что существует маршрут в Сеть 1 через маршрутизатор **C**, но метрика равна 4 переходам.
4. Маршрутизатор **E** обновит свою таблицу маршрутизации и перешлет обновление маршрутизатору **B** с метрикой в 5 переходов, и так далее по кольцу.
5. В этом случае любой пакет, предназначенный Сети 1 будет передаваться по кольцу (по петле) от маршрутизатора **D** к маршрутизатору **C**, затем к **B**, **E** и снова **D**.

Таким образом, образовалась маршрутная петля, из которой пакет не может выйти, если не принять специальных мер.

Меры борьбы с маршрутными петлями

Движение по петле теоретически может быть бесконечным. Однако в существующих протоколах имеется ряд средств, чтобы предотвратить бесконечную циркуляцию пакетов по петле маршрутизации.

1. В протоколе вектора расстояния **RIP максимальное значение метрики не может превышать 15**. Поэтому, как только при обмене маршрутной информацией (рис. 8.4) возрастающая на каждом шаге метрика достигает значения 16 , Сеть 1 будет считаться недостижимой и пакет отбрасывается.
2. В **заголовке сетевого протокола IP** (см. рис.8.1) имеется поле времени жизни **TTL**, которое декрементируется при прохождении каждого маршрутизатора. Таким образом, число устройств, через которые может пройти пакет, ограничено. При обнулении значения TTL маршрутизатор отбрасывает пакет и отправителю с помощью протокола ICMP посылается сообщение о недостижимости сети.
3. **Принцип расщепления горизонта** (split horizon) также позволяет бороться с маршрутными петлями. При описании возникновения маршрутной петли (рис. 8.4) показано, что если маршрутизатор **D** отправит обновление маршрутизатору **E**, и в нем укажет, что есть альтернативный маршрут в Сеть 1 через маршрутизатор **C**, то маршрутизатор **E** модернизирует свою таблицу маршрутизации и перешлет обновление маршрутизатору **B**. Таким образом, маршрутизатор **B** может ошибочно считать, что имеется путь к Сети 1, но с худшей метрикой. Однако ранее маршрутизатор **B** уже получил от маршрутизатора **A** информацию, что Сеть 1 недостижима. **Принцип расщепления горизонта** указывает, что **нельзя посылать информацию** маршрутизатору **B** о Сети 1 **в обратном направлении**, т.е. от маршрутизатора **C** или **E**.
4. **Пометка недоступного маршрута запрещенной метрикой** (route poisoning). В этом случае маршрутизатор, имеющий какой-то маршрут к сети, сразу же после получения сообщения о недостижимости данной сети, включает в соответствующую строку таблицы маршрутизации запрещенное значение метрики, равное 16. Обычно этот метод используется совместно с принципом расщепления горизонта и

механизмом мгновенной рассылки объявлений об изменении топологии сети.

5. Согласно **метода мгновенных обновлений** (triggered update) их рассылка производится сразу, как только маршрутизатор обнаружит какие-либо изменения в сети, не дожидаясь окончания периода обновления. Последующие маршрутизаторы также мгновенно рассылают информацию об изменении в сети. Это приводит к ускорению конвергенции сети.
6. **Таймер удержания информации** (holddown timer) запускается на маршрутизаторе, когда от соседнего устройства приходит информация о том, что ранее доступная сеть становится недоступной. Это дает больше времени для распространения информации об изменениях по всей сети. При этом возможны разные варианты действия протокола вектора расстояния:

а) если до истечения времени таймера удержания информации от того же устройства приходит обновление, что сеть снова стала достижимой, то протокол помечает сеть как доступную и выключает таймер;

б) если до истечения времени таймера приходит обновление от другого маршрутизатора с лучшей метрикой, чем была ранее, то протокол помечает сеть как доступную и выключает таймер;

в) если до истечения времени таймера приходит обновление от другого маршрутизатора с худшей метрикой, то это обновление игнорируется.

Таким образом, указанные меры борьбы с маршрутными петлями позволяют маршрутизаторам избегать их. Однако время конвергенции протокола RIP велико, по сравнению с протоколами состояния канала link-state. Поэтому протокол RIP используется только в малых сетях. Однако у названного протокола есть важное достоинство. Для его функционирования требуется существенно меньше объем оперативной памяти и быстродействие центрального процессора. Поэтому данный протокол разработан для новой версии адресации IPv6.

Для обеспечения бесклассовой маршрутизации **CIDR** и возможности использования сетевых масок переменной длины **VLSM** разработан и эксплуатируется протокол вектора расстояния RIPv2. Все другие параметры у него аналогичны протоколу RIPv1.

Краткие итоги лекции 8

1. Основным сетевым протоколом всемирной сети Интернет является Internet Protocol (IP).
2. Сетевые (routed) протоколы определяют формат пакета, логические адреса узла источника и назначения, прокладывают маршрут пакета на основе имеющихся таблиц маршрутизации.
3. Маршрутизирующие (routing) протоколы сетевого уровня создают и поддерживают таблицы маршрутизации.
4. Обновления (update) таблиц протоколами маршрутизации реализуется путем связи и обмена данными между маршрутизаторами.
5. При фрагментации пакета идентификационный номер будет единым для всех фрагментов.
6. Поле смещения данных задает смещение в байтах данных пакета от начала общего поля данных исходного не фрагментированного пакета.
7. Время жизни (TTL) при прохождении каждого маршрутизатора уменьшается на 1. Таким образом, число узлов, через которые может пройти пакет, ограничено.
8. Совокупность сетей, представленных набором маршрутизаторов под общим административным управлением, образует автономную систему.
9. Маршрутизаторы функционируют в дейтаграммных сетях с коммутацией пакетов, где все возможные маршруты уже существуют.
10. Маршрутизаторы при использовании алгоритма вектора расстояния обмениваются таблицами маршрутизации с соседними маршрутизаторами через определенные интервалы времени.
11. Протоколы состояния канала создают полную картину топологии сети и вычисляют кратчайший путь ко всем сетям назначения. Обмен маршрутной информацией проводится только при изменениях топологии.
12. Определение наиболее рационального (оптимального) пути производится маршрутизатором на основе критерия – метрики.
13. Маршрутная информация может быть сконфигурирована сетевым администратором – при этом реализуется статическая маршрутизация.
14. Маршрутизаторы блокируют широковещательные передачи, поэтому широковещательный шторм может быть только в пределах домена.
15. Маршрутизирующие протоколы разделяют сетевую информацию между маршрутизаторами.
16. Сходимость (конвергенция) – это процесс согласования между всеми маршрутизаторами сети информации о доступных маршрутах.
17. Первый кратчайший путь к сети назначения, вычисленный протоколом состояния канала, помещается в таблицу маршрутизации. В базе данных может храниться несколько путей к адресату назначения.
18. Когда происходят изменения в маршрутах или каналах, маршрутизатор, первым заметивший изменение в сети, создает извещение о состоянии этого соединения (LSA) и передает его всем соседним маршрутизаторам.

19. При маршрутизации на основе классов (classful routing) информация о маске подсети в модификацию (update) не включается.
20. При бесклассовой маршрутизации (classless routing) информация о маске подсети включается в обновления (update).
21. У протоколов вектора расстояния существует возможность возникновения маршрутных петель, для борьбы с которыми разработан ряд методов.
22. Принцип расщепления горизонта (split horizon) определяет, что нельзя посылать информацию маршрутизатору об изменениях в сети в обратном направлении.
23. После получения сообщения о недостижимости сети, маршрутизатор включает в соответствующую строку таблицы маршрутизации запрещенное значение метрики (равное 16 в протоколе RIP).
24. Метода мгновенных обновлений (triggered update) производит рассылку модификаций сразу, как только маршрутизатор обнаружит какие-либо изменения в сети, не дожидаясь окончания периода обновления.

Вопросы по лекции 8

1. Что определяют сетевые (routed) протоколы?
2. Каков размер заголовка пакета IPv4?
3. В каких случаях производится фрагментация пакета?
4. Что позволяет собрать отдельные фрагменты в единый пакет?
5. Какую функцию выполняет Время жизни (TTL) ?
6. Что такое автономная система?
7. Какие функции выполняют маршрутизирующие (routing) протоколы?
8. Как маршрутизаторы обмениваются таблицами маршрутизации с соседями при использовании алгоритма вектора расстояния?
9. Когда маршрутизаторы обмениваются маршрутной информацией при использовании протокола состояния канала?
10. На основании чего производится определение оптимального пути к сети назначения?
11. Что такое статическая и динамическая маршрутизация?
12. Что означает термин сходимость?
13. Где храниться полная информация о топологии сети при использовании протокола состояния канала?
14. Когда создается извещение о состоянии соединения LSA?
15. В каких типах маршрутизации информация о маске подсети включается в обновления?
16. Какие методы разработаны для борьбы с маршрутными петлями в протоколах вектора расстояния?
17. Какую функцию выполняет Время жизни (TTL) ?
18. Что характеризует принцип расщепления горизонта?

Упражнения

1. Объясните в чем различие протоколов вектора расстояния и состояния канала.
2. Укажите наиболее часто используемые метрики протоколов маршрутизации.
3. Объясните в чем различие методов маршрутизации на основе классов и бесклассовой маршрутизации.
4. Объясните, как формируется метрика пути к Сети 1 (рис. 8.4) на маршрутизаторах A, B, C, D.
5. Объясните, как образуется маршрутная петля в сети (рис. 8.4).
6. Объясните, как принцип расщепления горизонта позволяет бороться с маршрутными петлями.
7. Объясните, как позволяет бороться с маршрутными петлями пометка недоступного маршрута запрещенной метрикой.
8. Объясните, как функционирует таймер удержания информации в борьбе с маршрутными петлями.

Контрольный тест по разделу 3

Задача 3.1
Вариант 1 Задачи 3.1

61. В таблице маршрутизации может содержаться следующая информация: (выбрать три ответа)

Адреса устройств назначения
Адреса сетей назначения
Адреса непосредственно присоединенных сетей
MAC-адреса устройств назначения
Адрес следующего перехода
Входной интерфейс маршрутизатора

Вариант 2 Задачи 3.1

62. В таблице маршрутизации может содержаться следующая информация: (выбрать три ответа)

Тип маршрутизирующего протокола
Принцип инкапсуляции
Метрика
MAC-адрес устройства назначения
Входной интерфейс маршрутизатора
Выходной интерфейс маршрутизатора

Вариант 3 Задачи 3.1

63. Две основные функции маршрутизаторов:
    Предотвращение коммутационных петель
    Деление сети на сегменты коллизий
    Выбор наилучшего пути для пакетов на пути к адресату назначения.
    Продвижение принятого пакета с входного интерфейса на соответствующий выходной интерфейс
    Деление локальных сетей на домены коллизий

Задача 3.2
Вариант 1 Задачи 3.2

64. Заголовок пакета содержит информацию:
    О физическом MAC-адресе узла назначения
    О сетевом адресе узла назначения
    О MAC-адресе источника
    О сетевых адресах промежуточных маршрутизаторов на пути к адресату
    О физическом MAC-адресе предыдущего маршрутизатора

Вариант 2 Задачи 3. 2

65. Таблицу протокола разрешения адресов ARP можно просмотреть по команде:
    ipconfig
    ipconfig /all
    arp –a
    netstat
    nslookup

Вариант 3 Задачи 3.2

66. Таблица протокола разрешения адресов ARP содержит:
    IP адреса устройств назначения
    Пару соответствующих IP и MAC адресов устройств глобальных сетей
    Пару соответствующих IP и MAC адресов устройств локальных сетей
    MAC адреса устройств источников информации

Задача 3.3
Вариант 1 Задачи 3.3

67. Энергонезависимая оперативная память NVRAM хранит:
    Операционную систему IOS
    Программу начальной загрузки
    Программу теста аппаратных средств
    Конфигурационный файл

Вариант 2 Задачи 3.3

68. Энергонезависимая флэш-память хранит:
    Операционную систему IOS
    Программу начальной загрузки
    Программу теста аппаратных средств
    Конфигурационный файл

Вариант 3 Задачи 3.3

69. Энергонезависимая память ПЗУ хранит: (выбрать два ответа)
    Операционную систему IOS
    Программу начальной загрузки
    Программу теста аппаратных средств
    Конфигурационный файл

Задача 3.4
Вариант 1 Задачи 3.4

70. Адрес 130.200.255.255 является:
    Широковещательным адресом класса A
    Уникальным адресом класса A
    Широковещательным адресом класса B
    Уникальным адресом класса B
    Широковещательным адресом класса C
    Уникальным адресом класса C

Вариант 2 Задачи 3.4

71.Для создания подсетей из узловой (хостовой) части адреса сети класса C может быть заимствовано максимальное число бит:
    2, 4, 6, 8

Вариант 3 Задачи 3.4

72. Радикальное решение задачи расширения числа IP-адресов, доступных для публичного (общедоступного) использования, обеспечивает следующая технология:
    Бесклассовая адресация на основе префикса (CIDR)
    Маски переменной длины (VLSM)
    Трансляция сетевых адресов (NAT)
    Новая версия IPv4
    Новая версия IPv6

Задача 3.5
Вариант 1 Задачи 3.5

73. Узел с IP-адресом 172.30.100.11 и маской по умолчанию будет находиться в следующей сети:
    172.30.100.0
    172.30.100.10
    172.30.0.0
    172.30.100.11
    172.0.0.0

Вариант 2 Задачи 3.5

74. Из представленных адресов широковещательным адресом класса C будет:
    190.168.255.255
    100.168.255.255
    221.168.253.255
    224.168.253.255
    129.168.253.255

Вариант 3 Задачи 3.5

75. Двоичному адресу 11000000.10101000.11010010. 01101001 соответствует следующий адрес:

172.192.200.105
+ 192.168.210.105
200.201.102.101
192.210.102.161
192.172.168.95

Задача 3.6
Вариант 1 Задачи 3.6

76. При заимствовании четырех бит из поля адреса узла класса С подсетей может быть создано:

8
14
16
32
64
96

Вариант 2 Задачи 3.6

77. Какое количество устройств может быть адресовано при использовании маски 255.255.248.0?

2046
2048
254
1024
256

Вариант 3 Задачи 3.6

78. При использовании маски 255.255.240.0 для создания сетей и подсетей используется:

12 бит
16 бит
18 бит
20 бит
22 бита

Задача 3.7
Вариант 1 Задачи 7

79. При использовании адресов класса В для создания 100 подсетей необходимо сконфигурировать следующую маску:

255.255.0.0
255.255.240.0
255.255.254.0
255.255.255.0
255.255.255.128
255.255.0.192

Вариант 2 Задачи 3.7

80. При использовании адресов класса C для создания 20 подсетей необходимо сконфигурировать следующую маску:

255.255.255.0
255.255.255.252
255.255.255.248
255.255.255.240
255.255.255.224
255.255. 255.192

Вариант 3 Задачи 3.7

81. При создании сети 192.168.10.0/26 администратор задал адрес Ethernet-интерфейса, являющегося шлюзом по умолчанию - 192.168.10.63. Корректно ли задание такого адреса?

Корректно
Не корректно, потому что назначен неиспользуемый адрес
Не корректно, потому что на Ethernet-интерфейсе маршрутизатора сконфигурирован широковещательный адрес
Не корректно, потому что на Ethernet-интерфейсе маршрутизатора сконфигурирован адрес подсети

Задача 8
Вариант 1 Задачи 3.8

82. Из перечисленных протоколов сетевыми являются: (выбрать два ответа)

IP
BGP
RIP
OSPF
IPX

Вариант 2 Задачи 3.8

83. Протоколом автоматического назначения IP-адресов устройств является:

Протокол DNS
Протокол DHCP
Протокол ARP
Протокол HTTP
Протокол SMTP

Вариант 3 Задачи 3.8

84. Протоколом разрешения адресов (определения MAC-адреса по известному IP-адресу узла назначения) является:

Протокол DNS
Протокол DHCP
Протокол ARP
Протокол HTTP
Протокол SMTP

Задача 3.9
Вариант 1 Задачи 3.9

85. Заголовок пакета сетевого протокола IP содержит:
MAC-адрес узла назначения
IP-адрес только узла источника
MAC-адреса узлов назначения и источника
IP-адреса узлов назначения и источника
№ порта узла назначения

Вариант 2 Задачи 3.9

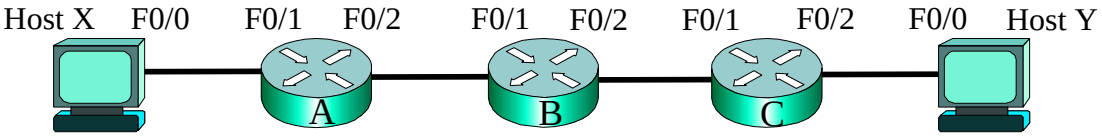
86. При назначении администратором IP-адресов на конечные узлы задаются следующие параметры: (выбрать три ответа)
IP-адрес узла
MAC-адрес узла
№ порта коммутатора
Маска сети или подсети
Адрес основного шлюза (шлюза по умолчанию)

Вариант 3 Задачи 3.9

87. Администратором обычно назначаются вручную адреса следующим устройствам: (выбрать три ответа)
Серверам
Сетевым принтерам
Локальным рабочим станциям
Ноутбукам
Маршрутизаторам
Удаленным рабочим станциям

Задача 3.10
Вариант 1 Задачи 3.10

88. При передаче кадра из маршрутизатора A в маршрутизатор B (см. рисунок и табл.)



Адреса узлов и интерфейсов маршрутизаторов

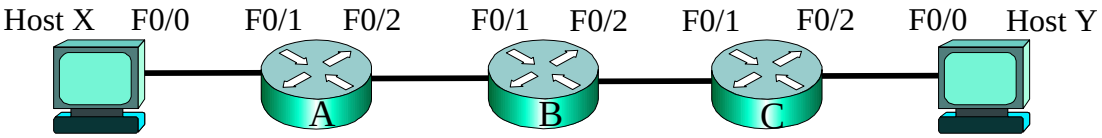
Устройство	Интерфейс	IP-адрес	MAC-адрес
Host X	F0/0	10.1.1.11	011ABC123456
Router_A	F0/1	10.1.1.1	0001AAAA1111
	F0/2	172.20.2.2	0002AAAA2222
Router_B	F0/1	172.20.2.1	0001BBBB1111
	F0/2	192.168.30.2	0002BBBB2222
Router_C	F0/1	192.168.30.1	0001CCCC1111
	F0/2	200.40.40.2	0002CCCC2222
Host Y	F0/0	200.40.40.6	022DEF123456

MAC-адресами источника и назначения будут:

011ABC123456 и 022DEF123456
011ABC123456 и 0001BBBB1111
0002AAAA2222 и 022DEF123456
0002AAAA2222 и 0001BBBB1111
0002AAAA2222 и 022DEF123456

Вариант 2 Задачи 3.10

89. При передаче кадра из маршрутизатора B в маршрутизатор C (см. рисунок и табл.)



Адреса узлов и интерфейсов маршрутизаторов

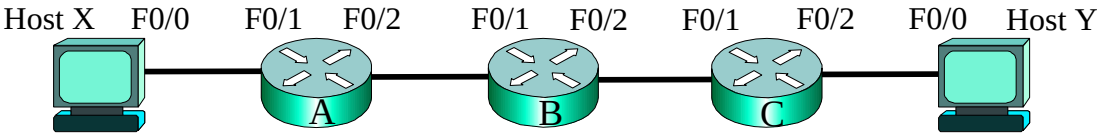
Устройство	Интерфейс	IP-адрес	MAC-адрес
Host X	F0/0	10.1.1.11	011ABC123456
Router_A	F0/1	10.1.1.1	0001AAAA1111
	F0/2	172.20.2.2	0002AAAA2222
Router_B	F0/1	172.20.2.1	0001BBBB1111
	F0/2	192.168.30.2	0002BBBB2222
Router_C	F0/1	192.168.30.1	0001CCCC1111
	F0/2	200.40.40.2	0002CCCC2222
Host Y	F0/0	200.40.40.6	022DEF123456

IP-адресами источника и назначения будут:

10.1.1.11 и 10.1.1.1
192.168.30.2 и 192.168.30.1
10.1.1.11 и 192.168.30.1
192.168.30.2 и 200.40.40.6
10.1.1.11 и 200.40.40.6

Вариант 3 Задачи 3.10

90. При передаче кадра из маршрутизатора A в маршрутизатор B (см. рисунок и табл.)



Адреса узлов и интерфейсов маршрутизаторов

Устройство	Интерфейс	IP-адрес	MAC-адрес
Host X	F0/0	10.1.1.11	011ABC123456
Router_A	F0/1	10.1.1.1	0001AAAA1111
	F0/2	172.20.2.2	0002AAAA2222
Router_B	F0/1	172.20.2.1	0001BBBB1111
	F0/2	192.168.30.2	0002BBBB2222
Router_C	F0/1	192.168.30.1	0001CCCC1111
	F0/2	200.40.40.2	0002CCCC2222
Host Y	F0/0	200.40.40.6	022DEF123456

IP-адрес назначения и MAC-адрес назначения будут:

10.1.1.1 и 0001BBBB1111
172.20.2.1 и 0001BBBB1111
172.20.2.1 и 022DEF123456
200.40.40.6 и 0001BBBB1111
200.40.40.6 и 022DEF123456

Задача 3.11
Вариант 1 Задачи 3.11

91. Максимальная общая длина пакета, включая заголовок и поле данных, может составлять:
64 Кбайт
20 Кбайт
1500 байт
32 Кбайт
256 Кбайт

Вариант 2 Задачи 3.11

92. Если длина пакета больше максимальной длины кадра, то пакет:

Фрагментируется
Отбрасывается
Возвращается узлу источнику
Передается через другой сегмент сети

Вариант 3 Задачи 3.11

93.Заголовок пакета IP имеет размер (без учета поля опций):
32 бита
32 байта
20 байт
128 бит
64 байта

Задача 3.12
Вариант 1 Задачи 3.12

94. Смещение в байтах поля данных фрагментированного пакета от начала общего поля данных исходного не фрагментированного пакета задает поле:
Поле Fragment Offset
Поле Header Checksum
Поле флагов
Поле Total Length

Вариант 2 Задачи 3.12

95. Поле контрольной суммы заголовка IP-пакета Header Checksum проверяет:
Поле данных
Заголовок
Заголовок и поле данных
Поле опций

Вариант 3 Задачи 3.12

96. Время жизни Time to Live используется:
    Для ограничения числа узлов, через которые может пройти пакет
    Для продления времени жизни пакета
    Для определения длительности задержки пакета
    Для ограничения скорости передачи данных

Задача 3.13
Вариант 1 Задачи 3.13

97. Каковы основные цели маршрутизирующего протокола?
    Передавать широковещательные послания
    Преобразовывать IP-адреса в MAC-адреса
    Коммутировать трафик на все доступные интерфейсы
    Разделять сетевую информацию между маршрутизаторами

Вариант 2 Задачи 3.13

98. Из нижеприведенных протоколов к протоколу вектора расстояния относится:
    IP
    BGP
    RIP
    OSPF
    IS-IS

Вариант 3 Задачи 3.13

99. Из нижеприведенных протоколов к протоколу состояния канала относится:
    IP
    IGRP
    RIP
    OSPF
    EIGRP

Задача 3.14
Вариант 1 Задачи 3.14

100. В протоколе вектора расстояния RIP максимальное значение метрики не может превышать значение:
    16
    15
    255
    1
    256

Вариант 2 Задачи 3.14

101. Если до истечения времени таймера удержания информации приходит обновление от другого маршрутизатора с лучшей метрикой, чем была ранее, то:

    Протокол помечает сеть как доступную и выключает таймер
    Это обновление игнорируется
    Маршрутизатор мгновенно рассылают информацию об изменении в сети
    Удаляет маршрут в обратном направлении (route poisoning).

Вариант 3 Задачи 3.14

102. Принцип расщепления горизонта указывает, что:

Запускается таймер удержания информации
Обновление производится сразу, как только маршрутизатор обнаружит изменения в сети
Нельзя посылать информацию маршрутизатору об изменениях в сети в обратном направлении
Маршрут помечается как недоступный (route poisoning).

Вариант 1 Задачи 3.15

103. Два места, где рекомендуется сохранять конфигурационный файл:

Сервер FTP
Узлы сети
Память NVRAM
TFTP сервер
Память flash

Вариант 2 Задачи 3.15

104. Два места, где рекомендуется сохранять образ операционной системы:

Сервер FTP
Узлы сети
Память NVRAM
TFTP сервер
Память flash

Вариант 3 Задачи 3.15

105. Подключение терминального оборудования к сети осуществляется через устройство:

DTE
CSU/DSU
Коммутатор
Маршрутизатор

Раздел 4. ПРОТОКОЛЫ МАРШРУТИЗАЦИИ

Лекция 9. ОСНОВЫ КОНФИГУРИРОВАНИЯ МАРШРУТИЗАТОРОВ

Краткая аннотация лекции: Рассмотрены режимы конфигурирования, вопросы создания начальной конфигурации маршрутизатора. Приведены примеры создания имен маршрутизаторов, паролей, задание адресов интерфейсов, их включение, сохранение и удаление конфигурации.
Цель лекции: изучить основы конфигурирования маршрутизаторов.

9.1. Режимы конфигурирования маршрутизаторов

Устройства Cisco имеют три режима функционирования (табл. 9.1):

1. Режим ROM monitor
2. Режим Boot ROM
3. Режим Cisco IOS

Каждый из режимов характеризуется своим собственным приглашением к работе (prompt), вид которых также приведен в табл. 9.1.

Таблица 9.1

Режимы функционирования устройств Cisco

Режим	Приглашение Prompt	Использование
ROM monitor	> или Rommon>	Исправление и восстановления пароля
Boot ROM	Router(boot)>	Модификация операционной системы Cisco IOS
Cisco IOS	Router>	Нормальное функционирование

Изменение режима функционирования маршрутизатора может производиться путем переустановки конфигурационного регистра, значение которого может задавать системный администратор. Режим **ROM monitor** выполняет процесс начальной загрузки и обеспечивает диагностику аппаратных средств. Этот режим также используется для исправления и восстановления утерянного пароля. Режим ROM monitor может быть доступен только при прямом подключении через **консольный порт**.

В режиме загрузки маршрутизатора **Boot ROM**, доступна только ограниченная группа установок. При этом идет обращение к постоянному запоминающему устройству ROM, где хранится сокращенная версия операционной системы Cisco IOS, записанной в ПЗУ при изготовлении маршрутизатора. Данный режим используется, когда повреждена IOS,

хранящаяся во флеш-памяти, и нет доступа к образу операционной системы на tftp-сервере. Режим Boot ROM позволяет записывать операции во флэш-память и модифицировать операционную систему Cisco IOS.

Для нормального функционирования маршрутизатора требуется запуск операционной системы (IOS) и конфигурационного файла (см. рис. 7.3). Нормальное функционирование маршрутизатора требует использования полной версии системы *Cisco IOS*, которая хранится во флэш-памяти или на tftp-сервере, и копируется в оперативную память.

Инициализация маршрутизатора происходит при начальной загрузке операционной системы и конфигурационного файла. Конфигурационный файл обычно хранится в энергонезависимой памяти NVRAM, откуда загружается в оперативную память RAM. Если маршрутизатор не может найти конфигурационный файл в памяти NVRAM или на tftp-сервере, то он входит в диалоговый режим **setup** создания конфигурационного файла. По завершению режима setup резервная копия конфигурационного файла (**backup configuration**) может быть сохранена в NVRAM. При последующем включении маршрутизатора сохраненный в NVRAM конфигурационный файл (**startup configuration**) будет загружен в оперативную память RAM.

Отказавшись от режима **setup**, администратор может создать новый конфигурационный файл. Система Cisco IOS имеет **интерфейс командной строки** (command line interface – **CLI**) для создания и изменения конфигурационного файла.

Обучение конфигурированию маршрутизаторов может проводиться как на реальном оборудовании, так и с использованием пакетов прикладных программ моделирования устройств и сетей, таких как *Packet Tracer, Router Sim* и других.

Создание конфигурационного файла маршрутизатора производится в нескольких режимах конфигурирования, которые приведены в табл. 9.2

Пользовательский режим (user mode) используется, для проверки состояния устройства, а также для перехода в **привилегированный режим** (**privileged mode**). Никаких изменений в конфигурационном файле, в том числе удаление и сохранение текущей конфигурации, в пользовательском режиме производиться не может. В этом режиме доступны только некоторые команды верификации **show**, т.е. команды просмотра состояния устройства.

Таблица 9.2

Режимы конфигурирования маршрутизаторов

Название режима	Приглашение (Prompt)	Описание
User EXEC Mode.	Router>	Пользовательский режим
Privileged EXEC Mode	Router#	Привилегированный режим
Global Configuration Mode	Router(cofig)#	Глобальный режим конфигурирования
Complex and multiple-line Configuration	Router(cofig-mode)#	Режим детального конфигурирования
SETUP Mode		Диалоговый режим начального конфигурирования
RXBOOT Mode		Режим начальной загрузки в аварийных ситуациях

Для создания конфигурационного файла маршрутизатора необходимо подключить его консольный порт (**console**) к последовательному порту COM1 или COM2 компьютера (терминала), включить маршрутизатор и обратиться к программе Hyper Terminal (последовательность: Программы, Стандартные, Связь, Hyper Terminal). При этом последовательно появляются окна (рис. 9.1):

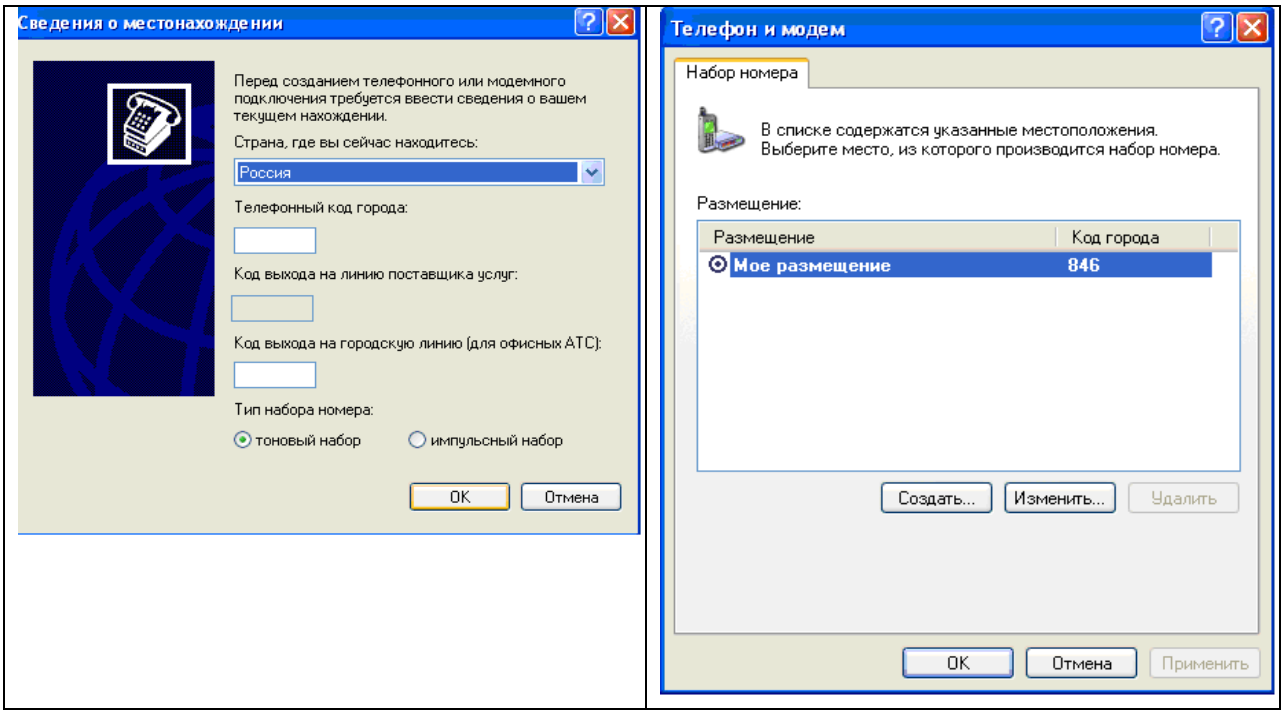
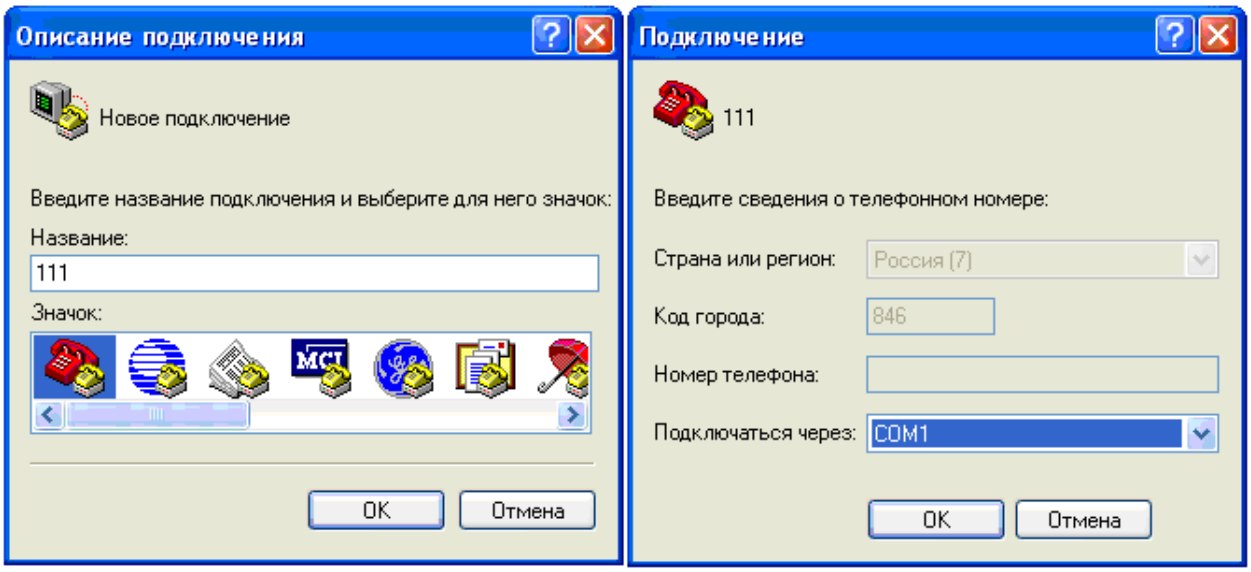


Рис. 9.1. Последовательность запуска программы Hyper Terminal

В первом окне необходимо задать страну (Россия), во втором – код города (например, 846).

В третьем окне (рис. 9.2а) следует обозначить подключение (например, 111), затем ввести интерфейс терминала – COM1 (рис. 9.2б).



а) б)

Рис. 9.2. Ввод названия подключения и интерфейса терминала

В последнем окне (рис. 9.3) необходимо задать параметры порта: скорость – **9600** бит/с; биты данных – **8**; четность – **нет**; стоповые биты – **1**; управление потоком – **нет.**

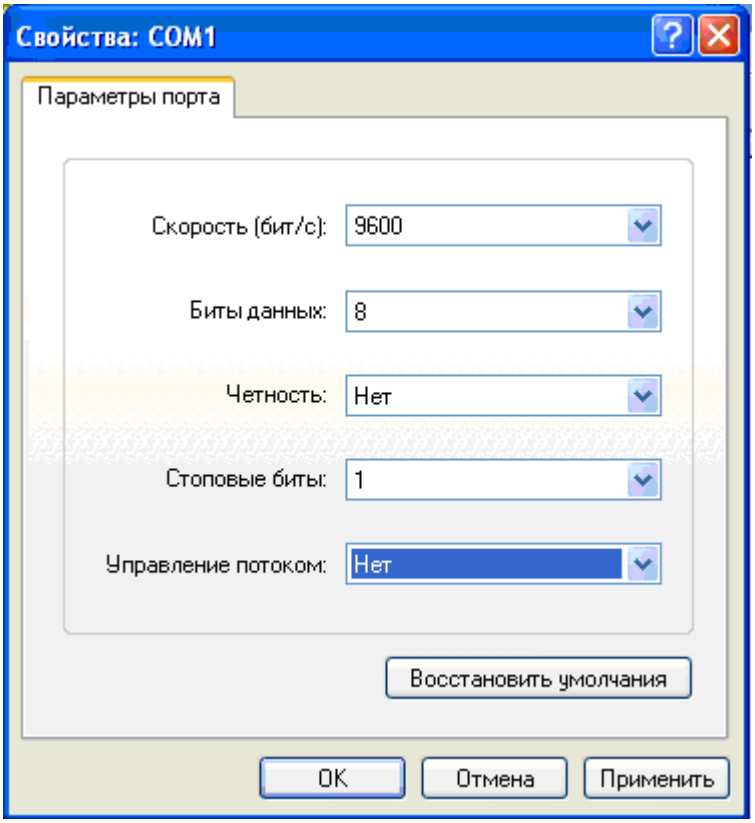


Рис. 9.3. Ввод параметров порта

После этого при нажатии клавиши «Enter» происходит начальная загрузка маршрутизатора.

При работе с пакетом Packet Tracer (рис. 9.4) необходимо запустить пакет, выбрать маршрутизатор, например, серии 2811, произвести «клик» по устройству. При этом в появившемся окне **выбрать режим CLI**.

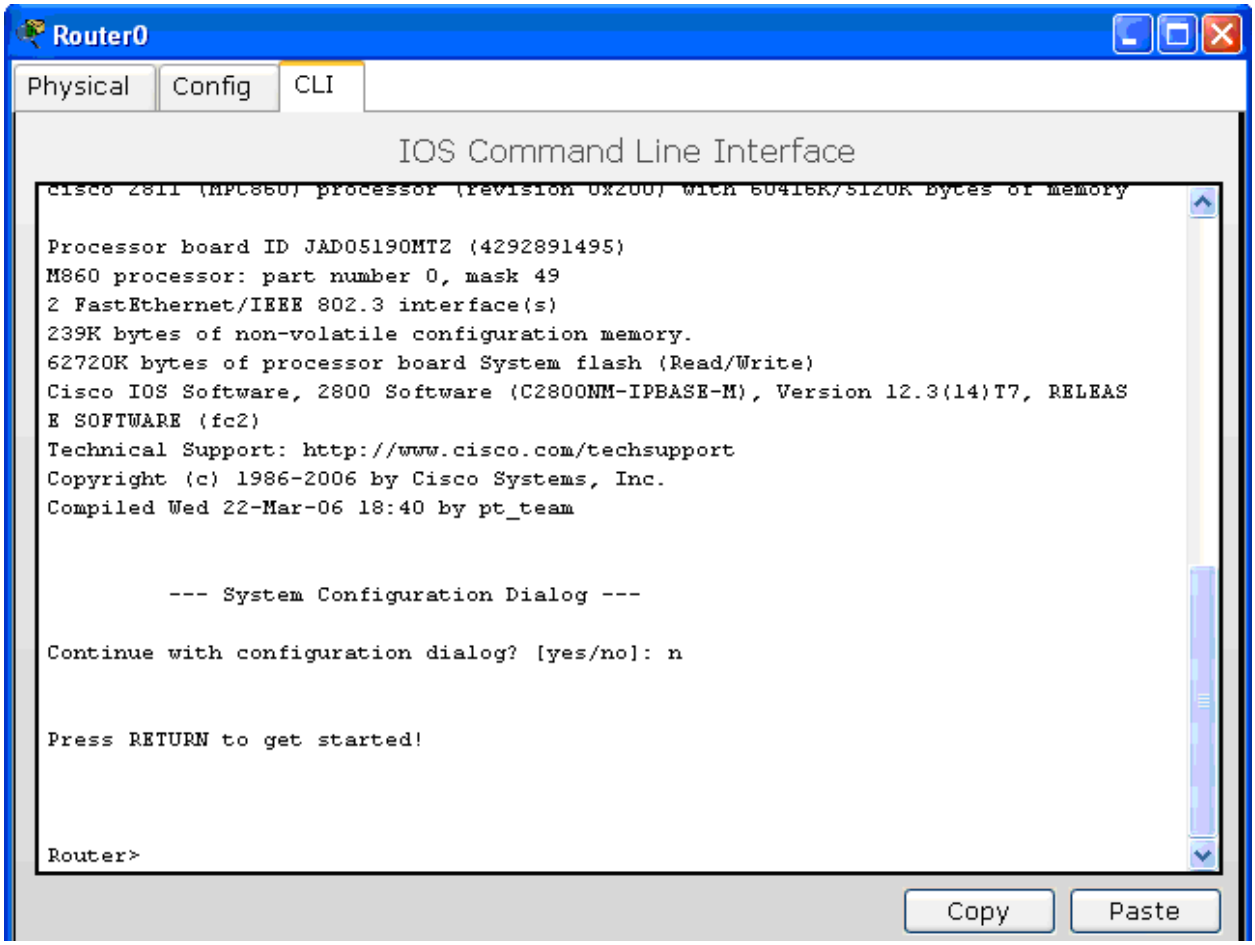


Рис. 9.4. Использование пакета Packet Tracer

После начальной загрузки маршрутизатора операционная система предложит продолжить **конфигурирование в диалоговом режиме, от которого следует отказаться** (Continue with configuration dialog? [yes/no]: **no**). Аналогичная запись появляется и при работе с реальными устройствами. В некоторых версиях операционных систем затем необходимо подтвердить завершение диалогового режима. Далее маршрутизатор входит в пользовательский режим конфигурирования, приглашение которого согласно табл. 9.2 будет:

```
Router>
```

Для перехода в привилегированный режим, необходимо ввести команду **enable**. При этом приглашение prompt изменяется с Router> на Router#:

```
Router>enable
Router#
```

В привилегированном режиме доступны все команды **show**, возможно удаление конфигурации и сохранение конфигурационного файла в памяти NVRAM. Возврат в пользовательский режим производится командой **disable** или **exit**:

```
Router#exit
```

При конфигурировании обычно используется сокращенное написание команд, например команда **enable** может быть представлена как **ena:**

```
Router>ena
Router#
```

9.2. Создание начальной конфигурации маршрутизатора

Изменение и создание конфигурации маршрутизатора Cisco возможно в режиме глобального конфигурирования, вход в который реализуется из привилегированного по команде **configure terminal** (сокращенно – **conf t**), которая вводит устройство в **глобальный режим** и позволяет изменять текущую конфигурацию (running-config). При этом приглашение изменяет вид на Router(config)#:

```
Router>ena
Router#conf t
Enter configuration commands, one per line.  End with
CNTL/Z.
Router(config)#
```

В глобальном режиме производятся изменения, которые затрагивают маршрутизатор в целом, поэтому он и называется **global configuration mode**. Например, в этом режиме можно устанавливать имя маршрутизатора по

команде **hostname**. Имя маршрутизатора не имеет значения в сети Интернет и существенно только в локальной, оно удобно при конфигурировании:

```
Router(config)#hostname Router_A
Router_A(config)#
```

В режиме глобального конфигурирования на маршрутизатор можно устанавливать пароли. Существует несколько видов паролей для обеспечения защиты маршрутизаторов Cisco. Первые два пароля **enable secret** и **enable password** используются для обеспечения авторизованного входа в привилегированный режим. На маршрутизаторе устанавливается один (или оба) из этих паролей. После установки пароля система запрашивает его у пользователя, когда вводится команда **enable**. Формат команд установки паролей **cisco** и **cisco1** для входа в привилегированный режим приведен ниже:

```
Router_A(config)#enable secret cisco
Router_A(config)#enable password cisco1
```

Пароль **enable secret криптографируется** по умолчанию, поэтому является более строгим. Если установлены оба пароля **enable secret** и **enable password**, то в приведенном примере система будет реагировать на пароль **cisco**. Пароль **enable password** по умолчанию не криптографируется, поэтому его можно посмотреть, например, по команде, **show running-configuration** (сокращенно **sh run**), которая выполняется из привилегированного режима. Ниже приведена часть распечатки команды верификации show running-configuration:

```
Router_A#sh run
Building configuration..

Carrent configuration: 594 bytes
!
version 12.3
no service password-encryption
!
hostname Router_A
!
!
enable secret 5 $1$mERr$hx5rVt7rPNos4wqbXKX7m0
enable password cisco1
        . . .
```

Из пользовательского режима команда sh run не выполняется!

Информация для конфигурирования маршрутизатора может приходить от различных источников через разные линии, например:

с линии консольного порта (Console);

с виртуальных линий интерфейсов терминалов (Virtual Terminals – **vty 0-4**) при использовании протоколов **Telnet** или **SSH**. Цифры **0-4** означают, что можно использовать 5 сессий **Telnet** удаленного доступа к устройству. Вход с линий может производиться в пользовательском режиме, поэтому на каждый из этих входов можно и **нужно установить пароль.**

Для задания пароля на вход в пользовательский режим необходимо сконфигурировать пароли на линии, через которые осуществляется вход. Например, установка пароля на линию 0 консольного порта (**console 0)** осуществляется следующей последовательностью команд:

```
Router_A(config)#line console 0
Router_A(config-line)#password cisco 2
Router_A(config-line)#login
```

а защита паролем виртуальных линий **vty 0 4** для организации удаленного доступа Telnet в маршрутизатор последовательностью:

```
Router_A(config-line)#line vty 0 4
Router_A(config-line)# password cisco 3
Router_A(config-line)# login
```

После установки паролей следует провести верификацию текущей конфигурации по команде **sh run**, для чего перейти в привилегированный режим, последовательно используя последовательно две команды **exit** или одну команду **ctr z**:

```
Router_A#sh run
     . . .
hostname Router_A
!
enable secret 5 $1$mERr$hx5rVt7rPNos4wqbXKX7m0
enable password cisco1
!
line con 0
 password cisco 2
 login
line vty 0 4
 password cisco 3
 login
```

Следует обратить внимание, что после ввода команды **line** маршрутизатор переходит в режим детального конфигурирования, когда приглашение изменяет вид `Router(config-line)#`.

Из других видов режима детального конфигурирования следует отметить режим конфигурирования интерфейсов:

`Router(config-if)#`,

субинтерфейсов:

`Router(config-subif)#`,

конфигурирования протоколов динамической маршрутизации:

`Router(config-router)#`.

В ряде случаев бывает необходимо режим криптографирования паролей распространить на все виды паролей. Это делается по команде **service password-encryption** в режиме глобального конфигурирования:

```
Router_A(config)# service password-encryption
```

При этом в текущей конфигурации будут следующие изменения:

```
Router_A#sh run
Building configuration..
     . . .
version 12.3
service password-encryption
!
hostname Router_A
!
enable secret 5 $1$mERr$hx5rVt7rPNos4wqbXKX7m0
enable password 7 0822455D0A1654
     . . .
!
line con 0
 password 7 0822455D0A164545
 login
line vty 0 4
 password 7 0822455D0A164544
 login
!
end
Router_A#
```

Из распечатки следует, что все пароли криптографированы, причем пароль enable secret имеет сложную криптограмму, а остальные пароли – простую.

При конфигурировании помимо комбинации клавиш **ctr z** бывает удобно использовать также следующие:

ctr A – перевод курсора в начало командной строки,

ctr E – перевод курсора в конец командной строки,

↑ – прокрутка, вызов ранее используемых команд.

9.3. Конфигурирование интерфейсов

Как было отмечено выше, маршрутизатор сетевого адреса не имеет, но каждый его интерфейс (порт) имеет уникальный адрес, сетевая часть которого совпадает с номером сети, соединенной с данным интерфейсом. Поэтому создание IP-сети производится с помощью интерфейсов маршрутизатора, которые имеют свои IP-адреса. Как правило, маршрутизатор имеет два или больше последовательных (serial) интерфейсов и один или несколько интерфейсов Ethernet или FastEthernet. Дальнейшее конфигурирование маршрутизаторов проведено на примере сети (рис. 9.5), включающей 4 маршрутизатора (A, B, C, D), объединяющих 4 локальных сети (Сеть 1, Сеть 2, Сеть 3, Сеть 4).

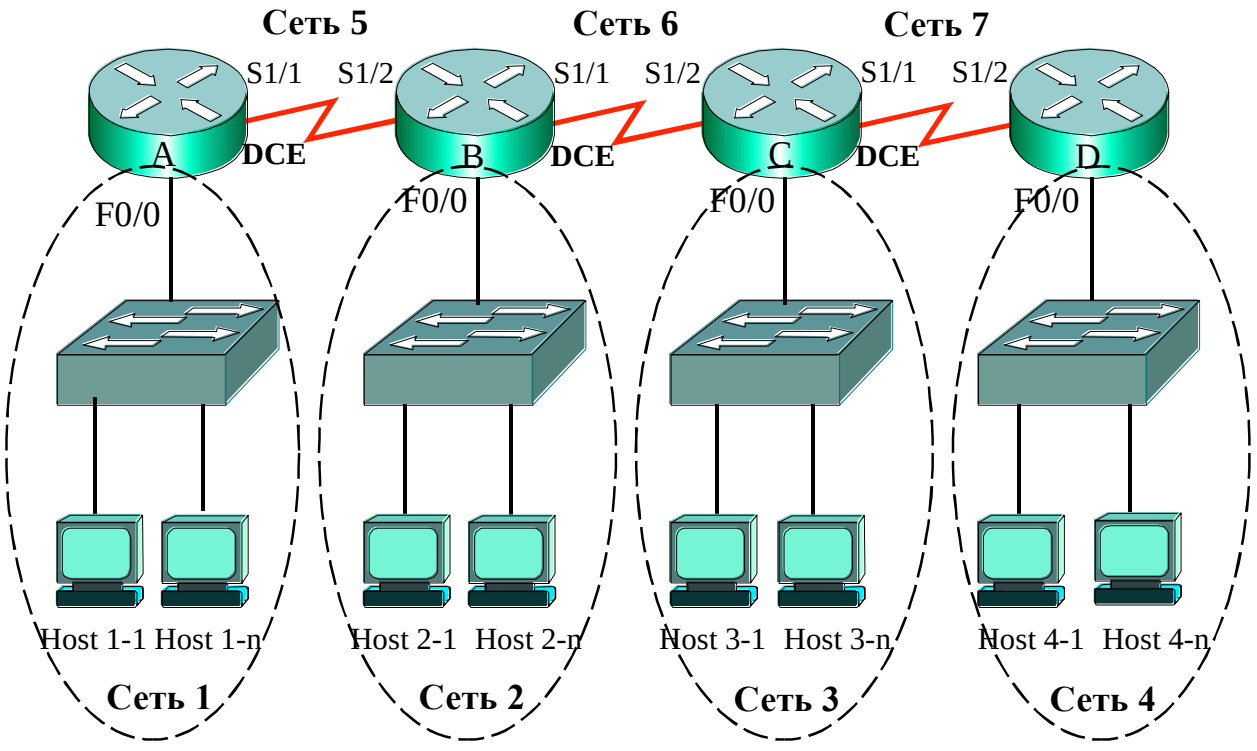


Рис. 9.5. Схема сети

Из рис.9.5 следует, что для нормального функционирования сети необходимо сконфигурировать:

у маршрутизатора A интерфейсы f0/0, s1/1,

у маршрутизатора B – интерфейсы f0/0, s1/1, s1/2,

у маршрутизатора C – интерфейсы f0/0, s1/1, s1/2,

у маршрутизатора D – интерфейсы f0/0, s1/2.

Адреса всех семи сетей, а также названия и адреса интерфейсов приведены в табл. 9.3.

Таблица 9.3

Адреса сетей и интерфейсов маршрутизаторов

Название сети	IP-адрес сети	Интерфейсы	IP-адрес интерфейса
Сеть 1	192.168.10.0/24	F0/0	192.168.10.1
Сеть 2	192.168.20.0/24	F0/0	192.168.20.1
Сеть 3	192.168.30.0/24	F0/0	192.168.30.1
Сеть 4	192.168.40.0/24	F0/0	192.168.40.1
Сеть 5	200.50.50.0/24	S1/1	200.50.50.11
		S1/2	200.50.50.12
Сеть 6	200.60.60.0/24	S1/1	200.60.60.11
		S1/2	200.60.60.12
Сеть 7	200.70.70.0/24	S1/1	200.70.70.11
		S1/2	200.70.70.12

Конфигурирование включает задание IP-адреса, включение интерфейса, который по умолчанию выключен, а для последовательных интерфейсов типа DCE (рис.10.6) – задание скорости передачи данных. Кроме того, конфигурация может включать описания и ряд других параметров.

Для того чтобы войти в режим детального конфигурирования интерфейса, используется команда **interface** в глобальном режиме конфигурации. Например, при конфигурировании интерфейса **East Ethernet** с **номером 0**, входящим в состав **слота 0** используется команда:

```
Router_A(config)#interface FastEthernet 0/0
Router_A(config-if)#.
```

Сокращенный вариант этой команды

```
Router_A(config)#int f0/0
```

Установка IP-адреса интерфейса производится следующей командой:

```
Router_A(config-if)#ip address 192.168.10.1 255.255.255.0
```

По умолчанию все интерфейсы выключены. Включение интерфейса производится по команде **no shutdown**, а выключение - командой **shutdown**:

```
Router_A(config-if)#no shutdown
```

Конфигурацию интерфейса можно просмотреть по команде **show interfaces** и **show running-config** (сокращенно **sh int** и **sh run**). По команде **sh int** производится верификация всех интерфейсов маршрутизатора. Верификация одного конкретного интерфейса производится по команде **sh int** с указанием проверяемого устройства. Ниже приведена часть распечатки команды **sh int f0/0**, по которой проводится проверка конфигурации интерфейса **FastEthernet 0/0**:

```
Router_A#sh int f0/0
FastEthernet0/0 is up, line protocol is up
Hardware is Lance, address is 0010.7b81.65e9 (bia
0010.7b81.65e9)
Internet address is 192.168.10.1/24
MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec, rely 252/255,
load 1/255
```

Из распечатки следует, что MAC-адрес интерфейса FastEthernet 0/0 будет 0010.7b81.65e9, IP-адрес – 192.168.10.1/24, где число 24 означает маску 255.255.255.0, максимальный размер кадра MTU 1500 байт, ширина полосы 100Мбит/с (BW 100000 Kbit), задержка 100 мкс (DLY 100 usec), надежность максимальная (rely 252/255), а загрузка минимальная (load 1/255). Интерфейс включен (FastEthernet0/0 is up) и протокол на нем – тоже (line protocol is up).

При конфигурировании последовательного интерфейса, имеющего DCE подключение, например интерфейса s1/1 маршрутизатора Router_A, задается не только IP-адрес, но и скорость передачи данных в битах в секунду с помощью команды **clock rate**:

```
Router_A#config t
Router_A(config)#int s1/1
Router_A(config-if)#ip address 200.50.50.11 255.255.255.0
Router_A(config-if)#clock rate 64000
Router_A(config-if)# no shutdown
```

Команда **clock rate** определяет, что интерфейс s1/1 маршрутизатора Router_A является ведущим (**DCE**) в соединении «точка-точка» с интерфейсом s1/2 маршрутизатора Router_B.

Ниже приведена часть распечатки команды **show running-config** после конфигурирования интерфейсов f0/0, s1/1 маршрутизатора Router_A:

```
Router_A#sh run
Current configuration:
version 12.3
     ...
hostname Router_A
     ...
interface FastEthernet0/0
ip address 192.168.10.1 255.255.255.0
duplex auto
speed auto
!
interface Serial1/0
no ip address
shutdown
!
interface Serial1/1
ip address 200.50.50.11 255.255.255.0
clock rate 64000
```

Из распечатки следует, что интерфейсы FastEthernet 0/0 и Serial 1/1 - включены, а интерфейс Serial 1/0 – выключен (shutdown). В распечатке приведены также IP-адреса включенных интерфейсов, скорость передачи интерфейса DCE типа Serial 1/1 (**clock rate 64000** бит/с).

Сохранение созданного конфигурационного файла производится по команде **copy running-cofig startup-config** или сокращенно **copy run start:**

```
Router_A#copy run start
Destination filename [startup-config]?
Building configuration…
[OK]
```

Сохраненный файл можно просмотреть с помощью команды **show startup-config.** Аналогично нужно сконфигурировать все другие маршрутизаторы (B, C, D) сети рис.9.5.

Конфигурационный файл может быть сохранен на сервере TFTP по команде **copy running-config tftp** или сокращенно **copy run tftp:**

```
Router_A#copy run tftp
```

Краткие итоги лекции 9

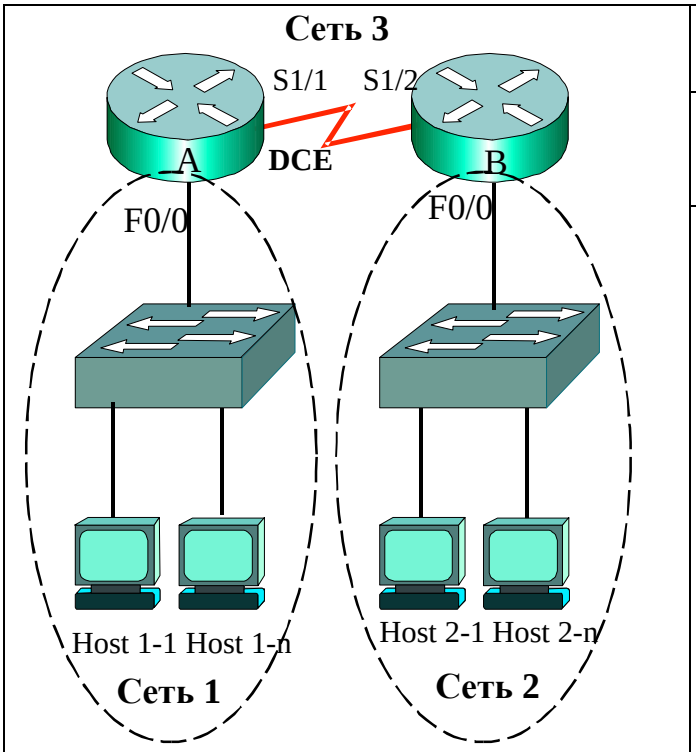
1. Устройства Cisco имеют несколько режимов функционирования: ROM monitor, Boot ROM, Cisco IOS, в которых выполняются различные задачи.
2. Для нормального функционирования маршрутизатора требуется запуск операционной системы IOS и конфигурационного файла.
3. Система Cisco IOS имеет интерфейс командной строки CLI для создания и изменения конфигурационного файла. Создание конфигурационного файла производится с консольного порта маршрутизатора, с использованием программы Hyper Terminal.
4. Создание конфигурационного файла маршрутизатора производится в нескольких режимах конфигурирования: пользовательском, привилегированном, глобального и детального конфигурирования.
5. В пользовательском режиме возможен просмотр ограниченного числа параметров и установок маршрутизатора, а также переход в привилегированный режим.
6. В привилегированном режиме можно просмотреть все параметры и установки маршрутизатора, поскольку режим защищен паролем, сохранить или удалить конфигурацию, перейти в режим глобального конфигурирования.
7. В режиме глобального конфигурирования можно задать имя маршрутизатора, защитить паролями входы маршрутизатора, перейти в режим детального конфигурирования.
8. Паролями, прежде всего, необходимо защитить консольный вход маршрутизатора, вход в привилегированный режим, удаленный доступ.
9. Режим детального конфигурирования используется для программирования интерфейсов, линий, протоколов маршрутизации.
10. При конфигурировании интерфейсов необходимо задать его адрес, маску сети или подсети, включить интерфейс; для интерфейсов типа DCE необходимо указать параметр скорости передачи данных.
11. Созданную конфигурацию можно верифицировать (проверить) с использованием различных команд show.
12. Наиболее часто используемой командой верификации является show running-config.

Вопросы по лекции 9

1. Какие режимы функционирования имеют устройства Cisco?
2. Какие режимы конфигурирования используются в маршрутизаторах для создания конфигурационного файла?
3. Что можно выполнить в пользовательском режиме конфигурирования?
4. Что можно выполнить в привилегированном режиме конфигурирования?
5. Что можно задать в режиме глобального конфигурирования?
6. Для чего используется режим детального конфигурирования?
7. Какие параметры задаются при конфигурировании интерфейсов?
8. Какие команды используются для проверки конфигурации?

Упражнения

Создайте конфигурацию маршрутизаторов нижеприведенной схемы с заданными в таблице адресами интерфейсов.



Марш-затор	Интерфейс	IP-адрес интерфейса
A	F0/0	192.168.1.1
	S1/1	200.5.5.1
B	F0/0	192.168.2.1
	S1/2	200.5.5.2

Необходимо:

1. Задать имена маршрутизаторов.
2. Сконфигурировать интерфейсы в соответствие с таблицей.
3. Установить пароль на консольную линию.
4. Установить пароль на виртуальные линии.
5. Установить на вход в привилегированный режим.
6. Проверить и сохранить конфигурацию.

Лекция 10. КОНФИГУРИРОВАНИЕ МАРШРУТИЗАЦИИ

Краткая аннотация лекции: Рассмотрены основы конфигурирования статической и динамической маршрутизации, а также маршрутизации по умолчанию. Приведены примеры конфигурирования маршрутизаторов. Проанализированы таблицы маршрутизации, методы отладки сети.
Цель лекции: изучить основы конфигурирования статической и динамической маршрутизации.

10.1. Конфигурирование статической маршрутизации

Маршруты к адресатам назначения могут быть сконфигурированы для каждого маршрутизатора вручную администратором (**статическая маршрутизация**) или созданы с помощью маршрутизирующих протоколов (**динамическая маршрутизация**). При рассмотрении конфигурирования статической маршрутизации используется составная сеть, структурная схема которой приведена на рис. 10.1.

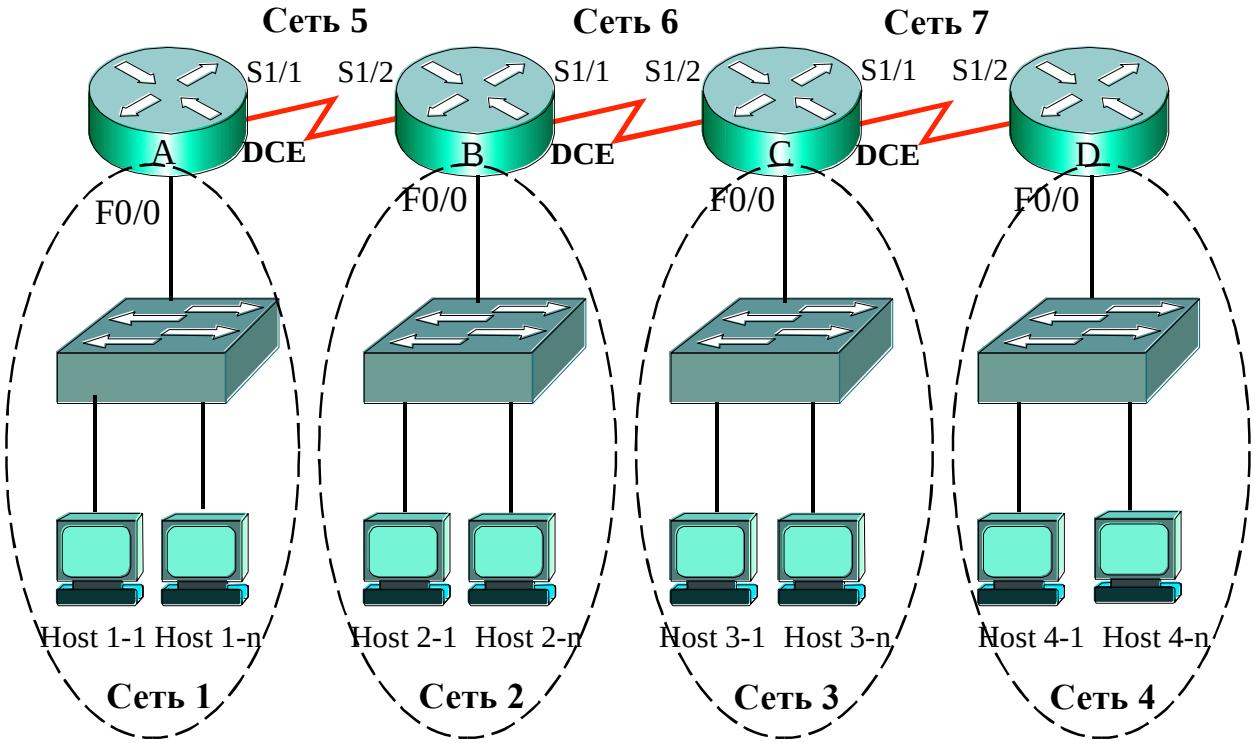


Рис.10.1. Пример составной сети

Именно для этой сети ниже приведены примеры конфигурирования маршрутизаторов. Адреса интерфейсов маршрутизаторов и узлов составной сети приведены в табл. 10.1.

Таблица 10.1

Адреса узлов составной сети

Наименование	Адрес	Наименование	Адрес
Сеть 1 f0/0 Host 1-1 Host 1-*n*	192.168.10.0/24 192.168.10.1 192.168.10.2 192.168.10.*n*	Сеть 2 f0/0 Host 2-1 Host 2-*n*	192.168.20.0/24 192.168.20.1 192.168.20.2 192.168.20.*n*
Сеть 3 f0/0 Host 3-1 Host 3-*n*	192.168.30.0/24 192.168.30.1 192.168.30.2 192.168.30.*n*	Сеть 4 f0/0 Host 4-1 Host 4-*n*	192.168.40.0/24 192.168.40.1 192.168.40.2 192.168.40.*n*
Сеть 5 s1/1 s1/2	200.50.50.0/24 200.50.50.11 200.50.50.12	Сеть 6 s1/1 s1/2	200.60.60.0/24 200.60.60.11 200.60.60.12
Сеть 7 s1/1 s1/2	200.70.70.0/24 200.70.70.11 200.70.70.12		

Чтобы сконфигурировать статическую маршрутизацию администратор должен задать маршруты ко всем возможным сетям назначения, которые не присоединены к данному маршрутизатору. Для конфигурирования статической маршрутизации используется **команда ip route**, которая содержит три параметра:

- адрес сети назначения,

- сетевую маску и

- адрес входного интерфейса следующего маршрутизатора на пути к адресату (**next hop**).

Адрес входного интерфейса следующего маршрутизатора на пути к адресату иногда называют **шлюзом по умолчанию**. Например для пакетов, попавших в маршрутизатор Router_B, шлюзами по умолчанию будут:

1. Интерфейс s1/1 маршрутизатора Router_A с адресом 200.50.50.11,
2. Интерфейс s1/2 маршрутизатора Router_C с адресом 200.60.60.12.

Ниже приведен пример конфигурирования статической маршрутизации для маршрутизатора Router_B. Данный маршрутизатор непосредственно связан с сетями 192.168.20.0, 200.50.50.0 и 200.60.60.0, поэтому статическая маршрутизация должна создаваться для остальных четырех сетей, которые непосредственно не присоединены к Router_B.

```
Router>enable
Router#config t
Router(config)#hostname Router_B
Router_B(config)#ip route 192.168.10.0 255.255.255.0 200.50.50.11
Router_B(config)#ip route 192.168.30.0 255.255.255.0 200.60.60.12
Router_B(config)#ip route 192.168.40.0 255.255.255.0 200.60.60.12
Router_B(config)#ip route 200.70.70.0 255.255.255.0 200.60.60.12
Router_B(config)#exit
Router_B#copy run start
```

Верификация статической конфигурации производится по командам **show ip route** и **show running-config**. Например, по команде **show ip route** отображается таблица маршрутизации:

```
Router_B#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       * - candidate default, U - per-user static route, o – ODR
       P – periodic downloaded static route

Gateway of last resort is not set

S     192.168.10.0/24 [1/0] via 200.50.50.11
C     192.168.20.0/24 is directly connected. FastEthernet0/0
S     192.168.30.0/24 [1/0] via 200.60.60.12
S     192.168.40.0/24 [1/0] via 200.60.60.12
C     200.50.50.0/24 is directly connected. Serial1/2
C     200.60.60.0/24 is directly connected. Serial1/1
S     200.70.70.0/24 [1/0] via 200.60.60.12
Router_B#
```

Символами C в таблице маршрутизации помечены непосредственно присоединенные к маршрутизатору сети, а символом S – созданные администратором статические маршруты к указанным сетям. Так

статический маршрут к сети 192.168.10.0 проложен через интерфейс s1/1 маршрутизатора Router_A с адресом 200.50.50.11, маршруты к трем другим сетям проложены через шлюз 200.60.60.12. Приведенные в распечатке значения [1/0] представляют собой «административное расстояние» и метрику. Маршрутизатор использует административное расстояние каждого маршрута, чтобы определить лучший путь к адресату. **Административное расстояние** – это число, величина которого определяется источником задаваемого маршрута. Меньшее административное расстояние означает более надежный источник. Например, при статической маршрутизации используется значение административного расстояния равное 1, а для протокола маршрутизации RIP административное расстояние – 120. Различные протоколы маршрутизации имеют различные заданные по умолчанию административные расстояния (табл. 10.2). В таблице маршрутизации устанавливается путь с самым низким административным расстоянием. Метрика статического маршрута равна 0.

Таблица 10.2

Административные расстояния по умолчанию

Протокол	Административное расстояние	Протокол	Административное расстояние
Connected	0	OSPF	110
Static	1	IS-IS	115
EIGRP summary	5	RIP	120
eBGP	20	EIGRP (External)	170
EIGRP (Internal)	90	iBGP (External)	200
IGRP	100		

Таким образом, по команде **sh ip route** в таблице маршрутизации отображаются адреса сетей назначения и адреса входных интерфейсов ближайших маршрутизаторов на пути к адресату. Созданные статические маршруты можно также посмотреть с помощью команды **show running-config** (сокращенно **sh run**), часть распечатки которой приведена ниже:

```
  Router_B#sh run
Current configuration:
version 12.3
        ...
hostname Router_B
!
```

```
interface FastEthernet0/0
ip address 192.168.20.1 255.255.255.0
duplex auto
speed auto
         ...
interface Serial1/0
no ip address
shutdown
!
interface Serial1/1
ip address 200.60.60.11 255.255.255.0
clock rate 64000
!
interface Serial1/2
ip address 200.50.50.12 255.255.255.0
         ...
ip classless
ip route 192.168.10.0 255.255.255.0 200.50.50.11
ip route 192.168.30.0 255.255.255.0 200.60.60.12
ip route 192.168.40.0 255.255.255.0 200.60.60.12
ip route 200.70.70.0 255.255.255.0 200.60.60.12
         ...
```

Удаление статических маршрутов производится командой **no ip route**, например:

```
Router_B(config)#no ip route 200.70.70.0 255.255.255.0
200.60.60.12
```

При необходимости можно полностью очистить конфигурацию любого маршрутизатора, что производится с помощью команды:

```
Router#erase start
```

При этом удаляется файл startup-configuration, хранящийся в NVRAM. Если после этого выключить маршрутизатор и затем вновь его включить, то конфигурация маршрутизатора будет очищена.

В ряде случаев при маршрутизации задают наименование выходного интерфейса маршрутизатора вместо адреса шлюза по умолчанию (next hop). Ниже приведен пример конфигурирования маршрутизатора Router_B (рис.10.1) с использованием выходного интерфейса:

```
Router_B(config)#ip route 192.168.10.0 255.255.255.0 S1/2
Router_B(config)#ip route 192.168.30.0 255.255.255.0 S1/1
Router_B(config)#ip route 192.168.40.0 255.255.255.0 S1/1
Router_B(config)#ip route 200.70.70.0 255.255.255.0 S1/1
```

Подобное конфигурирование ускоряет процесс обработки пакета в маршрутизаторе.

Верификация работоспособности сети и таблицы маршрутизации производится с использованием **команд ping** и **traceroute**, которые проверяют обеспечение ip связи между маршрутизаторами. Команды **ping** и **traceroute** являются **утилитами протокола ICMP**, который разработан в дополнение к протоколу IP, не имеющему средств проверки достижимости или недостижимости узлов и сетей. Эти команды позволяют с каждого маршрутизатора производить тестирование (прозвонку) интерфейсов других маршрутизаторов и узлов, например:

```
Router_B#ping 192.168.10.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.1, timeout is
2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
4/4/4 ms
```

Значки !!!!! означают, что связь между маршрутизатором Router_B и интерфейсом 192.168.10.1 маршрутизатора Router_A функционирует, 100% запросов и ответов (5 из пяти) переданы без искажений. При отсутствии связи, когда невозможно прозвонить узел или интерфейс, вместо символов !!!! будет последовательность из пяти точек …..

При использовании команды **traceroute** ответ трижды передается с каждого промежуточного интерфейса, например:

```
Router_A#traceroute 192.168.40.1
Type escape sequence to abort.
Tracing the route to 192.168.40.1
   1 200.50.50.12  58 msec   48 msec   55 msec
   2 200.60.60.12  106 msec  97 msec   49 msec
   3 200.70.70.12  171 msec  120 msec  127 msec
```

Конфигурирование статической маршрутизации по умолчанию

Статическая маршрутизация по умолчанию означает, что, если пакет предназначен для сети, которая не указана в таблице маршрутизации, то маршрутизатор отправит пакет по заданному по умолчанию маршруту. При этом маршрутизатор направляет пакеты к следующему маршрутизатору, когда тот в таблице не задан явно. Заданные по умолчанию маршруты устанавливаются как часть статической конфигурации.

В процессе конфигурирования маршрутизации по умолчанию, также как при статической маршрутизации, используют команду **ip route**, но в адресе и маске сети (и подсети) используют все **нули**, которые означают **все сети и все маски**. Подобная маршрутизация устанавливается для тупиковых маршрутизаторов, т.е. она может быть установлена для маршрутизаторов A и D (рис.10.1), потому что через них лежит единственный путь в составную сеть и из нее. Например, для всех пакетов, попавших в маршрутизатор A маршрут по умолчанию будет через его порт s1/1, т.е. шлюзом будет входной интерфейс маршрутизатора Router_B с адресом 200.50.50.12.

При конфигурировании маршрутизаторов A и D необходимо предварительно *удалить все статические маршруты и затем установить маршрут по умолчанию*, например:

```
Router_A#config t
Router_A(config)#ip route 0.0.0.0 0.0.0.0 200.50.50.12
```

После конфигурирования маршрутизации по умолчанию необходимо протестировать сеть (рис. 10.1), используя команды **ping, traceroute**, **tracert**.

Иногда маршрутизатор получает пакеты, предназначенные для неизвестной подсети, входящей в известную сеть, которая объединяет подсети. При этом маршрутизатор может уничтожить такие пакеты. Для предотвращения этого нужно использовать команду глобальной конфигурации **ip classless**, чтобы программное обеспечение Cisco IOS не уничтожало пакеты, а отправляло эти пакеты по маршруту умолчания:

```
Router_A#config t
Router_A(config)#ip route 0.0.0.0 0.0.0.0 192.168.50.2
Router_A(config)#ip classless
Router_A(config)#
```

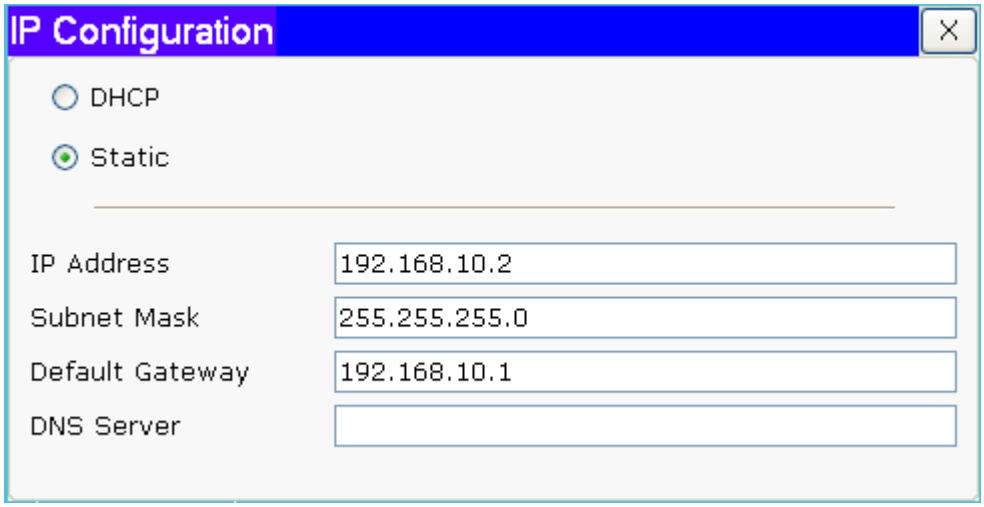
В режиме **ip classless** пакеты могут быть отправлены по маршруту умолчания или по суммарному (агрегированному) маршруту, который охватывает больший диапазон подсетей с единственным входом. Например, если какое-то предприятие использует полную подсеть 10.10.0.0/16, то суммарным маршрутом для подсети 10.10.10.0/24 будет 10.10.0.0/16. Команда **ip classless** используется по умолчанию в Cisco IOS Software Release 11.3 и позже. Чтобы отключить эту команду используется ее отрицающая форма – **no ip classless**.

10.2. Конфигурирование конечных узлов и верификация сети

Для включения в работу сети конечных узлов (host) необходимо на них установить ряд параметров: IP-адрес узла, маску, адрес шлюза. Функцию шлюзов, через которые узлы передают пакеты в сеть и получают сообщения из сети, выполняют интерфейсы f0/0 каждого маршрутизатора (рис.10.1). Технология задания IP-адреса, маски и адрес шлюза приведена на рис.6.10.

При работе с пакетом Packet Tracer задание параметров узла производится следующим образом:

1. «Кликнуть» конфигурируемый узел, например, *первый узел* Сети 1.
2. Во всплывшем окне выбрать опцию «Desktop», затем «IP Configuration» и затем в новом окне установить IP-адрес узла, маску подсети и адрес шлюза в соответствии с табл. 10.1.



Для проверки работоспособности сети «кликнуть» конфигурируемый узел, во всплывшем окне выбрать «Desktop», затем «Command Prompt», при

этом реализуется режим командной строки. Тестирование проводится с помощью команд **ping** и **tracert**. Ниже приведен пример тестирования адресов 192.168.40.1 и 192.168.40.2 с первого узла (IP-адрес 192.168.10.2) Сети 1.

```
PC>ping 192.168.40.1

Pinging 192.168.40.1 with 32 bytes of data:

Reply from 192.168.40.1: bytes=32 time=230ms TTL=252
Reply from 192.168.40.1: bytes=32 time=236ms TTL=252
Reply from 192.168.40.1: bytes=32 time=229ms TTL=252
Reply from 192.168.40.1: bytes=32 time=231ms TTL=252

Ping statistics for 192.168.40.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 229ms, Maximum = 236ms, Average = 231ms

PC>ping 192.168.40.2

Pinging 192.168.40.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.40.2: bytes=32 time=255ms TTL=124
Reply from 192.168.40.2: bytes=32 time=275ms TTL=124
Reply from 192.168.40.2: bytes=32 time=308ms TTL=124

Ping statistics for 192.168.40.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 255ms, Maximum = 308ms, Average = 279ms
```

По команде **ping** посылается четыре запроса и принимаются ответы (Reply). В первом примере тестирование проводилось интерфейса f0/0 маршрутизатора D (IP-адрес 192.168.40.1). Получены все 4 ответа, при этом указана длина пакета и время от посылки запроса до получения ответа. Во втором примере проводилась проверка узла 192.168.40.2. Первый ответ на запрос не был получен (превышено время ожидания – Request time out), остальные три ответа успешно получены.

Результатом тестирования несуществующего в сети узла 198.168.40.1 является ответ, что узел недоступен (unreachable):

```
PC>ping 198.168.40.1

Pinging 198.168.40.1 with 32 bytes of data:
```

```
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.

Ping statistics for 198.168.40.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

В следующем примере тестирование узла 192.168.40.2 проводилось с помощью команды **tracert**. По этой команде получены ответы от пяти узлов (или интерфейсов): 192.168.10.1, 200.50.50.12, 200.60.60.12, 200.70.70.12, 192.168.40.2, находящихся на трассе к адресату назначения.

```
PC>tracert 192.168.40.2

Tracing route to 192.168.40.2 over a maximum of 30 hops:

  1    89 ms     91 ms     77 ms     192.168.10.1
  2    131 ms    134 ms    137 ms    200.50.50.12
  3    212 ms    168 ms    182 ms    200.60.60.12
  4    207 ms    170 ms    198 ms    200.70.70.12
  5    288 ms    320 ms    228 ms    192.168.40.2

Trace complete.

PC>
```

10.3. Динамическая маршрутизация. Конфигурирование протокола RIP

Широко распространенным маршрутизирующим протоколом в сетях малого размера является **Routing Information Protocol** (**RIP**), который использует в качестве метрики число переходов **hop count** на пути к адресату назначения. RIP относится к протоколам вектора расстояния (distance-vector), в котором максимальное число переходов (hop) на пути от источника до назначения ограничивается числом 15. При обмене маршрутной информацией с соседями маршрутизатор увеличивает значение метрики на 1. Если значение метрики выше 15, сеть назначение считают недостижимой, т.е. при значении hop count = 16 пакет в маршрутизаторе уничтожается.

Конфигурирование протокола RIP производится путем использования команды **router rip** и сообщения протоколу **номеров непосредственно**

присоединенных сетей. При обмене маршрутной информацией между маршрутизаторами они последовательно получают от соседей информацию о всех доступных сетях автономной системы. Обмен маршрутной информацией протокол RIP производит периодически каждые 30 секунд. Таким образом, спустя некоторое время таблица маршрутизации каждого маршрутизатора будет содержать не только информацию о непосредственно присоединенных сетях, но и пути к удаленным сетям.

Важно отметить, что протокол **RIP при обмене маршрутной информацией не пересылает значение масок**. Поэтому сетевой адрес является адресом полного класса (classful). Это является основным недостатком протокола RIP.

В настоящее время в дополнение к Classful Routing Protocol – RIP Version 1 (**RIP v1**), разработан бесклассовый маршрутизирующий протокол Classless Routing Protocol – RIP Version 2 (**RIP v2**). Протокол RIP v2 дополнительно включают следующие функции:

- способность нести дополнительную информацию о маршрутизации,
- механизм аутентификации, чтобы обеспечить безопасность модернизации таблиц,
- поддержка масок подсети переменной длины (**VLSM**).

Ниже приведен пример конфигурирования протокола RIP v1 на маршрутизаторе Router_C сети рис.10.1. Предварительно на всех маршрутизаторах (A, B, C, D) автономной системы необходимо отменить все статические маршруты, используя ряд команд:

```
Router_C(config)#no ip route 200.50.50.0 255.255.255.0 200.60.60.11
```

Затем конфигурируется протокол по команде **router rip**, после которой маршрутизатор переходит в режим детального конфигурирования с расширением Router_C(config-router)# и дается описание всех непосредственно присоединенных сетей:

```
Router_C(config)#router rip
Router_C(config-router)#network 200.60.60.0
Router_C(config-router)#network 200.70.70.0
Router_C(config-router)#network 192.168.30.0
```

В приведенном примере по команде **network** перечислены три сети, непосредственно присоединенные к маршрутизатору.

После установки протокола RIP на все маршрутизаторы сети рис.10.1 необходимо провести её тестирование с использованием команд **ping, traceroute** и **tracert**. В случае недостижимости каких-либо сетей или узлов следует проверить таблицу маршрутизации и созданные в ней маршруты, используя команды **show ip route**, **show run** и **show int**.

Входы или строки таблицы маршрутизации задают пути к сетям назначения. Распечатка команды **show ip route**, отображающая таблицу маршрутизации устройства Router_C приведена ниже.

```
Router_C#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

R    192.168.10.0/24 [120/2] via 200.60.60.11, 00:00:15, Serial1/2
R    192.168.20.0/24 [120/1] via 200.60.60.11, 00:00:15, Serial1/2
C    192.168.30.0/24 is directly connected, FastEthernet0/0
R    192.168.40.0/24 [120/1] via 200.70.70.12, 00:00:21, Serial1/1
R    200.50.50.0/24 [120/1] via 200.60.60.11, 00:00:15, Serial1/2
C    200.60.60.0/24 is directly connected, Serial1/2
C    200.70.70.0/24 is directly connected, Serial1/1
Router_C#
```

Указанная распечатка команды **show ip route** показывает, что для передаваемых пакетов шлюзами (адресами следующего перехода – next hop) будут являться интерфейсы с адресами 200.60.60.11 и 200.70.70.12. Информация в квадратных скобках, например [120/2] в первой строке таблицы (на первом входе), показывает административное расстояние 120, означающее, что маршрут создан протоколом RIP (см. табл. 10.2), и что расстояние до сети 192.168.10.0 составляет 2 перехода (2 hop). Время 00:00:15 говорит о том, что предыдущее обновление было 15 секунд назад и следующее будет через 15 секунд, поскольку обновления (update) проводятся каждые 30 сек.

Конфигурирование динамической маршрутизации по умолчанию

Для маршрутизатора желательно поддерживать маршруты к каждому возможному адресу назначения. Кроме того, маршрутизаторы поддерживают маршрут по умолчанию или шлюз последней надежды (Gateway of last resort), который используются, когда маршрутизатор неспособен достичь сети назначения с более определенным входом в таблице маршрутизации.

Это позволяет маршрутизаторам отправлять пакеты, предназначенные любому узлу Интернета, без необходимости поддерживать в таблице записи (входы) для каждой сети Интернета. Маршруты по умолчанию могут быть введены администратором статически или динамически на основе маршрутизирующего протокола. Прежде, чем маршрутизаторы начнут динамически обмениваться информацией, администратор должен сформировать, по крайней мере, один маршрутизатор с маршрутом по умолчанию. Администратор может использовать любую из следующих команд, чтобы сконфигурировать маршрут по умолчанию:

ip default-network или **ip route 0.0.0.0 0.0.0.0**

Команда **ip default-network** применяется, чтобы установить маршрут по умолчанию в сетях, использующих динамические протоколы маршрутизации. Команда **ip default-network** означает, что если маршрутизатор имеет маршрут к подсети, обозначенной этой командой, он устанавливает маршрут к главной сети.

При использовании команды **ip default-network 200.70.70.0** на маршрутизаторе Router_C (рис.10.1) в таблице маршрутизации появляется строка, помеченная символом C* (кандидат сети по умолчанию):

```
Router_C(config)#ip default-network 200.70.70.0

Router_C#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set
```

```
R    192.168.10.0/24 [120/2] via 200.60.60.11, 00:00:16, Serial1/2
R    192.168.20.0/24 [120/1] via 200.60.60.11, 00:00:16, Serial1/2
C    192.168.30.0/24 is directly connected, FastEthernet0/0
R    192.168.40.0/24 [120/1] via 200.70.70.12, 00:00:04, Serial1/1
R    200.50.50.0/24 [120/1] via 200.60.60.11, 00:00:16, Serial1/2
C    200.60.60.0/24 is directly connected, Serial1/2
C*   200.70.70.0/24 is directly connected, Serial1/1
Router_C#
```

После обмена маршрутной информацией с соседями таблица маршрутизации Router_B будет иметь следующий вид:

```
Router_B#sh ip route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route
Gateway of last resort is 200.60.60.12 to network 0.0.0.0

R    192.168.10.0/24 [120/1] via 200.50.50.11, 00:00:28, Serial1/2
C    192.168.20.0/24 is directly connected, FastEthernet0/0
R    192.168.30.0/24 [120/1] via 200.60.60.12, 00:00:11, Serial1/1
R    192.168.40.0/24 [120/2] via 200.60.60.12, 00:00:11, Serial1/1
C    200.50.50.0/24 is directly connected, Serial1/2
C    200.60.60.0/24 is directly connected, Serial1/1
R    200.70.70.0/24 [120/1] via 200.60.60.12, 00:00:11, Serial1/1
R*   0.0.0.0/0 [120/1] via 200.60.60.12, 00:00:11, Serial1/1
Router_B#
```

Шлюз последней надежды для сети с неизвестным адресом – 200.60.60.12 (`Gateway of last resort is 200.60.60.12 to network 0.0.0.0`).

Последняя строка таблицы маршрутизации помечена символом R*, означающим, что маршрут по умолчанию ко всем сетям с любыми масками (0.0.0.0/0) создан с помощью протокола RIP, информация о маршруте получена от другого маршрутизатора.

Аналогичная ситуация будет в таблице маршрутизатора Router_A:

```
Router_A#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 200.50.50.12 to network 0.0.0.0

C    192.168.10.0/24 is directly connected, FastEthernet0/0
R    192.168.20.0/24 [120/1] via 200.50.50.12, 00:00:10, Serial1/1
R    192.168.30.0/24 [120/2] via 200.50.50.12, 00:00:10, Serial1/1
R    192.168.40.0/24 [120/3] via 200.50.50.12, 00:00:10, Serial1/1
C    200.50.50.0/24 is directly connected, Serial1/1
R    200.60.60.0/24 [120/1] via 200.50.50.12, 00:00:10, Serial1/1
R    200.70.70.0/24 [120/2] via 200.50.50.12, 00:00:10, Serial1/1
R*   0.0.0.0/0 [120/2] via 200.50.50.12, 00:00:10, Serial1/1
Router_A#
```

Итак, в таблице маршрутизатора Router_A появился вход (строка), помеченный символом R*, означающий, что для всех сетей с неизвестным адресом и любой маской (0.0.0.0/0) шлюзом последней надежды (**Gateway of last resort**) будет адрес 200.50.50.12, поэтому пакеты будут направляться в сторону сети 200.70.70.0.

Краткие итоги лекции 10

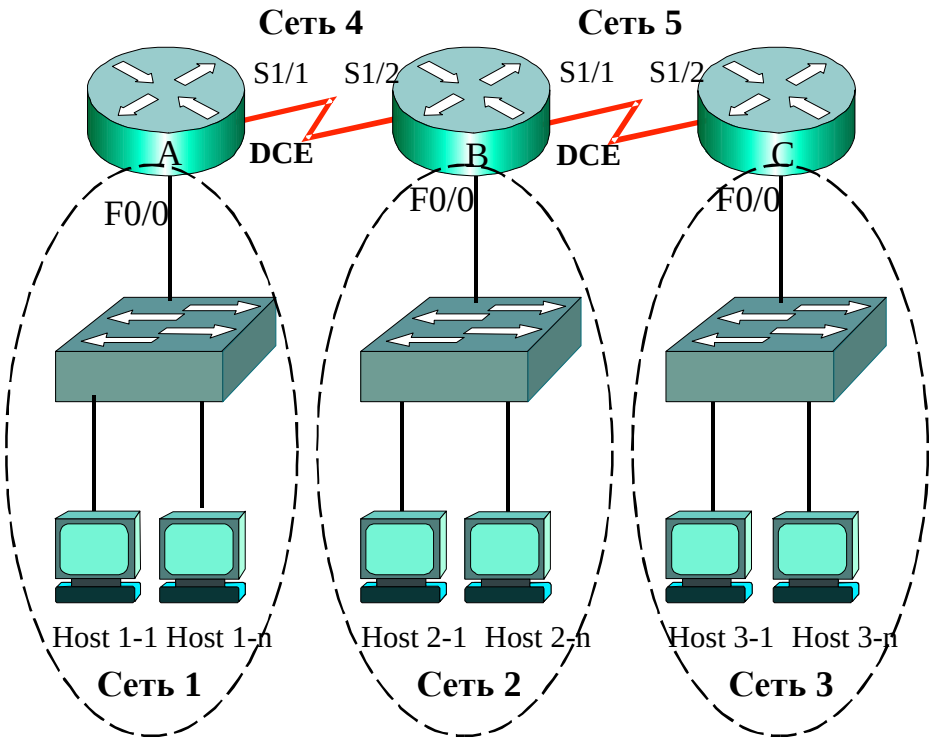
1. Статическая маршрутизация создается администратором вручную.
2. Динамическую маршрутизацию реализуют маршрутизирующие протоколы.
3. Для конфигурирования статической маршрутизации используется команда **ip route**, которая содержит параметры: адрес сети назначения, сетевую маску и адрес входного интерфейса следующего маршрутизатора на пути к адресату (**next hop**).
4. Формат команды конфигурирования статической маршрутизации следующий:
   `Router(config)#ip route <адрес> <маска> <next hop>`
5. Формат команды конфигурирования статической маршрутизации с использованием выходного интерфейса следующий:
   `Router(config)#ip route <адрес> <маска> <интерфейс>`
6. Формат команды конфигурирования статической маршрутизации по умолчанию следующий:
   `Router(config)#ip route 0.0.0.0 0.0.0.0 <next hop>`
7. Символами C в таблице маршрутизации помечены непосредственно присоединенные к маршрутизатору сети, а символом S – созданные администратором статические маршруты к удаленным сетям.
8. Маршрутизатор использует административное расстояние каждого маршрута, чтобы определить лучший путь к адресату.
9. Административное расстояние – это число, величина которого определяется источником задаваемого маршрута. Меньшее административное расстояние означает более надежный источник.
10. Различные протоколы маршрутизации имеют различные заданные по умолчанию административные расстояния. Административное расстояние протокола маршрутизации RIP равно 120.
11. Конфигурирование протокола RIP производится путем использования команды **router rip** и формального описания номеров непосредственно присоединенных сетей.
12. Команды **ping** и **traceroute** проверяют обеспечение ip связи между маршрутизаторами при отладке сети.
13. Верификация таблицы маршрутизации производится с использованием команды **show ip route.**
14. Статическая маршрутизация по умолчанию используется для отправки пакетов, когда сеть назначения отсутствует в таблице маршрутизации.
15. Команда **ip default-network** применяется, чтобы установить маршрут по умолчанию в сетях, использующих динамические протоколы маршрутизации.

Вопросы по лекции 10

1. Кто создает статическую маршрутизацию?
2. Как формируется динамическая маршрутизация?
3. Какие команды используются для создания статической маршрутизации?
4. Каков формат команды конфигурирования статической маршрутизации?
5. Каков формат команды конфигурирования статической маршрутизации с использованием выходного интерфейса?
6. Каков формат команды конфигурирования статической маршрутизации по умолчанию?
7. Каким символом помечаются непосредственно присоединенные к маршрутизатору сети?
8. Каким символом помечаются маршруты, созданные администратором?
9. Каким символом помечаются маршруты, созданные протоколом RIP?
10. Каков формат команды конфигурирования протокола RIP?
11. По какой команде можно посмотреть таблицу маршрутизации?
12. Какие команды используются для проверки и отладки конфигурации?

Упражнения

1. Сконфигурируйте статическую маршрутизацию нижеприведенной схемы с заданными в таблице адресами. Проведите проверку и отладку с использованием команд **show running-config**, **show ip route**, **ping**, **traceroute** и **tracert**.



Наименование	Адрес	Наименование	Адрес
Сеть 1 f0/0 Host 1-1 Host 1-*n*	10.1.10.0/24 10.1.10.1 10.1.10.2 10.1.10.*n*	Сеть 2 f0/0 Host 2-1 Host 2-*n*	172.16.20.0/24 172.16.20.1 172.16.20.2 172.16.20.*n*
Сеть 3 f0/0 Host 3-1 Host 3-*n*	192.168.30.0/24 192.168.30.1 192.168.30.2 192.168.30.*n*	Сеть 4 s1/1 s1/2	204.4.4.0/24 204.4.4.1 204.4.4.2
Сеть 5 s1/1 s1/2	205.5.5.0/24 200.5.5.1 200.5.5.2		

2. Удалите статическую и сконфигурируйте динамическую маршрутизацию вышеприведенной схемы с заданными в таблице адресами с использованием протокола RIP. Проведите проверку и отладку.

Контрольный тест по разделу 4

Задача 4.1
Вариант 1 Задачи 4.1

106. В качестве метрики протокола RIP используется:

Количество переходов до адресата назначения
Задержка
Сходимость
Надежность
Стоимость (cost)
Ширина полосы пропускания

Вариант 2 Задачи 4.1

107. В качестве метрики протокола EIGRP используется: (выбрать три ответа)

Количество переходов до адресата назначения
+ Задержка
Сходимость
+ Надежность
Стоимость (cost)
+ Ширина полосы пропускания

Вариант 3 Задачи 4.1

108. В качестве метрики протокола OSPF используется:

Количество переходов до адресата назначения
Задержка
Сходимость
Надежность
Стоимость (cost)
Ширина полосы пропускания

Задача 4.2
Вариант 1 Задачи 4.2

109. Информацию о конфигурационном файле, сохраненном в памяти маршрутизатора, отображает команда:

```
Router#show flash
Router#show hosts
Router#show history
Router#show version
Router#show startup-config
```

Вариант 2 Задачи 4.2

110. Информацию об операционной системе отображает команда:

```
Router#show run
Router#show hosts
Router#show history
Router#show version
Router#show startup-config
```

Вариант 3 Задачи 4.2

111. По умолчанию на последовательном интерфейсе маршрутизатора установлена следующая информация: (выбрать три ответа)

DTE
DCE
shutdown
no IP address
clock rate 64000

Задача 4.3
Вариант 1 Задачи 4.3

112. По команде `Router(config)#hostname Router-AB` маршрутизатор выдаст следующий ответ:

```
Router-AB#
Router-AB(config)#
Router-AB(config-host)#
hostname Router-AB(config)#
Router(config)#
```

Вариант 2 Задачи 4.3

113. Интерфейс маршрутизатора включает команда:

```
Router(config-if)#enable
Router(config-if)#shutdown
Router(config-if)#s0 active
Router(config-if)#interface up
Router(config-if)#no shutdown
```

Вариант 3 Задачи 4.3

114. Из нижеприведенных команд корректно будет выполняться следующая:

```
Router>sh run
Router#sh run
Router(config)#sh run
Router(config-router)#sh run
Router(config-if)#sh run
```

Задача 4.4
Вариант 1 Задачи 4.4

115. Чтобы не показывать по команде `Router#sh run`
пароли в открытом тексте, необходимо использовать следующую команду:

```
Router(config)#enable cisco secret
Router(config)#enable password cisco
Router(config)#service password-encryption
Router(config)# secret enable cisco
Router(config)#service encryption-password
```

Вариант 2 Задачи 4.4

116. Удаленный доступ к виртуальным линиям маршрутизатора по команде Telnet при использовании пароля «samara» будет разрешен при следующем наборе команд:

1.
```
Router(config-line)#config telnet
Router(config-line)#line vty 0 5
Router(config-line)#password samara
```

2.
```
Router(config)#line vty 0 4
Router(config)#password samara
```

3.
```
Router(config)#line vty 0 4
Router(config-line)#password samara
Router(config-line)#login
```

4.
```
Router(config-line)#config telnet
Router(config-line)#password samara
Router(config-line)#login
```

Вариант 3 Задачи 4.4

117. При нижеприведенной конфигурации

```
Router(config)#line console 0
Router(config-line)#password cisco1
```

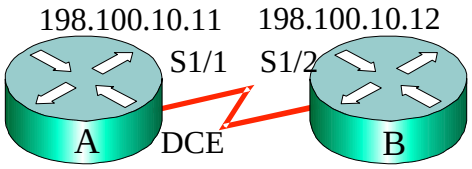
```
Router(config-line)#login
Router(config)#line vty 0 4
Router(config-line)#password cisco2
Router(config-line)#login
Router(config)#enable password cisco3
Router(config)#enable secret cisco4
```

вход в привилегированный режим конфигурирования будет разрешен по паролю:

```
cisco1
cisco2
cisco3
cisco4
```

Задача 4.5
Вариант 1 Задачи 4.5

118. При конфигурировании последовательного интерфейса S1/1 маршрутизатора A



будут использоваться три следующих команды: (выбрать три ответа)

```
Router_A(config-if)#ip address 198.100.10.12 255.255.255.0
Router_A(config-if)#no shutdown
Router_A(config-if)#ip address 198.100.10.11 255.255.255.0
Router_A(config-if)#clock rate 64000
Router_A(config-if)#ip host Router_B 198.100.10.12
```

Вариант 2 Задачи 4.5

119. Две команды, которые будут сохранять текущий конфигурационный файл на сетевом TFTP сервере будут следующие:

```
Router#copy run tftp
Router#copy tftp run
Router#copy running-config tftp
Router#copy tftp running-config
Router(config)#copy running-config tftp
Router(config)#copy tftp running-config
```

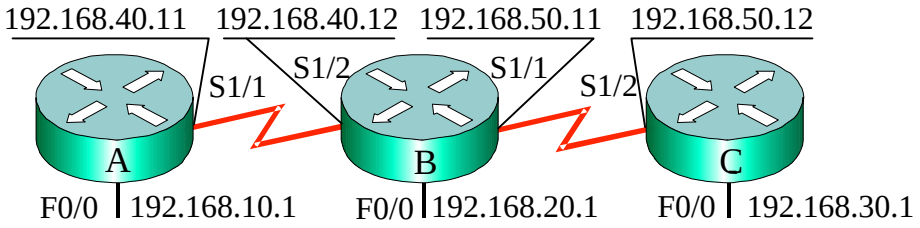
Вариант 3 Задачи 4.5

120. В режиме детального конфигурирования можно задать:

Пароль на вход в привилегированный режим
MAC-адрес интерфейса
IP-адрес интерфейса
Имя маршрутизатора
Команду верификации конфигурации

Задача 4.6
Вариант 1 Задачи 4.6

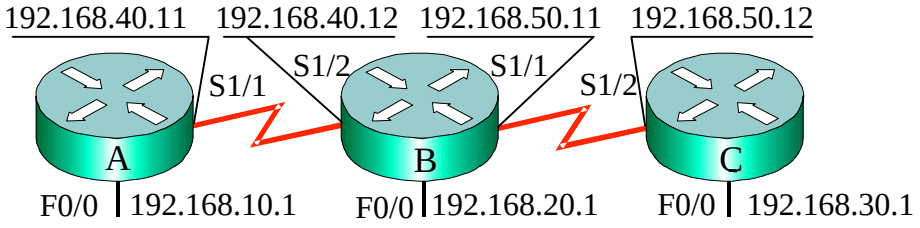
121. Для нижеприведенной схемы отметить три правильно заданных маршрута:




```
Router-A(config)#ip route 192.168.20.0 255.255.255.0 192.168.40.12
Router-A(config)#ip route 192.168.30.0 255.255.255.0 192.168.50.12
Router-B(config)#ip route 192.168.10.0 255.255.255.0 192.168.40.12
Router-B(config)#ip route 192.168.30.0 255.255.255.0 192.168.50.11
Router-C(config)#ip route 192.168.10.0 255.255.255.0 192.168.50.11
Router-C(config)#ip route 192.168.20.0 255.255.255.0 192.168.50.11
```

Вариант 2 Задачи 4.6

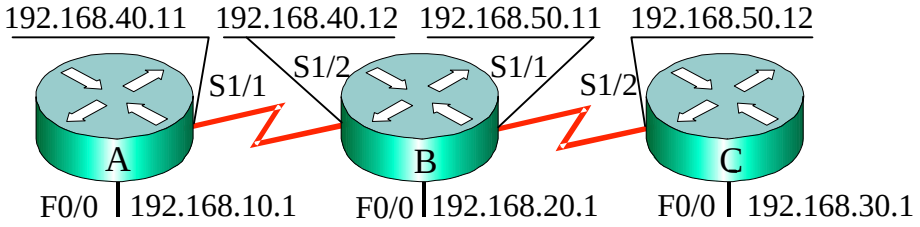
122. Для нижеприведенной схемы отметить вариант статической маршрутизации, при котором обеспечивается наиболее быстрая обработка пакета в маршрутизаторе:




```
Router-A(config)#ip route 192.168.20.0 255.255.255.0 S1/2
Router-A(config)#ip route 192.168.30.0 255.255.255.0 192.168.40.11
Router-B(config)#ip route 192.168.10.0 255.255.255.0 S1/1
Router-B(config)#ip route 192.168.30.0 255.255.255.0 192.168.50.12
Router-C(config)#ip route 192.168.10.0 255.255.255.0 S1/2
Router-C(config)#ip route 192.168.20.0 255.255.255.0 192.168.50.11
```

Вариант 3 Задачи 4.6

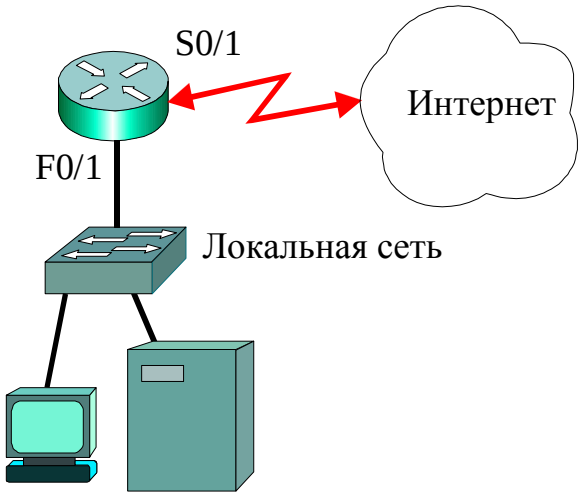
123. Для нижеприведенной схемы отметить два правильных варианта статической маршрутизации по умолчанию:




```
Router-A(config)#ip route 0.0.0.0 0.0.0.0 192.168.40.12
Router-A(config)#ip route 0.0.0.0 255.255.255.0 192.168.40.11
Router-B(config)#ip route 0.0.0.0 0.0.0.0 192.168.40.12
Router-C(config)#ip route 0.0.0.0 0.0.0.0 192.168.50.11
Router-C(config)#ip route 0.0.0.0 255.255.255.0 192.168.50.12
```

Задача 4.7
Вариант 1 Задачи 4.7

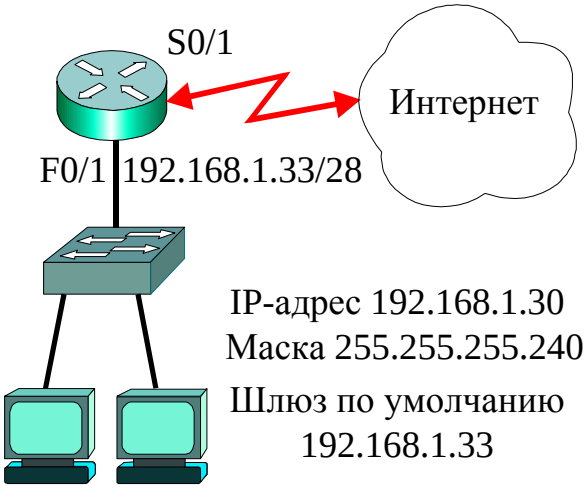
124. В нижеприведенной схеме локальная сеть 192.168.1.32/28 соединяется с Интернетом через интерфейс F0/1 маршрутизатора. Первый адрес локальной сети будет назначен интерфейсу F0/1, а последний – серверу. Необходимо отметить правильный вариант адресации сервера:



IP-адрес 192.168.1.31, маска 255.255.240.0, шлюз по умолчанию 192.169.10.33
IP-адрес 192.168.1.46, маска 255.255.240.0, шлюз по умолчанию 192.169.1.33
IP-адрес 192.168.1.33, маска 255.255.240.0, шлюз по умолчанию 192.169.1.46
IP-адрес 192.168.1.33, маска 255.255.248.0, шлюз по умолчанию 192.169.1.46
IP-адрес 192.168.1.46, маска 255.255.255.0, шлюз по умолчанию 192.169.1.47

Вариант 2 Задачи 4.7

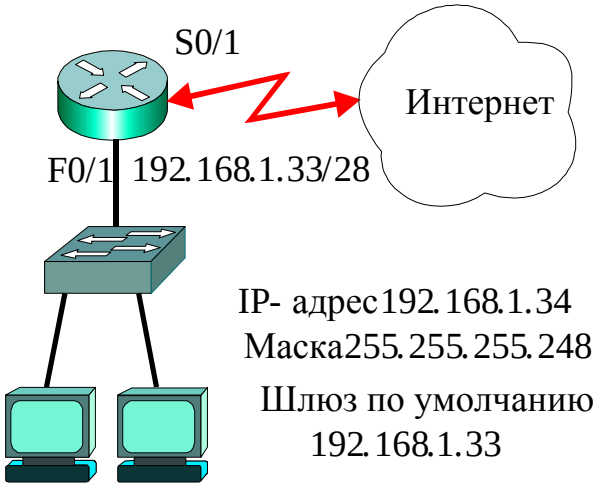
125. В нижеприведенной схеме локальной сети 192.168.1.32/28 конечный узел с адресом 192.168.1.30 не может соединяться с Интернетом, поскольку:



На конечном узле задана некорректная маска
Шлюз по умолчанию имеет адрес сети
Шлюз по умолчанию имеет широковещательный адрес
Шлюз по умолчанию и конечный узел находятся в разных подсетях

Вариант 3 Задачи 4.7

126. В нижеприведенной схеме локальной сети 192.168.1.32/28



конечный узел с адресом 192.168.1.34 не может соединяться с Интернетом, поскольку:

На конечном узле задана некорректная маска
Конечный узел не сконфигурирован для работы с подсетями
Шлюз по умолчанию имеет адрес сети
Шлюз по умолчанию и конечный узел находятся в разных подсетях

Задача 4.8
Вариант 1 Задачи 4.8

127. В строке таблицы маршрутизации

R 192.168.10.0/24 [120/2] via 200.60.60.11, 00:00:18, Serial1/2

цифра 2 в квадратных скобках означает:

До сети назначения имеется два пути
Маршрут создан протоколом RIP-2
Маршрут создан администратором
До сети назначения – два перехода
В маршрутизации используются входной и выходной интерфейс

Вариант 2 Задачи 4.8

128. В строке таблицы маршрутизации

R 192.168.10.0/24 [120/2] via 200.60.60.11, 00:00:18, Serial1/2

число 192.168.10.0/24 означает:

Адрес сети назначения
Адрес входного интерфейса маршрутизатора на пути к сети назначения
Адрес сети источника
Адрес выходного интерфейса маршрутизатора, с которого поступил пакет
Адрес шлюза по умолчанию (next hop)

Вариант 3 Задачи 4.8

129. В строке таблицы маршрутизации

R 192.168.10.0/24 [120/2] via 200.60.60.11, 00:00:18, Serial1/2

Serial1/2 означает:

Выходной интерфейс маршрутизатора на пути к сети назначения
Входной интерфейс соседнего маршрутизатора на пути к сети назначения
Входного интерфейса маршрутизатора, с которого поступил пакет
Шлюз по умолчанию (next hop)

Задача 4.9
Вариант 1 Задачи 4.9

130. Максимальное число переходов на пути к адресату назначения протокола RIP равно:

10, 15, 16, 24, 255

Вариант 2 Задачи 4.9

131. Пакет в маршрутизаторе уничтожается при значении метрики:

10, 15, 16, 24, 255

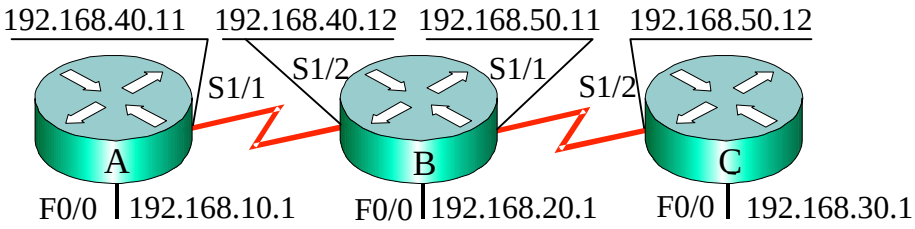
Вариант 3 Задачи 4.9

132. Обмен маршрутной информацией протокол RIP производит каждые:

5 секунд
10 секунд
30 секунд
90 секунд
180 секунд

Задача 4.10
Вариант 1 Задачи 4.10

133. Для нижеприведенной схемы отметить правильный вариант динамической маршрутизации:



1.
```
Router-A(config)#router rip
Router-A(config-router)#network 192.168.20.0
Router-A(config-router)#network 192.168.30.0
Router-A(config-router)#network 192.168.50.0
```

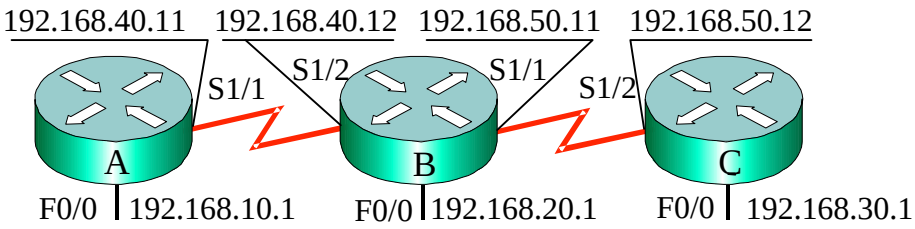
2. Router-A(config)#**router rip**
   Router-A(config-router)#**network 192.168.20.0**
   Router-A(config-router)#**network 192.168.30.0**

3. Router-A(config)#**router rip**
   Router-A(config-router)#**network 192.168.10.0**
   Router-A(config-router)#**network 192.168.40.0**

4. Router-A(config)#**router rip**
   Router-A(config)#**network 192.168.10.0**
   Router-A(config)#**network 192.168.20.0**
   Router-A(config)#**network 192.168.30.0**

Вариант 2 Задачи 4.10

134. Для нижеприведенной схемы отметить правильный вариант динамической маршрутизации:



1. Router-B(config)#**router rip**
   Router-B(config-router)#**network 192.168.20.0**
   Router-B(config-router)#**network 192.168.40.0**
   Router-B(config-router)#**network 192.168.50.0**

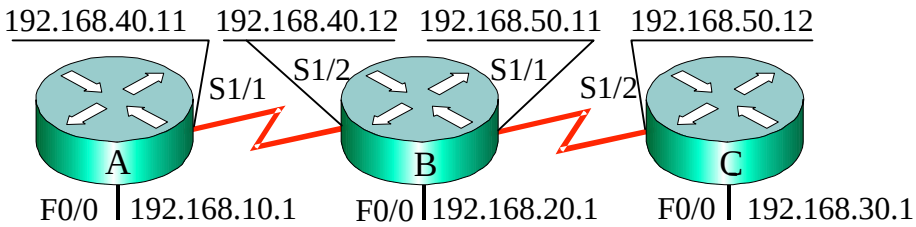
2. Router-B(config)#**router rip**
   Router-B(config-router)#**network 192.168.10.0**
   Router-B(config-router)#**network 192.168.30.0**

3. Router-B(config)#**router rip**
   Router-B(config)#**network 192.168.10.0**
   Router-B(config)#**network 192.168.30.0**

4. Router-B(config)#**router rip**
   Router-B(config-router)#**network 192.168.10.0**
   Router-B(config-router)#**network 192.168.20.0**
   Router-B(config-router)#**network 192.168.30.0**

Вариант 3 Задачи 4.10

135. Для нижеприведенной схемы отметить правильный вариант динамической маршрутизации:



1. Router-C(config)#**router rip**
   Router-C(config-router)#**network 192.168.20.0**
   Router-C(config-router)#**network 192.168.30.0**
   Router-C(config-router)#**network 192.168.50.0**

2. Router-C(config)#**router rip**
   Router-C(config-router)#**network 192.168.30.0**
   Router-C(config-router)#**network 192.168.50.0**

3. Router-C(config)#**router rip**
   Router-C(config-router)#**network 192.168.10.0**
   Router-C(config-router)#**network 192.168.20.0**
   Router-C(config-router)#**network 192.168.40.0**

4. Router-C(config)#**router rip**
   Router-C(config)#**network 192.168.10.0**
   Router-C(config)#**network 192.168.20.0**

Раздел 5. ОСОБЕННОСТИ КОНФИГУРИРОВАНИЯ МАРШРУТИЗАТОРОВ

Лекция 11. ОСОБЕННОСТИ ПРОТОКОЛОВ ВЕКТОРА РАССТОЯНИЯ

Краткая аннотация лекции: Рассмотрены особенности функционирования протокола маршрутизации RIP в не корректно спроектированной сети. Приведены общие сведения о протоколе EIGRP и его конфигурировании. Даны примеры отладки сети.
Цель лекции: изучить особенности функционирования протоколов вектора расстояния.

11.1. Протокол RIP

Протокол Routing Information Protocol (RIP) широко используется в сетях малого размера, где на пути от источника до назначения максимальное число переходов между маршрутизаторами не превышает 15. Однако в случае не корректно спроектированной сети применение протокола RIP может привести к проблемам маршрутизации. Примером не корректно спроектированной сети является схема рис.11.1 с таблицей адресов 11.1.

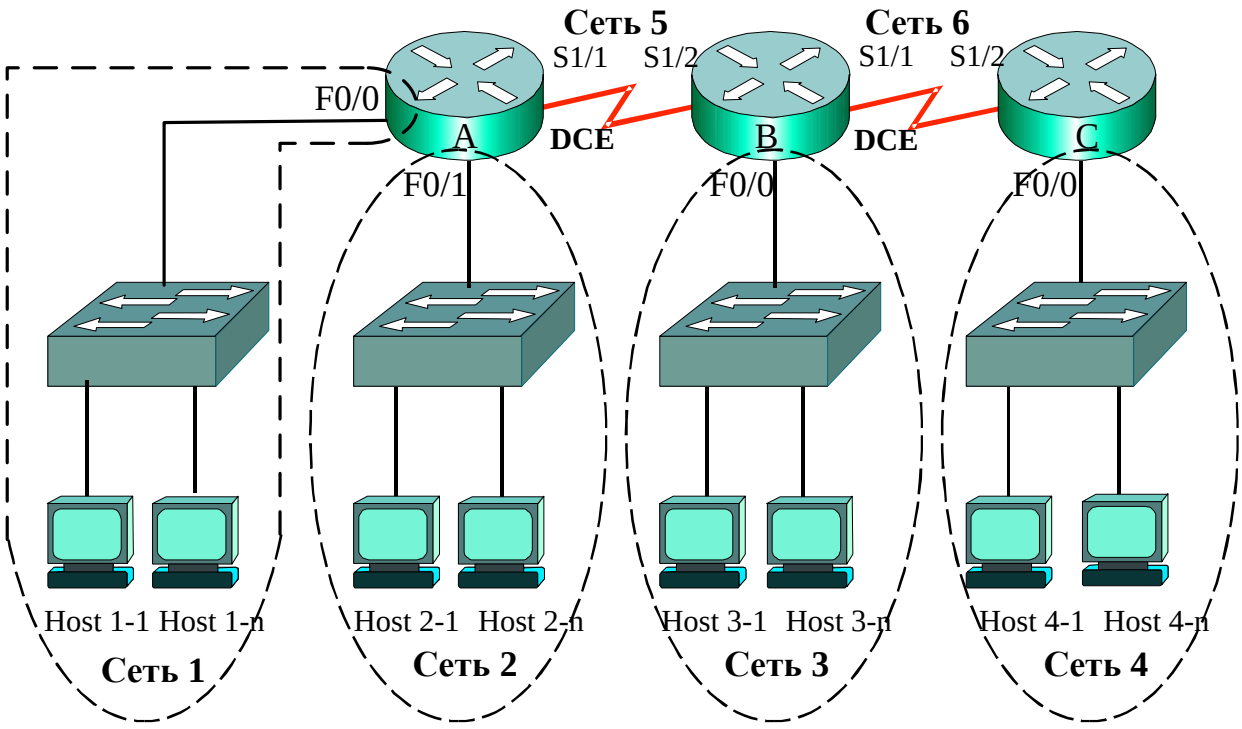


Рис.11.1. Пример составной сети

Из рис.11.1 и табл.11.1 следует, что Сеть 1 (192.168.10.16/28), Сеть 2 (192.168.10.32/27) и Сеть 4 (192.168.10.128/26) являются подсетями сети 192.168.10.0/24. Причем, Сети 1, 2 и Сеть 4 разделены Сетью 5 и Сетью 6.

Таблица 11.1

Адреса сетей, интерфейсов и узлов составной сети

Наименование	Адрес	Наименование	Адрес
Сеть 1 f0/0 Host 1-1 Host 1-*n*	192.168.10.16/28 192.168.10.17 192.168.10.18 192.168.10.*n*	Сеть 2 f0/0 Host 2-1 Host 2-*n*	192.168.10.32/27 192.168.10.33 192.168.10.34 192.168.10.*n*
Сеть 3 f0/0 Host 3-1 Host 3-*n*	192.168.20.64/29 192.168.20.65 192.168.20.66 192.168.20.*n*	Сеть 4 f0/0 Host 4-1 Host 4-*n*	192.168.10.128/26 192.168.10.129 192.168.10.130 192.168.10.*n*
Сеть 5 s1/1 s1/2	200.5.5.0/30 200.5.5.1 200.5.5.2	Сеть 6 s1/1 s1/2	200.5.5.4/30 200.5.5.5 200.5.5.6

Конфигурирование маршрутизаторов (адресов интерфейсов и протокола RIP) проведено в соответствие с материалами Лекций 9, 10:

```
R_A(config)#router rip
R_A(config-router)#network 192.168.10.16
R_A(config-router)#network 192.168.10.32
R_A(config-router)#network 200.5.5.0 ,
```

Ниже приведены результаты конфигурирования маршрутизатора А с использованием команд **sh run** и **sh ip route**:

```
R-A#sh run
...
interface FastEthernet0/0
 ip address 192.168.10.17 255.255.255.240
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 192.168.10.33 255.255.255.224
 duplex auto
 speed auto
!
interface Serial1/1
 ip address 200.5.5.1 255.255.255.252
 clock rate 64000
!
router rip
network 192.168.10.0
 network 200.5.5.0
```

```
R-A#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.10.16/28 is directly connected, FastEthernet0/0
C       192.168.10.32/27 is directly connected, FastEthernet0/1
R    192.168.20.0/24 [120/1] via 200.5.5.2, 00:00:05, Serial1/1
     200.5.5.0/30 is subnetted, 2 subnets
C       200.5.5.0 is directly connected, Serial1/1
R       200.5.5.4 [120/1] via 200.5.5.2, 00:00:05, Serial1/1
```

Поскольку RIP относится к протоколам типа **classfull**, то он объединяет отдельные подсети в рамках сети заданного класса, в данном случае сети класса С, что можно увидеть из распечатки команды **show running-config**. Две подсети (192.168.10.16 и 192.168.10.32), которые были заданы при конфигурировании, протокол RIP объединил в сеть класса С (`network 192.168.10.0`).

Из распечатки команды **sh ip route** следует, что сеть 192.168.10.0 с маской 255.255.255.0 разделена на две непосредственно присоединенных подсети с масками разной длины: 192.168.10.16/28 и 192.168.10.32/27. При этом сеть класса С 192.168.10.0/24 называется **родительской**, а сети 192.168.10.16/28 и 192.168.10.32/27 – **дочерними.**

Кроме того, в таблице маршрутизации R_A отсутствует маршрут к сети 192.168.10.128/26, поскольку протокол RIP в своих обновлениях не передает маску подсети, поэтому подсети объединены в рамках сети 192.168.10.0/24. Из-за отсутствия в таблице маршрутизации R_A маршрута к сети 192.168.10.128/26 «пингование» интерфейса 192.168.10.129 – неудачное:

```
R-A>ping 192.168.10.129

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.129, timeout is 2
seconds:
.....
Success rate is 0 percent (0/5)
```

Конфигурирование маршрутизатора B дало следующие результаты:

```
R-B#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
...

Gateway of last resort is not set

R    192.168.10.0/24 [120/1] via 200.5.5.1, 00:00:15, Serial1/2
                     [120/1] via 200.5.5.6, 00:00:02, Serial1/1
     192.168.20.0/29 is subnetted, 1 subnets
C       192.168.20.64 is directly connected, FastEthernet0/0
     200.5.5.0/30 is subnetted, 2 subnets
C       200.5.5.0 is directly connected, Serial1/2
C       200.5.5.4 is directly connected, Serial1/1
```

Из распечатки команды **show running-config** следует, что протокол RIP объединил две подсети 200.5.5.0/30 и 200.5.5.4/30 в сеть `network 200.5.5.0`. Кроме того, и это очень важно, в таблице маршрутизации R_B имеется два маршрута к сети 192.168.10.0/24, причем, один путь направлен влево через интерфейс 200.5.5.1, а другой вправо через 200.5.5.6. Поскольку оба пути характеризуются одинаковой метрикой, равной 1, то протокол RIP использует **баланс маршрутов** и поочередно посылает пакеты через два разных интерфейса (next hop). Поэтому один пакет доходит до адресата, а второй – нет, что видно из следующей команды:

```
R_B#ping 192.168.10.17

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.17, timeout is 2
seconds:
!U!.!
Success rate is 60 percent (3/5), round-trip min/avg/max = 34/59/59 ms
```

Пакеты эхо запроса поочередно попадают, то к адресату назначения (ответ !), то направляются в другую сторону, где устройство назначения недоступно (U) или время ожидания превышает допустимое (.).

В таблице маршрутизации R_C отсутствует маршрут к подсетям 192.168.10.16/28 и 192.168.10.32/27, поскольку они объединены с подсетью 192.168.10.128 в рамках одной родительской сети 192.168.10.0:

```
R_C#sh ip route
...

     192.168.10.0/26 is subnetted, 1 subnets
C       192.168.10.128 is directly connected, FastEthernet0/0
R    192.168.20.0/24 [120/1] via 200.5.5.5, 00:00:03, Serial1/2
     200.5.5.0/30 is subnetted, 2 subnets
R       200.5.5.0 [120/1] via 200.5.5.5, 00:00:03, Serial1/2
C       200.5.5.4 is directly connected, Serial1/2
```

Таким образом, в неправильно спроектированной сети (рис. 11.1) подсети 192.168.10.16/28, 192.168.10.32/27 и 192.168.10.128/26 разделены (или, по-другому, разобщены) сетями 200.5.5.0/30 и 200.5.5.4/30. При использовании протокола RIP в такой сети ее работоспособность нарушена. Это происходит из-за того, что протокол RIP в своих **обновлениях** (**update**) маршрутной информацией не передает значения маски подсетей.

Протокол RIP-2

Основным недостатком протокола первой версии RIPv1 является то, что в обновлениях не передается значение маски, поэтому протокол RIPv1 не поддерживает бесклассовую междоменную маршрутизацию CIDR и маски переменной длины VLSM. От этого недостатка свободен **протокол** второй версии **RIPv2**, который **в своих сообщениях update дополнительно к адресу сети назначения передает значение маски** и **адрес следующего перехода** (next-hop). При этом используется значение маски интерфейса, к которому присоединена сеть, поэтому маска при конфигурировании не задается. Обмен маршрутной информацией происходит с использованием сегментов UDP (адрес порта 250). Сегмент может содержать до 25 маршрутов. Остальные параметры RIPv2 такие же, как у протокола RIPv1.

При конфигурировании RIPv2 на маршрутизаторах A, B, C (рис. 11.1, табл. 11.1) необходимо дополнительно указать, что используется протокол версии 2. Например, при конфигурировании маршрутизатора A:

```
R_A(config)#router rip
R_A(config-router)#version 2
R_A(config-router)#network 192.168.10.16
R_A(config-router)#network 192.168.10.32
R_A(config-router)#network 200.5.5.0
```

Кроме того, для того чтобы не корректно спроектированная сеть (рис. 11.1) функционировала, необходимо отменить автоматическое суммирование сетей. Автоматическое суммирование дает возможность сократить число входов (строк) таблицы маршрутизации, что ускоряет процесс обработки адресов назначения маршрутизатором. При этом вместо адресов нескольких подсетей будет задан один агрегированный (объединенных) адрес. Однако в случае не корректно спроектированной сети (рис. 11.1) подсети 192.168.10.16/28, 192.168.10.32/27 и 192.168.10.128/26 будут объединены в рамках адреса 192.168.10.0/24, поэтому работоспособность сети будет нарушена, также как в случае функционирования протокола RIPv1.

Для нормального функционирования сети (рис. 11.1) достаточно отменить режим автосуммирования на всех маршрутизаторах:

```
R_A(config)#router rip
R_A(config-router)#version 2
R_A(config-router)#no auto-summary
```

После этого все узлы и интерфейсы должны иметь связь между собой, что проверяется по командам ping, tracert, traceroute.

11.2. Общие сведения о протоколе EIGRP

В настоящее время дистанционно-векторный маршрутизирующий протокол Interior Gateway Routing Protocol (IGRP) заменен улучшенной (расширенной) версией **Enhanced IGRP**. Оба протокола являются разработкой фирмы Cisco и предназначены для работы с аппаратурой Cisco. Административное расстояние EIGRP равно 90 (см. табл. 11.2). Протокол EIGRP используется внутри автономных систем (АС), в которых группы маршрутизаторов разделяют маршрутную информацию (см. рис. 9.1).

Автономные системы объединяют сети под общим административным управлением. Поскольку все маршрутизаторы в АС должны совместно использовать маршрутную информацию, то у них конфигурируется одинаковый **номер автономной системы**.

При формировании маршрутов протокол EIGRP использует специально разработанный для этих целей **алгоритм** Diffusing Update Algorithm (**DUAL**). Согласно алгоритма DUAL протокол EIGRP не проводит периодический обмен объемными обновлениями (update) маршрутной информации, а

использует небольшие **пакеты Hello** для контроля связи с соседними маршрутизаторами. Обмен маршрутной информацией производится только при возникновении изменений в сети (появление новых связей, недоступных узлов и сетей, изменение метрики). Причем, производится обмен **неполной** (partial) маршрутной информацией, касающейся только изменений в сети, и с **ограниченным** (bounded) числом тех маршрутизаторов, которые затрагивают эти изменения. Кроме того, алгоритм DUAL не использует таймеры удержания информации holddown (см. раздел 9.3), как это делает алгоритм Беллмана-Форда протокола RIP. Поэтому **сходимость** (convergence) сетей EIGRP более быстрая.

Протоколы маршрутизации используют метрику, чтобы определить кратчайший маршрут к устройству назначения. Значение метрики определяет желательность маршрута. **Метрика протокола EIGRP** учитывает целый ряд параметров. Алгоритм DUAL протокола рассчитывает значение метрики для каждого пути через сеть. Меньшее число указывает лучший маршрут. **Полоса пропускания** и **задержка** являются статическими параметрами, они остаются неизменными для каждого интерфейса, пока не будет перестроена сеть или реконфигурирован маршрутизатор. Параметры **загрузка** (load) и **надежность (**reliability**)** являются динамическими, они могут рассчитываться маршрутизатором для каждого интерфейса в реальном времени.

Чем больше факторов, которые составляют метрику, тем больше гибкость, чтобы учитывать особенности сети. По умолчанию, протокол **EIGRP использует статические параметры полосы пропускания и задержки**, чтобы вычислить значение метрики. Но при вычислении метрики могут также использоваться динамические факторы загрузки и надежности, т.е маршрутизатор может принять решение, основанное на текущем состоянии сети. Если соединение становится сильно загруженным или ненадежным, метрика увеличится. При этом может использоваться запасной маршрут.

Для вычисления метрики M протоколов IGRP, EIGRP используется следующая формула:

$$M = [k1 * Bandwidth + (k2 * Bandwidth)/(256-load) + k3*Delay] * [k5/(reliability + k4)],$$

где * – обобщенный оператор,

k – коэффициенты, которые могут принимать значения 0 или 1.

По умолчанию коэффициенты k1 = k3 = 1 и k2 = k4 = k5 = 0, при этом метрика EIGRP вычисляется следующим образом:

Метрика = (10 000 000/ Bandwidth + Σ delay/10) ·256

При вычислении значения метрики **полоса пропускания** задается в **кбит/с**, а **суммарная задержка** – в **мкс**. **Задержка** определяется **типом выходного интерфейса** маршрутизатора и технологией среды передачи данных. Задержка интерфейсов FastEthernet равна 100 мкс, Ethernet – 1000 мкс, интерфейсов первичных потоков E1, T1 – 20 000 мкс. Задержка интерфейсов ОЦК (64 кбит/с) также составляет 20 000 мкс.

***Метрика сети, состоящей из нескольких соединений, определяется полосой пропускания самого «медленного» соединения и суммарной задержкой всех выходных интерфейсов маршрутизаторов*.**

Например, если сообщение передается с узла локальной сети через интерфейс FastEthernet маршрутизатора и далее через последовательный интерфейс, предназначенный для передачи первичного цифрового потока с полосой пропускания 2048 кбит/с, то метрика будет равна:

$10^7 \cdot 256 / 2048 + (20\,000 + 100) \cdot 256/10 = 125 \cdot 10^4 + 514560 =$ **1 764 560.**

Метрика соединения со скоростью передачи 64 кбит/с будет равна $\mathbf{40 \cdot 10^6}$, а при скорости 128 кбит/с метрика – $\mathbf{20 \cdot 10^6}$. По умолчанию на соединениях задана либо скорость 128 кбит/с, либо скорость E1 или T1.

Значения коэффициентов k1, k2, k3, k4, k5 можно изменить по команде:

```
Router(confi-router)#metric weights tos k1 k2 k3 k4 k5
```

Значения k1, k2, k3, k4, k5 передается в пакете протокола EIGRP.

Заголовок пакета EIGRP располагается следом за заголовком IP-пакета и содержит код типа пакета, номер автономной системы. В самом EIGRP-пакете содержится информация о значениях коэффициентов k1, k2, k3, k4, k5, задержки, ширины полосы пропускания, надежности, загрузки, префиксе, т.е. о маске переменной длины и другая информация.

Особенностью протокола EIGRP является использование собственного **протокола надежной доставки** (Reliable Transport Protocol – **RTP**) транспортного уровня, поскольку EIGRP взаимодействует не только с IP-

протоколом, но и с протоколами IPX, Apple-Talk, которые не поддерживают TCP и UDP. Протокол надежной доставки RTP может работать с подтверждением доставки (reliable) и без подтверждения (unreliable).

Для обмена информацией между маршрутизаторами протокол EIGRP использует пять типов пакетов:

1. Hello
2. Update
3. Acknowledgment
4. Query
5. Replay

Hello-пакеты используются, чтобы поддерживать **отношения смежности** (adjacency) между соседними устройствами. Они передаются периодически с использованием многоадресного режима (адрес 224.0.0.10) и без подтверждения доставки. В большинстве случаев период рассылки Hello-пакетов составляет 5 сек. Если в течение утроенного периода времени рассылки Hello-пакет не будут получены, то это будет означать, что связь с устройством потеряна. Результатом обмена Hello-пакетами является построение таблицы соседних устройств (Neighbor Table). **Таблицу соседних устройств**, например, маршрутизатора R_B (рис.11.1) можно посмотреть по команде:

```
R_B#show ip eigrp neighbors
IP-EIGRP neighbors for process 1
H   Address      Interface      Hold Uptime    SRTT   RTO   Q   Seq
                                     (sec)      (ms)        Cnt  Num
0   200.5.5.1    Ser1/2          10   00:01:09  40     500   0   12
1   200.5.5.6    Ser1/1          11   00:01:09  40     500   0   17
```

В таблице указаны адреса входных интерфейсов соседних маршрутизаторов (Address), типы собственных выходных интерфейсов (Interface), значение текущего времени (Holdtime) и другая информация.

Второй тип **пакетов Update** рассылается не периодически, а только по мере возникновения изменений в сети. Пакеты могут рассылаться в одноадресном (unicast) или многоадресном (multiicast) режиме. Рассылка пакетов Update проводится с *подтверждением доставки* (Acknowledgment),

сами пакеты подтверждения Acknowledgment рассылаются в одноадресном режиме без подтверждения доставки.

Пакеты **Query** и **Replay** используются алгоритмом DUAL для начального создания топологии сети и при ее изменениях. При этом всегда применяется надежная доставка. Пакеты Query могут рассылаться в одноадресном или многоадресном режимах, Replay – всегда в одноадресном.

Для эффективного функционирования помимо **таблицы соседних устройств** (Neighbor Table) протокол EIGRP строит и поддерживает **таблицу топологии** сети (Topology Table) и **таблицу маршрутизации** (Routing Table). *При любых изменениях топологии*, которые фиксируются в таблицах соседних устройств и топологии сети, *алгоритм DUAL либо включает в таблицу маршрутизации запасные маршруты из таблицы топологии, либо вычисляет новые маршруты и затем включает их в таблицу маршрутизации*. Алгоритм DUAL обеспечивает вычисление **маршрутов свободных от маршрутных петель** (loop-free).

11.3. Конфигурирование протокола EIGRP

Составная сеть (рис.12.1) может быть интерпретирована, как автономная система, например, номер 30. Адреса сетей, интерфейсов и узлов составной сети приведены в табл. 11.1. При адресации типа classless в сетях EIGRP можно адресовать подсети с использованием масок переменной длины, поскольку протокол EIGRP передает значение масок в своих пакетах Update. Причем используется **маска переменной длины типа wildcard-mask.** Подобная маска получается путем инвертирования обычной маски подсети. Если при конфигурировании ввести обычную маску, то операционная система IOS исправит маску на инвертированную, например, маску 255.255.255.240 операционная система исправит на 0.0.0.15.

Ниже приведен пример конфигурирования на маршрутизаторах A, B, C протокола EIGRP. Маршрутизация протокола EIGRP производится командой **router eigrp 30** в режиме глобального конфигурирования с указанием номера автономной системы (в данном примере 30). После перехода маршрутизатора в режим детального конфигурирования вводятся адреса непосредственно присоединенных сетей с указанием инвертированной маски.

Маршрутизатор R_A:

```
R_A(config)#router eigrp 30
R_A(config-router)#network 192.168.10.16 0.0.0.15
R_A(config-router)#network 192.168.10.32 0.0.0.31
R_A(config-router)#network 200.5.5.0 0.0.0.3
```

Маршрутизатор R_B:

```
R_B(config)#router eigrp 30
R_B(config-router)#network 192.168.20.64 0.0.0.7
R_B(config-router)#network 200.5.5.0 0.0.0.3
R_B(config-router)#network 200.5.5.4 0.0.0.3
```

Маршрутизатор R_C:

```
R_C(config)#router eigrp 30
R_C(config-router)#network 192.168.10.128 0.0.0.63
R_C(config-router)#network 200.5.5.4 0.0.0.3
```

Результат маршрутизации можно посмотреть по команде **sh ip route**. Ниже приведены распечатки таблиц маршрутизации всех маршрутизаторов. Маршруты, созданные протоколом EIGRP, помечены символом D.

Таблица маршрутизации R_A:

```
R_A#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
  D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
  N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
  E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
  i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
        * - candidate default, U - per-user static route, o - ODR
        P - periodic downloaded static route

Gateway of last resort is not set

     192.168.10.0/24 is variably subnetted, 3 subnets, 3 masks
D       192.168.10.0/24 is a summary, 00:02:05, Null0
C       192.168.10.16/28 is directly connected, FastEthernet0/0
C       192.168.10.32/27 is directly connected, FastEthernet0/1
D    192.168.20.0/24 [90/20514560] via 200.5.5.2, 00:01:05, Serial1/1
     200.5.5.0/24 is variably subnetted, 3 subnets, 2 masks
D       200.5.5.0/24 is a summary, 00:01:27, Null0
C       200.5.5.0/30 is directly connected, Serial1/1
D       200.5.5.4/30 [90/21024000] via 200.5.5.2, 00:01:27, Serial1/1
R_A#
```

Из таблицы следует, что путь в сеть 192.168.10.128/26 отсутствует, поскольку он входит в суммарный маршрут 192.168.10.0/24. Протокол EIGRP автоматически формирует суммарные маршруты, которые в таблицах отмечены интерфейсом Null0, что показывает вторая строка таблицы маршрутизации. **Пакеты, поступающие на интерфейс Null0, уничтожаются**. То есть, пакет адресованный подсети 192.168.10.128/26 при поступлении в маршрутизатор R_A будет уничтожен!

То, что в протоколе RIP **называлось адресом следующего перехода** (next hop) или шлюзом, в терминах протокола EIGRP **называется преемником** (successor). Например, для маршрута к сети 192.168.20.0/24 (строка 5 таблицы) преемником будет интерфейс 200.5.5.2 маршрутизатора R_B. Административное расстояние EIGRP равно 90, а метрика составляет 20514560, выходным интерфейсом маршрутизатора R_A является Serial1/1.

Таблица маршрутизации R_B:

```
R_B#sh ip route
...

Gateway of last resort is not set

D   192.168.10.0/24 [90/20514560] via 200.5.5.1, 00:01:45, Serial1/2
                    [90/20514560] via 200.5.5.6, 00:00:23, Serial1/1
    192.168.20.0/24 is variably subnetted, 2 subnets, 2 masks
D       192.168.20.0/24 is a summary, 00:01:18, Null0
C       192.168.20.64/29 is directly connected, FastEthernet0/0
     200.5.5.0/24 is variably subnetted, 3 subnets, 2 masks
D       200.5.5.0/24 is a summary, 00:00:43, Null0
C       200.5.5.0/30 is directly connected, Serial1/2
C       200.5.5.4/30 is directly connected, Serial1/1
```

Из анализа таблицы маршрутизации R_B следует, что путь в объединенную сеть 192.168.10.0/24 может быть как влево через 200.5.5.1, так и вправо через 200.5.5.6, т.е. ситуация аналогична протоколу RIP.

Таблица маршрутизации Router_C:

```
R_C#sh ip route
...

Gateway of last resort is not set

    192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
D      192.168.10.0/24 is a summary, 00:00:11, Null0
C      192.168.10.128/26 is directly connected, FastEthernet0/0
D   192.168.20.0/24 [90/20514560] via 200.5.5.5, 00:00:07, Serial1/2
```

```
    200.5.5.0/24 is variably subnetted, 3 subnets, 2 masks
D      200.5.5.0/24 is a summary, 00:00:07, Null0
D      200.5.5.0/30 [90/21024000] via 200.5.5.5, 00:00:07, Serial1/2
C      200.5.5.4/30 is directly connected, Serial1/2
```

Из таблицы маршрутизации R_C следует, что маршрут к сетям 192.168.10.16/28 и 192.168.10.32/27 отсутствует, вследствие того что протокол EIGRP автоматически суммировал маршруты и использовал выходной интерфейс Null0. Функцию автоматического суммирования маршрутов (auto-summary) можно видеть по команде **show running-config**. Например, для маршрутизатора R_B:

```
R_B#sh run
Building configuration...
...
!
router eigrp 30
 network 192.168.20.64 0.0.0.7
 network 200.5.5.0 0.0.0.3
 network 200.5.5.4 0.0.0.3
 auto-summary
!
...
```

Чтобы протокол EIGRP мог обеспечить маршрутизацию в сети (рис.12.1), необходимо *отменить авто-суммирование маршрутов на всех маршрутизаторах*. Например, на маршрутизаторе R_B отмена авто-суммирования производится по следующей команде:

```
R_B(config)#router eigrp 30
R_B(config-router)#no auto-summary
```

Проверка подтверждает отмену авто-суммирования:

```
R_B#sh run
Building configuration...
...
!
router eigrp 30
 network 192.168.20.64 0.0.0.7
 network 200.5.5.0 0.0.0.3
 network 200.5.5.4 0.0.0.3
 no auto-summary
!
...
```

Отмена авто-суммирования приводит к увеличению количества строк в таблице маршрутизации. Так в таблице R_A вместо имевшихся ранее четырех строк пути к удаленным сетям (входы помеченные символом D), теперь имеется шесть строк, что повышает нагрузку на процессор при обработке маршрутов. Однако пятая строка таблицы теперь содержит маршрут к подсети 192.168.10.128/26, которого ранее не было, что можно видеть из распечатки команд **sh ip route**:

```
R_A#sh ip route
...
Gateway of last resort is not set

  192.168.10.0/24 is variably subnetted, 4 subnets, 4 masks
D  192.168.10.0/24 is a summary, 00:05:09, Null0
C  192.168.10.16/28 is directly connected, FastEthernet0/0
C  192.168.10.32/27 is directly connected, FastEthernet0/1
D  192.168.10.128/26 [90/21026560] via 200.5.5.2, 00:00:14, Serial1/1
 192.168.20.0/24 is variably subnetted, 2 subnets, 2 masks
D  192.168.20.0/24 [90/20514560] via 200.5.5.2, 00:00:32, Serial1/1
D  192.168.20.64/29 [90/20514560] via 200.5.5.2, 00:00:32, Serial1/1
  200.5.5.0/24 is variably subnetted, 3 subnets, 2 masks
D  200.5.5.0/24 is a summary, 00:04:23, Null0
C  200.5.5.0/30 is directly connected, Serial1/1
D  200.5.5.4/30 [90/21024000] via 200.5.5.2, 00:00:32, Serial1/1
```

Аналогичная ситуация и в маршрутизаторе R_B. Если раньше путь в объединенную сеть 192.168.10.0/24 мог быть как влево через 200.5.5.1, так и вправо через 200.5.5.6, то после отмены авто-суммирования, путь к подсетям 192.168.10.16/28 и 192.168.10.32/27 лежит влево через интерфейс 200.5.5.1, а к подсети 192.168.10.128/26 – вправо, через 200.5.5.6:

```
R_B#sh ip route
...
Gateway of last resort is not set

  192.168.10.0/24 is variably subnetted, 4 subnets, 4 masks
D  192.168.10.0/24 is a summary, 00:01:44, Null0
D  192.168.10.16/28 [90/20514560] via 200.5.5.1, 00:01:30, Serial1/2
D  192.168.10.32/27 [90/20514560] via 200.5.5.1, 00:01:30, Serial1/2
```

```
D  192.168.10.128/26 [90/20514560] via 200.5.5.6, 00:01:13, Serial1/1
  192.168.20.0/24 is variably subnetted, 2 subnets, 2 masks
D  192.168.20.0/24 is a summary, 00:05:27, Null0
C  192.168.20.64/29 is directly connected, FastEthernet0/0
  200.5.5.0/24 is variably subnetted, 3 subnets, 2 masks
D  200.5.5.0/24 is a summary, 00:01:43, Null0
C  200.5.5.0/30 is directly connected, Serial1/2
C  200.5.5.4/30 is directly connected, Serial1/1
```

В маршрутизаторе R_C появились пути к подсетям 192.168.10.16/28 и 192.168.10.32/27:

```
R_C#sh ip route
...
  192.168.10.0/24 is variably subnetted, 4 subnets, 4 masks
D  192.168.10.0/24 is a summary, 00:02:18, Null0
D  192.168.10.16/28 [90/21026560] via 200.5.5.5, 00:02:02, Serial1/2
D  192.168.10.32/27 [90/21026560] via 200.5.5.5, 00:02:02, Serial1/2
C  192.168.10.128/26 is directly connected, FastEthernet0/0
  192.168.20.0/24 is variably subnetted, 2 subnets, 2 masks
D  192.168.20.0/24 is a summary, 00:02:18, Null0
D  192.168.20.64/29 [90/20514560] via 200.5.5.5, 00:02:02, Serial1/2
  200.5.5.0/24 is variably subnetted, 3 subnets, 2 masks
D  200.5.5.0/24 is a summary, 00:02:18, Null0
D  200.5.5.0/30 [90/21024000] via 200.5.5.5, 00:02:02, Serial1/2
C  200.5.5.4/30 is directly connected, Serial1/2
```

С изменением топологии сети (рис. 11.2) меняются и таблицы маршрутизации. Интерфейс s1/0 – имеет адрес 200.5.5.9, s1/3 – адрес 200.5.5.10. Изменения в сети отображаются в таблицах топологии (Topology Table) и соседних устройств (neighbors). На основании этих изменений алгоритм DUAL обеспечивает вычисление свободных от маршрутных петель путей и затем формируется новая таблица маршрутизации. При добавлении в схему рис.11.1 нового соединения между R_A и R_B (рис. 11.2), путь из R_A в сеть 192.168.10.128/26 будет проложен через 200.5.5.10, поскольку на этом пути меньше последовательных выходных интерфейсов (s1/0) и метрика равна 20514560.

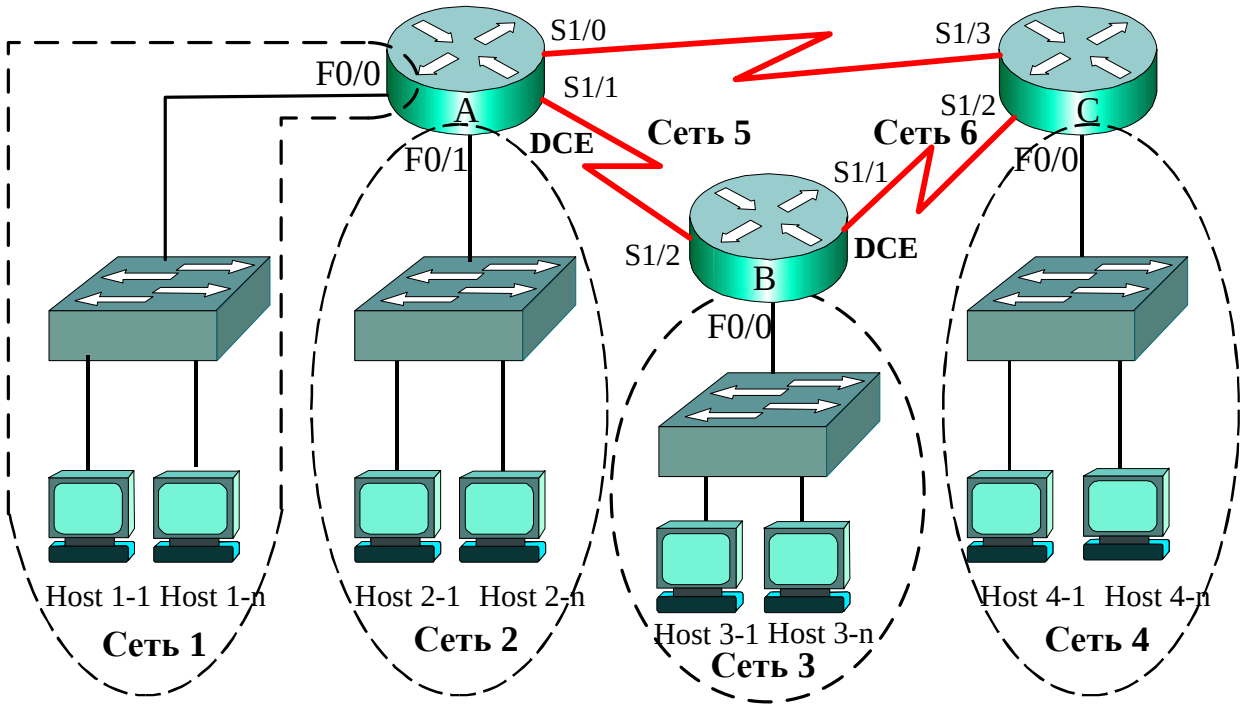


Рис. 11.2. Пример составной сети

Прежний маршрут через 200.5.5.2 характеризовался метрикой 21026560, т.к. включал выходные интерфейсы s1/1 сети 200.5.5.0/30 и s1/1 сети 200.5.5.4/30. Суммарная задержка последовательного и Fast Ethernet интерфейсов характеризуется метрикой (20000/10 + 100/10)*256 = 514560. Суммарная задержка двух последовательных интерфейсов и Fast Ethernet интерфейса составит значение метрики 1026560. Изменения отображают распечатки команд **sh ip route**. Следует учесть, что по умолчанию метрика вычисляется для полосы пропускания 128 кбит/с и составляет $(10^7/128)256 = 20000000$. Причем, 128 кбит/с задается по умолчанию, несмотря на то, что по команде **clock rate** была задана скорость 64000 бит/с.

```
R_A#sh ip route
...
Gateway of last resort is not set

 192.168.10.0/24 is variably subnetted, 4 subnets, 4 masks
D  192.168.10.0/24 is a summary, 00:26:55, Null0
C  192.168.10.16/28 is directly connected, FastEthernet0/0
C  192.168.10.32/27 is directly connected, FastEthernet0/1
D  192.168.10.128/26 [90/20514560] via 200.5.5.10, 00:00:58, Serial1/0
 192.168.20.0/24 is variably subnetted, 2 subnets, 2 masks
```

```
D   192.168.20.0/24 [90/20514560] via 200.5.5.2, 00:22:17, Serial1/1
D   192.168.20.64/29 [90/20514560] via 200.5.5.2, 00:22:17, Serial1/1
  200.5.5.0/24 is variably subnetted, 3 subnets, 2 masks
D   200.5.5.0/24 is a summary, 00:26:09, Null0
C   200.5.5.0/30 is directly connected, Serial1/1
C   200.5.5.8/30 is directly connected, Serial1/0
```

Изменение расчетной скорости или полосы пропускания соединения, например, до 64 кбит/с, производится по команде:

```
Router(config)#int s1/0
Router(config-if)#bandwidth 64
```

Если изменить полосу пропускания соединения между R_A и R_B (рис. 12.2) до 64 кбит/с, оставив остальные соединения без изменений, то путь из R_A в сеть 192.168.10.128/26 будет проложен через 200.5.5.2:

```
R_A#sh ip route
...
Gateway of last resort is not set

  192.168.10.0/24 is variably subnetted, 4 subnets, 4 masks
D  192.168.10.0/24 is a summary, 00:50:25, Null0
C  192.168.10.16/28 is directly connected, FastEthernet0/0
C  192.168.10.32/27 is directly connected, FastEthernet0/1
D  192.168.10.128/26 [90/21026560] via 200.5.5.2, 00:11:19, Serial1/1
  192.168.20.0/24 is variably subnetted, 2 subnets, 2 masks
D   192.168.20.0/24 [90/20514560] via 200.5.5.2, 00:45:47, Serial1/1
D   192.168.20.64/29 [90/20514560] via 200.5.5.2, 00:45:47, Serial1/1
  200.5.5.0/24 is variably subnetted, 4 subnets, 2 masks
D   200.5.5.0/24 is a summary, 00:49:39, Null0
C   200.5.5.0/30 is directly connected, Serial1/1
D   200.5.5.4/30 [90/21024000] via 200.5.5.2, 00:11:23, Serial1/1
C   200.5.5.8/30 is directly connected, Serial1/0
```

Таким образом, пакеты будут передаваться не напрямую от R_A к R_C, а через R_B. При этом преемником (succcessor) будет интерфейс s1/2 маршрутизатора R_B с адресом 200.5.5.2. Новая метрика (21026560) немного хуже старой (20514560), но значительно лучше метрики прямого пути от R_A к R_C через 200.5.5.10, которая при скорости 64 кбит/с составляет 40514560.

Краткие итоги лекции 11

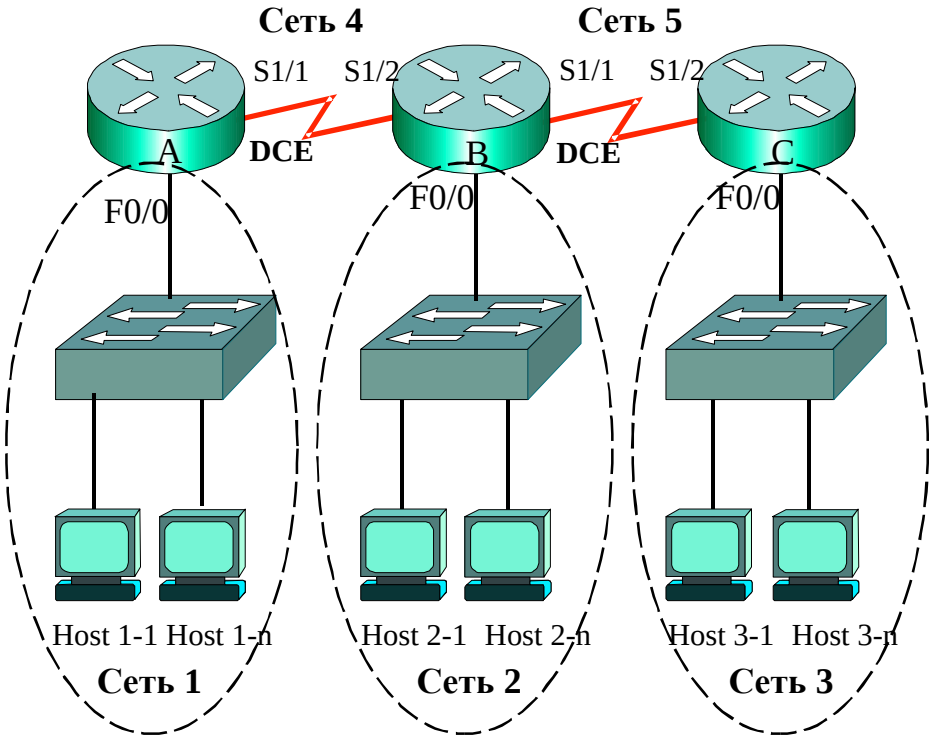
1. В случае не корректно спроектированной сети применение протокола RIP может привести к проблемам маршрутизации.
2. Протокол RIP в своих обновлениях (update) маршрутной информацией каждые 30 сек. не передает значения маски подсетей.
3. Протокол второй версии RIPv2 в своих сообщениях update дополнительно к адресу сети назначения передает значение маски и адрес следующего перехода (next-hop).
4. Протокол Enhanced IGRP предназначен для работы с аппаратурой Cisco.
5. Для контроля связи с соседними маршрутизаторами протокол EIGRP периодически каждые 5 секунд рассылает пакеты Hello с использованием многоадресного режима (адрес 224.0.0.10). Результатом обмена Hello-пакетами является построение таблицы соседних устройств.
6. Протокол EIGRP строит и поддерживает таблицу соседних устройств, таблицу топологии сети и таблицу маршрутизации.
7. Протокол EIGRP производит обмен маршрутной информацией, касающейся только изменений в сети, и с ограниченным числом тех маршрутизаторов, которые затрагивают эти изменения. Причем, в обновлениях передаются значения масок переменной длины.
8. Сходимость сетей EIGRP более быстрая по сравнению с сетями, использующими RIP.
9. Протокол EIGRP автоматически суммирует маршруты и при этом использует выходной интерфейс Null0.
10. Пакеты, поступающие на интерфейс Null0, уничтожаются.
11. Метрика протокола EIGRP учитывает целый ряд параметров: полосу пропускания и задержку, а также дополнительно загрузку и надежность.
12. Метрика сети, состоящей из нескольких соединений, определяется полосой пропускания самого «медленного» соединения и суммарной задержкой всех выходных интерфейсов маршрутизаторов.
13. Полоса пропускания задается в кбит/с, а суммарная задержка – в мкс.
14. По умолчанию на соединениях задается полоса 128 кбит/с. В некоторых случаях задается скорость E1 или T1.
15. Заголовок пакета EIGRP располагается следом за заголовком IP-пакета.
16. Протокол EIGRP взаимодействует с протоколом надежной доставки транспортного уровня (Reliable Transport Protocol – RTP).
17. Чтобы протокол EIGRP мог обеспечить маршрутизацию в топологии с разделенными сетями, необходимо отменить авто-суммирование маршрутов на маршрутизаторах.

Вопросы по лекции 11

1. Какие протоколы передают, и какие не передают в своих обновлениях значения маски подсетей?
2. Каков период передачи обновлений протокола RIP, RIP2?
3. Каков период передачи пакетов Hello протокола EIGRP?
4. Какой адрес используется при передаче пакетов Hello протокола EIGRP?
5. Какая таблица строится на основе обмена пакетами Hello? Какую информацию она содержит?
6. Когда протокол EIGRP производит обмен маршрутной информацией?
7. Какая таблица содержит полную информацию о топологии сети?
8. Как протокол EIGRP использует выходной интерфейс Null0?
9. Какие параметры учитывает метрика протокола EIGRP?
10. Какие параметры метрики протокола EIGRP учитываются по умолчанию?
11. Каковы достоинства и недостатки авто-суммирования?
12. С каким протоколом EIGRP взаимодействует на транспортном уровне?
13. Каков формат команд конфигурирования протокола EIGRP?
14. Какую информацию содержат таблицы топологии?

Упражнения

1. Сконфигурируйте динамическую маршрутизацию нижеприведенной схемы с заданными в таблице адресами с использованием протокола RIP. Проведите проверку и отладку с использованием команд **show running-config**, **show ip route**, **ping**, **traceroute** и **tracert**.



Наименование	Адрес	Наименование	Адрес
Сеть 1 f0/0 Host 1-1 Host 1-*n*	10.1.10.16/29 10.1.10.17 10.1.10.21 10.1.10.2*n*	Сеть 2 f0/0 Host 2-1 Host 2-*n*	172.16.20.64/28 172.16.20.65 172.16.20.71 172.16.20.7*n*
Сеть 3 f0/0 Host 3-1 Host 3-*n*	192.168.30.128/27 192.168.30.129 192.168.30.131 192.168.30.13*n*	Сеть 4 s1/1 s1/2	204.4.4.16/30 204.4.4.17 204.4.4.18
Сеть 5 s1/1 s1/2	204.4.4.20/30 204.4.4.21 204.4.4.22		

2. Удалите протокол RIP и сконфигурируйте динамическую маршрутизацию вышеприведенной схемы с заданными в таблице адресами с использованием протокола EIGRP. Проведите проверку и отладку сети.
3. Нужно ли отменять режим авто-суммирования? Почему?

Лекция 12. ПРОТОКОЛ МАРШРУТИЗАЦИИ OSPF

Краткая аннотация лекции: Рассмотрены особенности функционирования протокола состояния канала. Приведены общие сведения о протоколе OSPF и его конфигурировании. Даны примеры отладки сети.
Цель лекции: изучить особенности функционирования и конфигурирования протокола состояния канала OSPF.

12.1. Общие сведения о протоколе OSPF

Open Shortest Path First (**OSPF**) является **протоколом состояния канала** Link-state, который быстро реагируют на изменения в сети, рассылая модификации при изменениях в сетевой топологии всем маршрутизаторам в пределах некоторой области сети. OSPF предназначен для работы в больших гибких составных сетях и **может работать с оборудованием разных фирм** производителей, поэтому получил широкое распространение.

Административное расстояние протокола OSPF равно **110** (см. табл. 10.2). Протокол используется внутри определенной области, в которой маршрутизаторы разделяют маршрутную информацию между собой (рис.12.1). Таких областей может быть несколько, среди которых **нулевая область** (area 0) является главной или единственной. Далее рассматривается случай единственной области area 0.

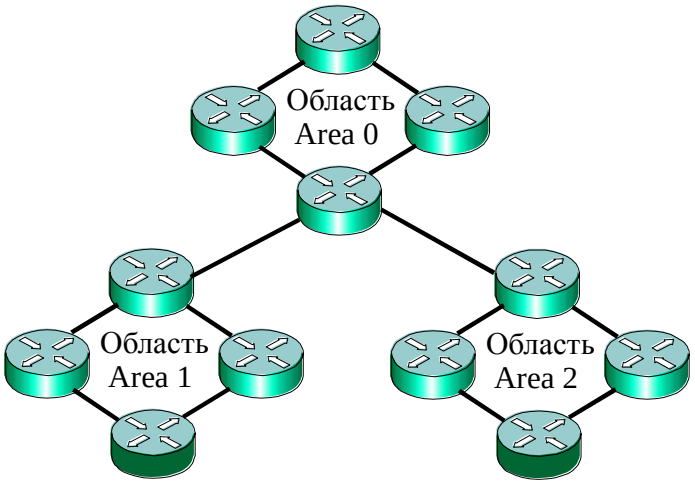


Рис.12.1. Области функционирования протокола OSPF

Протоколы Link-state создают таблицы маршрутизации на основе информации, хранящейся в **специальной базе данных** (link-state database), а также в **таблице данных соседних устройств** (neighbor table). При этом алгоритм Дийкстра (Dijkstra) обеспечивается выбор **кратчайшего пути** (shortest path) к адресату назначения. Протокол **OSPF не проводит периодический обмен объемными обновлениями** (update) маршрутной информации, также как протокол EIGRP, и характеризуется **быстрой сходимостью** (convergence).

Для обмена маршрутной информацией между устройствами протокол OSPF использует пять типов пакетов:

1. Пакет Hello
2. Пакет описания базы данных DataBase Description – DBD
3. Пакет запроса Link-State Request – LSR
4. Пакет обновлений Link-State Update – LSU
5. Пакет подтверждения Link-State Acknowledgment – LSAck.

Hello-пакеты используются, чтобы устанавливать и поддерживать **отношения смежности** (adjacency) между соседними устройствами. Hello-пакеты содержат **идентификатор устройства** (Router ID), который по сути является адресом одного из интерфейсов маршрутизатора. На этапе формирования смежности устанавливаются 3 значения пароаметров:

1. Период времени обмена Hello-пакетами (Hello Interval)
2. Период времени (Dead Interval), по истечению которого связь считается потерянной, если за это время не было получено ни одного Hello-пакета.
3. Тип сети (Network Type).

Различают три типа сетей:

1. Широковещательные с множественным доступом (Broadcast multi-access), например Ethernet.

2. Сети типа точка-точка (Point-to-point)/

3. Нешироковещательные с множественным доступом (Nonbroadcast multi-access – NBMA), например, сети Frame Relay, ATM.

В сетях первых двух типов **период рассылки Hello-пакетов** составляет 10 секунд, а в сетях NBMA – 30 сек. Период Dead Interval – в четыре раза больше. Обмен Hello-пакетами производится с использованием

адресов **224.0.0.5** или **224.0.0.6 многоадресного режима** (multicast) без подтверждения доставки.

Пакет DBD содержит сокращенный список базы данных передающего маршрутизатора и используется принимающим маршрутизатором для проверки своей базы данных. Принимающий маршрутизатор может запросить полную информацию о входах базы данных, используя пакет запроса Link-State Request – LSR .

Для ответа на запрос LSR используется **пакет обновлений** Link-State Update – LSU. Пакет LSU может содержать 7 различных типов извещений или объявлений (Link-State Advertisements – **LSA**s). Обмен маршрутной информацией производится только при возникновении изменений в сети. Когда происходят изменения, маршрутизатор, первым заметивший это изменение, создает извещение о состоянии этого соединения LSAs, которое передается соседним устройствам. Каждое устройство маршрутизации получив обновление LSAs, модифицирует свою базу данных и транслирует копии LSAs всем соседним маршрутизаторам.

Для подтверждения принятого пакета обновлений LSU используется **пакет подтверждения** (Link-State Acknowledgment – LSAck).

Когда в сети происходит изменение, например, соседнее устройство становится недостижимым, протоколы состояния связи заполняют всю область обновлениями **LSA**s с использованием многоадресного режима multicast 224.0.0.5. Информация рассылается во все порты, кроме порта, на котором данная информация была получена. Каждый маршрутизатор копирует сообщение LSAs и модифицирует свое состояние связи, т.е. **топологическую базу данных**, которая содержит весь набор состояний. Затем маршрутизатор передает LSAs на все соседние маршрутизаторы в пределах области (area) и они **повторно вычисляют маршруты**. Итак, **обновления маршрутной информации вызываются изменениями в сети.**

Состояние связи (соединения) – это **описание интерфейса**, которое должно включать IP адрес интерфейса, маску подсети, тип сети и так далее. Содержащаяся в топологической базе данных информация используется, чтобы вычислить лучшие пути через сеть. Для вычисления кратчайшего пути к адресату назначения строится дерево, где корнем является сам маршрутизатор. Затем отбираются кратчайшие пути к сетям назначения и помещаются в таблицу маршрутизации. При вычислениях используется

алгоритм Dijkstra выбора первого кратчайшего пути (shortest path first algorithm). Построение топологического дерева с использованием алгоритма Dijkstra позволяет формировать **пути свободные от маршрутных петель** (loop-free routing). Для этого протокол OSPF создает и поддерживает:

Топологическую базу данных (link-state database).

Базу данных смежных устройств (adjacency database).

Таблицу маршрутизации.

Пакет OSPF размещается внутри IP-пакета сразу вслед за заголовком. Основной информацией пакета OSPF является:

- тип пакета,
- идентификатор маршрутизатора (Router ID),
- номер области (area 0),
- маска сети или подсети,
- интервалы времени (Hello Interval, Dead Interval),
- идентификаторы **главного назначенного маршрутизатора** (Designated Router - **DR**) и **запасного** (Backup Designated Router - **BDR**) определяющего маршрутизатора данной области,
- список соседних устройств.

Выбор главного назначенного маршрутизатора области сети (**DR**) и запасного назначенного маршрутизатора сети (**BDR**), производится в сетях с множественным доступом. В сетях «точка-точка» этот механизм не используется. В сегменте сети с множественным доступом, несколько маршрутизаторов связаны между собой. Поскольку каждый маршрутизатор должен установить полное отношение смежности со всеми соседними маршрутизаторами и обменяться информацией о состоянии связи (соединений), то, например, при 5 маршрутизаторах необходим обмен десятью состояниями связи. В общем случае для n маршрутизаторов должно быть $n\cdot(n-1)/2$ обменов, на что должны быть выделены дополнительные ресурсы, прежде всего, полоса пропускания.

Если в сети выбран главный назначенный маршрутизатор области (**DR**), то маршрутизатор, первым обнаруживший изменение в сети, посылает информацию об изменениях только маршрутизатору **DR**, а тот в свою очередь, рассылает LSAs всем другим OSPF маршрутизаторам области, используя адрес 224.0.0.5. Если маршрутизатор **DR** выходит из строя, то его

функции начинает выполнять запасной назначенный маршрутизатор области сети **BDR**.

Существует механизма выбора маршрутизаторов **DR** и **BDR**.

1. Выбор **DR** и **BDR** происходит на основе сравнения приоритетов маршрутизаторов. По умолчанию приоритет всех маршрутизаторов равен 1. Приоритеты могут быть установлены на любое значение от 0 до 255. Маршрутизатор с приоритетом 0 не может быть избранным **DR** или **BDR**. Маршрутизатор с самым высоким OSPF приоритетом будет отобран как DR маршрутизатор. Маршрутизатор со вторым приоритетом будет BDR.

2. Когда не задано никаких дополнительных параметров и приоритет одинаков, в качестве идентификатора ID маршрутизатора протокол OSPF выбирает адрес одного из своих интерфейсов с наибольшим значением. Маршрутизатор с высшим значением идентификатора **ID** становится **DR**. Маршрутизатор со вторым наибольшим значением идентификатора ID становится **BDR**.

3. Поскольку у интерфейсов используются разъемы, то они являются ненадежными элементами сети. Для повышения надежности на маршрутизаторах формируют **виртуальные логические интерфейсы** loopback. OSPF использует адрес интерфейса loopback как ID маршрутизатора, независимо от значения адресов других интерфейсов. Маршрутизатор, на котором сформировано несколько интерфейсов loopback, использует самый большой адрес интерфейса loopback в качестве ID маршрутизатора. Таким образом, выбор **DR** и **BDR** происходит на основе сравнения адресов интерфейсов loopback.

После выбора, DR и BDR сохраняют свои роли, даже если к сети добавляются маршрутизаторы с более высоким приоритетом до тех пор, пока маршрутизаторы не будут переконфигурированы.

Создание интерфейса loopback производится по команде **interface loopback**, например:

```
Router(config)# interface loopback 0
Router(config-if)#ip address 10.1.1.1 255.255.255.255
```

Интерфейс loopback должен формироваться с маской подсети на 32 бита – **255.255.255.255**. Такая маска называется маской узла, потому что маска подсети определяет сеть одного узла.

Изменение OSPF приоритета может производиться администратором по команде **ip ospf priority** в режиме конфигурирования интерфейса:

```
Router(config-if)#ip ospf priority №
```

Значение приоритета (№) интерфейса может изменяться в пределах от 0 до 255. Приоритет можно посмотреть по команде **show ip ospf interface**:

```
Router#show ip ospf interface тип интерфейса
```

Кроме того, идентификатор маршрутизатора может быть задан администратором по команде:

```
Router(config)#router ospf № процесса
Router(config-router)#router-id ip-адрес
```

Метрика протокола OSPF

Протокол маршрутизации OSPF использует метрику **cost**. Метрика протокола OSPF базируются на полосе пропускания **bandwidth**. Алгоритм протокола рассчитывает **суммарное значение метрики всех соединений** через сеть. Меньшее число указывает лучший маршрут. Для вычисления метрики OSPF используется следующая формула:

$$\textbf{Метрика (Cost)} = 10^8 / \textbf{Bandwidth.}$$

Соединение FastEthernet имеет стоимость – 1 единица, Ethernet – 10 единиц, канал ОЦК со скоростью 64 кбит/с – 1562,5 ≈ 1562, канал со скоростью 128 кбит/с – 781, канал Т1 – 64, канал Е1 – 48 единиц. Если маршрут состоит из нескольких соединений, то значения метрик складываются. Например, для сети (рис.12.2) метрика маршрута из локальной Сети 1 в локальную Сеть 2 будет складываться из метрики исходящей Сети 1 – Fast Ethernet (1), метрики соединения маршрутизаторов А и В (48), метрики соединения маршрутизаторов В и С (1562) и метрики сети назначения Ethernet (10).

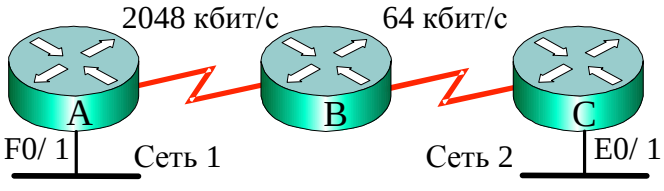


Рис. 12.2. Метрика сети OSPF

Суммарное значение метрики будет равно M_{Σ} = 1+48+1562+10 = 1621.

Значение полосы пропускания может быть изменено по команде **bandwidth**, например:

```
Router(config)#interface serial 0/0
Router(config-if)#bandwidth 64
```

Изменение полосы пропускания должно соответствовать реальным линиям связи. Причем, ширина полосы пропускания должна быть задана одинаковой на обеих сторонах соединения «точка-точка». Операционная система Cisco IOS позволяет задавать не только ширину полосы **bandwidth**, но и непосредственно значение **cost** по команде:

```
Router(config-if)#ip ospf cost значение
```

Применение соединений GigabitEthernet и 10-GigabitEthernet приводит к необходимости изменения значений метрики.

12.2. Конфигурирование протокола OSPF

Ниже приведен пример конфигурирования протокола OSPF на маршрутизаторах составной сети (рис. 12.3) с таблицей адресов (табл. 12.1).

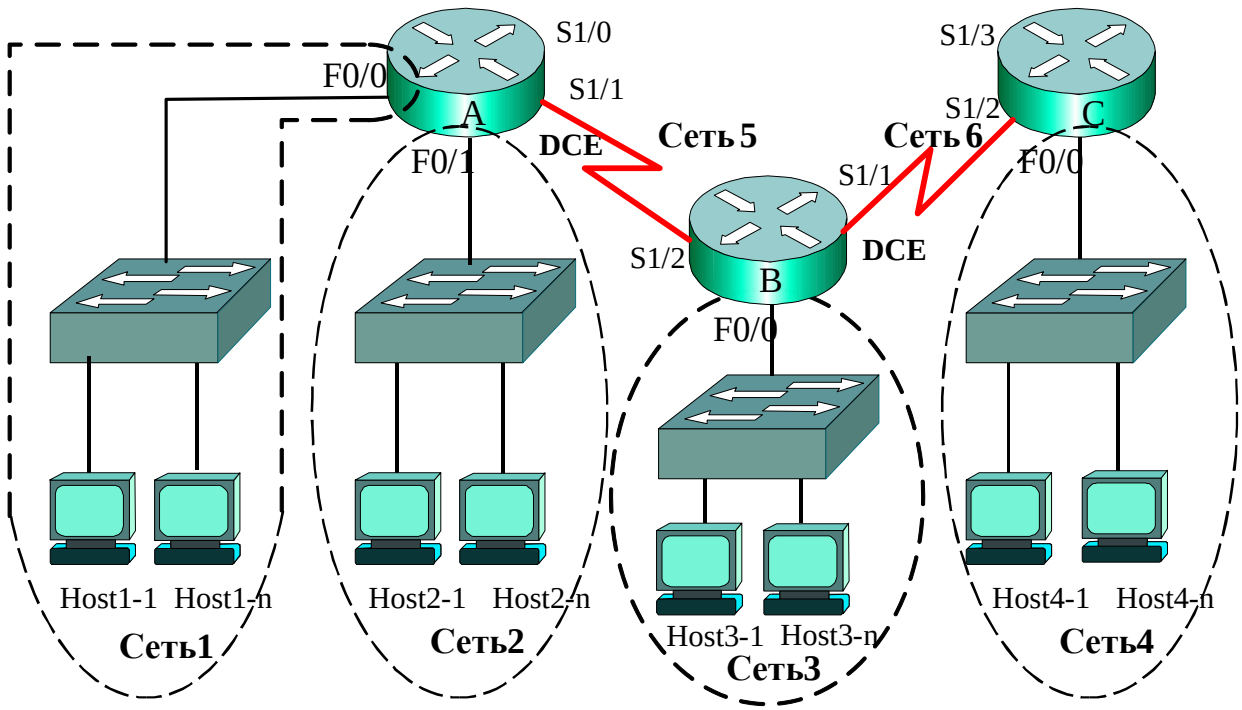


Рис.12.3. Пример составной сети OSPF

Таблица 12.1

Адреса сетей, интерфейсов и узлов составной сети

Наименование	Адрес	Наименование	Адрес
Сеть 1 f0/0 Host 1-1 Host 1-*n*	10.10.10.16/28 10.10.10.17 10.10.10.18 102.10.10.*n*	Сеть 2 f0/1 Host 2-1 Host 2-*n*	10.10.10.32/27 10.10.10.33 10.10.10.34 10.10.10.*m*
Сеть 3 f0/0 Host 3-1 Host 3-*n*	172.16.20.64/29 172.16.20.65 172.16.20.66 172.16.20.*k*	Сеть 4 f0/0 Host 4-1 Host 4-*n*	10.10.10.128/26 10.10.10.129 10.10.10.130 10.10.10.*n*
Сеть 5 s1/1 s1/2	200.5.5.20/30 200.5.5.21 200.5.5.22	Сеть 6 s1/1 s1/2	200.5.5.24/30 200.5.5.25 200.5.5.26

Из рис. 12.3 и табл. 12.1 следует, что Сеть 1 (192.168.10.16/28), Сеть 2 (192.168.10.32/27) и Сеть 4 (192.168.10.128/26) являются подсетями сети 192.168.10.0/24. Причем, Сети 1, 2 и Сеть 4 разделены Сетью 5 и Сетью 6.

При конфигурировании протокола OSPF необходимо задать номер процесса (по умолчанию 1) и адреса непосредственно присоединенных сетей с их масками переменной длины (wildcard-mask). При этом для каждой сети указывается номер области (по умолчанию area 0). Адреса сетей и интерфейсов приведены в табл. 12.1.

Маршрутизатор Router_A:

```
Router_A(config)#router ospf 1
Router_A(config-router)#network 10.10.10.16 0.0.0.15 area 0
Router_A(config-router)#network 10.10.10.32 0.0.0.31 area 0
Router_A(config-router)#network 200.5.5.20 0.0.0.3 area 0
```

Маршрутизатор Router_B:

```
Router_B(config)#router ospf 1
Router_B(config-router)#network 172.16.20.64 0.0.0.7 area 0
Router_B(config-router)#network 200.5.5.20 0.0.0.3 area 0
Router_B(config-router)#network 200.5.5.24 0.0.0.3 area 0
```

Маршрутизатор Router_C:

```
Router_C(config)#router ospf 1
Router_C(config-router)#network 10.10.10.128 0.0.0.63 area 0
Router_C(config-router)#network 200.5.5.24 0.0.0.3 area 0
```

Скорость передачи на всех последовательных соединениях по умолчанию равна **128 кбит/с**, т.е. каждое соединение характеризуется **метрикой** в **781** единицу. Ниже приведены таблицы маршрутизации всех маршрутизаторов (A, B, C).

Таблица маршрутизации R_A:

```
R_A#sh ip route
...
Gateway of last resort is not set

   10.0.0.0/8 is variably subnetted, 3 subnets, 3 masks
C     10.10.10.16/28 is directly connected, FastEthernet0/0
C     10.10.10.32/27 is directly connected, FastEthernet0/1
O     10.10.10.128/26 [110/1563] via 200.5.5.22, 00:10:18, Serial1/1
   172.16.0.0/29 is subnetted, 1 subnets
O     172.16.20.64 [110/782] via 200.5.5.22, 00:12:16, Serial1/1
   200.5.5.0/30 is subnetted, 3 subnets
C     200.5.5.20 is directly connected, Serial1/1
O     200.5.5.24 [110/1562] via 200.5.5.22, 00:12:46, Serial1/1
```

Маршруты протокола OSPF помечены символом O, административное расстояние – 110. Метрика пути к сети 172.16.20.64 составляет 782 единицы (781 единица последовательное соединение «точка-точка» со скоростью 128 кбит/с и соединение FastEthernet с метрикой в 1 единицу). В распечатке таблицы маршрутизации Router_A следует обратить внимание на то, что метрика к сети 200.5.5.24 составляет 1562 единицы (два последовательных соединения «точка-точка»), а к сети 10.10.10.128 – на 1 больше (1563 единицы). Это объясняется тем, что на пути к сети 10.10.10.128 дополнительно имеется соединение FastEthernet с метрикой в 1 единицу.

Таблица маршрутизации Router_B:

```
R_B#sh ip route
...
Gateway of last resort is not set

    10.0.0.0/8 is variably subnetted, 3 subnets, 3 masks
O      10.10.10.16/28 [110/782] via 200.5.5.21, 00:04:09, Serial1/2
O      10.10.10.32/27 [110/782] via 200.5.5.21, 00:04:09, Serial1/2
O      10.10.10.128/26 [110/782] via 200.5.5.26, 00:01:52, Serial1/1
    172.16.0.0/29 is subnetted, 1 subnets
C      172.16.20.64 is directly connected, FastEthernet0/0
    200.5.5.0/30 is subnetted, 2 subnets
C      200.5.5.20 is directly connected, Serial1/2
C      200.5.5.24 is directly connected, Serial1/1
```

Из распечатки таблицы маршрутизации R_B следует, что в сети 10.10.10.16/28 и 10.10.10.32/27 можно попасть через шлюз 200.5.5.21, а в сеть 10.10.10.128/26 через интерфейс 200.5.5.26. Таким образом, протокол OSPF не суммирует маршруты в рамках сети полного класса.

Таблица маршрутизации Router_C:

```
R_C#sh ip route
...
Gateway of last resort is not set

    10.0.0.0/8 is variably subnetted, 3 subnets, 3 masks
O      10.10.10.16/28 [110/1563] via 200.5.5.25, 00:02:34, Serial1/2
O      10.10.10.32/27 [110/1563] via 200.5.5.25, 00:02:34, Serial1/2
C      10.10.10.128/26 is directly connected, FastEthernet0/0
    172.16.0.0/29 is subnetted, 1 subnets
O      172.16.20.64 [110/782] via 200.5.5.25, 00:02:34, Serial1/2
    200.5.5.0/30 is subnetted, 3 subnets
O      200.5.5.20 [110/1562] via 200.5.5.25, 00:02:34, Serial1/2
C      200.5.5.24 is directly connected, Serial1/2
```

Из распечатки таблицы маршрутизации R_C видно, что существуют маршруты ко всем подсетям сети рис.12.3.

Введение нового соединения между маршрутизаторами A и C (рис. 12.4) несколько изменяет топологию сети и таблиц маршрутизации. Сеть 7 имеет адрес 200.5.5.28/30, интерфейс s1/0 маршрутизатора A – 200.5.5.29, интерфейс s1/3 маршрутизатора B – 200.5.5.30.

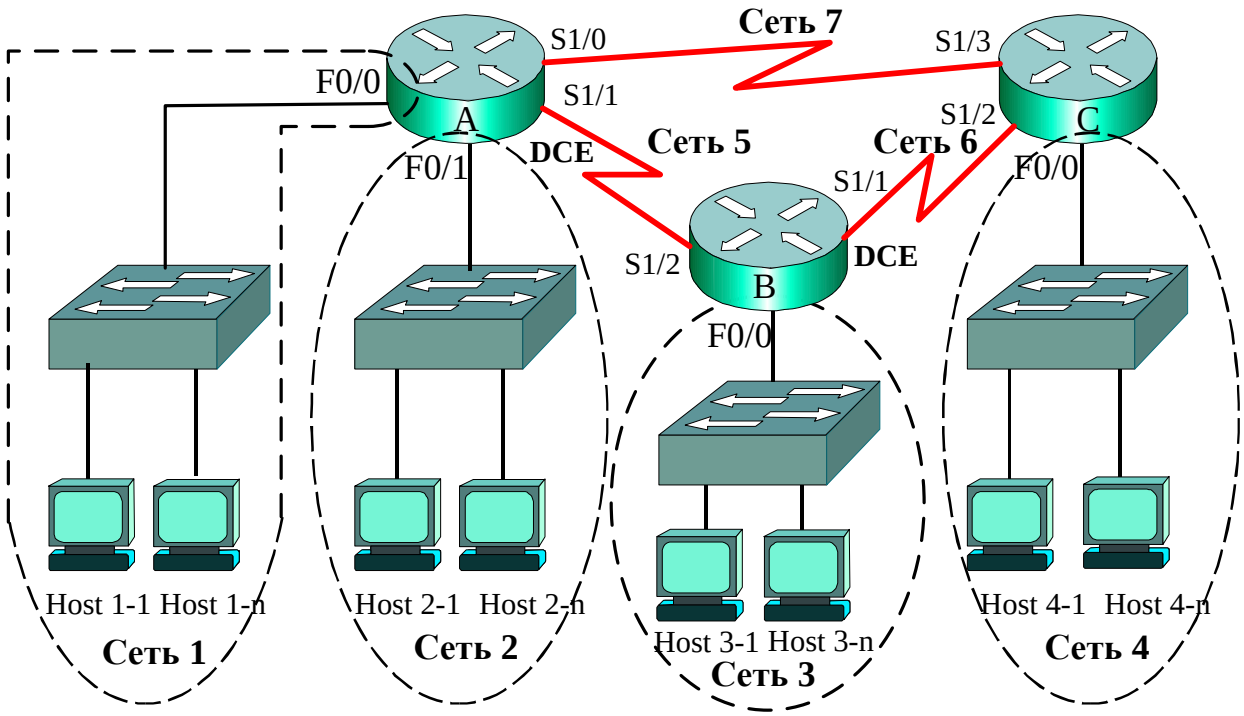


Рис.12.4. Измененная топология составной сети OSPF

Таблица маршрутизации R_A:

```
R_A# sh ip route
...
    10.0.0.0/8 is variably subnetted, 3 subnets, 3 masks
C       10.10.10.16/28 is directly connected, FastEthernet0/0
C       10.10.10.32/27 is directly connected, FastEthernet0/1
O       10.10.10.128/26 [110/782] via 200.5.5.30, 00:04:02, Serial1/0
    172.16.0.0/29 is subnetted, 1 subnets
O       172.16.20.64 [110/782] via 200.5.5.22, 00:20:44, Serial1/1
    200.5.5.0/30 is subnetted, 3 subnets
C       200.5.5.20 is directly connected, Serial1/1
O       200.5.5.24 [110/1562] via 200.5.5.22, 00:20:30, Serial1/1
                   [110/1562] via 200.5.5.30, 00:04:02, Serial1/0
C       200.5.5.28 is directly connected, Serial1/0
```

Из распечатки следует, что путь до сети 10.10.10.128/26 сократился со значения 1563 до 782. В сеть 200.5.5.24 можно попасть как через интерфейс 200.5.5.22, так и через – 200.5.5.30, причем метрика одинакова (1562). Появилась непосредственно присоединенная сеть 200.5.5.28. Остальные параметры таблицы маршрутизации R-A остались без изменений.

Первая строка таблицы маршрутизации R_A содержит родительский маршрут 10.0.0.0/8, где указано, что сеть включает три подсети с масками

переменной длины. В этом случае маска /8 относится именно к родительской сети полного класса. Далее указаны три дочерних подсети, каждая со своим префиксом /28, /27, /26.

Когда родительская сеть включает одну подсеть, как в пятой строке таблицы R_A (172.16.0.0/29), то префикс /29 относится к дочерней сети, которая представлена в следующей строке таблицы – 172.16.20.64.

Таблица маршрутизации R_B:

```
R_B>sh ip route
...
    10.0.0.0/8 is variably subnetted, 3 subnets, 3 masks
O      10.10.10.16/28 [110/782] via 200.5.5.21, 00:18:37, Serial1/2
O      10.10.10.32/27 [110/782] via 200.5.5.21, 00:18:37, Serial1/2
O      10.10.10.128/26 [110/782] via 200.5.5.26, 00:14:13, Serial1/1
    172.16.0.0/29 is subnetted, 1 subnets
C      172.16.20.64 is directly connected, FastEthernet0/0
    200.5.5.0/30 is subnetted, 3 subnets
C      200.5.5.20 is directly connected, Serial1/2
C      200.5.5.24 is directly connected, Serial1/1
O      200.5.5.28 [110/1562] via 200.5.5.26, 00:04:26, Serial1/1
                  [110/1562] via 200.5.5.21, 00:02:06, Serial1/2
```

Изменения в таблице R_B связаны только с новой сетью 200.5.5.28, к которой ведут два равнозначных пути: через 200.5.5.21 и через 200.5.5.26.

Таблица маршрутизации R_C:

```
R_C#sh ip route
...
     10.0.0.0/8 is variably subnetted, 3 subnets, 3 masks
O       10.10.10.16/28 [110/782] via 200.5.5.29, 00:03:01, Serial1/3
O       10.10.10.32/27 [110/782] via 200.5.5.29, 00:03:01, Serial1/3
C       10.10.10.128/26 is directly connected, FastEthernet0/0
     172.16.0.0/29 is subnetted, 1 subnets
O       172.16.20.64 [110/782] via 200.5.5.25, 00:15:18, Serial1/2
     200.5.5.0/30 is subnetted, 3 subnets
O       200.5.5.20 [110/1562] via 200.5.5.25, 00:15:18, Serial1/2
                   [110/1562] via 200.5.5.29, 00:03:01, Serial1/3
C       200.5.5.24 is directly connected, Serial1/2
C       200.5.5.28 is directly connected, Serial1/3
```

Распечатка таблицы маршрутизации R_C позволяет сделать вывод о том, что маршруты к подсетям 10.10.10.16 и 10.10.10.32 сократились практически в два раза (метрика 782 вместо 1563), и проходят через

интерфейс 200.5.5.29 (ранее был 200.5.5.25). Трафик в сеть 200.5.5.20 может передаваться поочередно (режим баланса) как через интерфейс 200.5.5.25, так и через 200.5.5.29. Остальные параметры таблицы маршрутизации остались без изменений.

Краткие итоги лекции 12

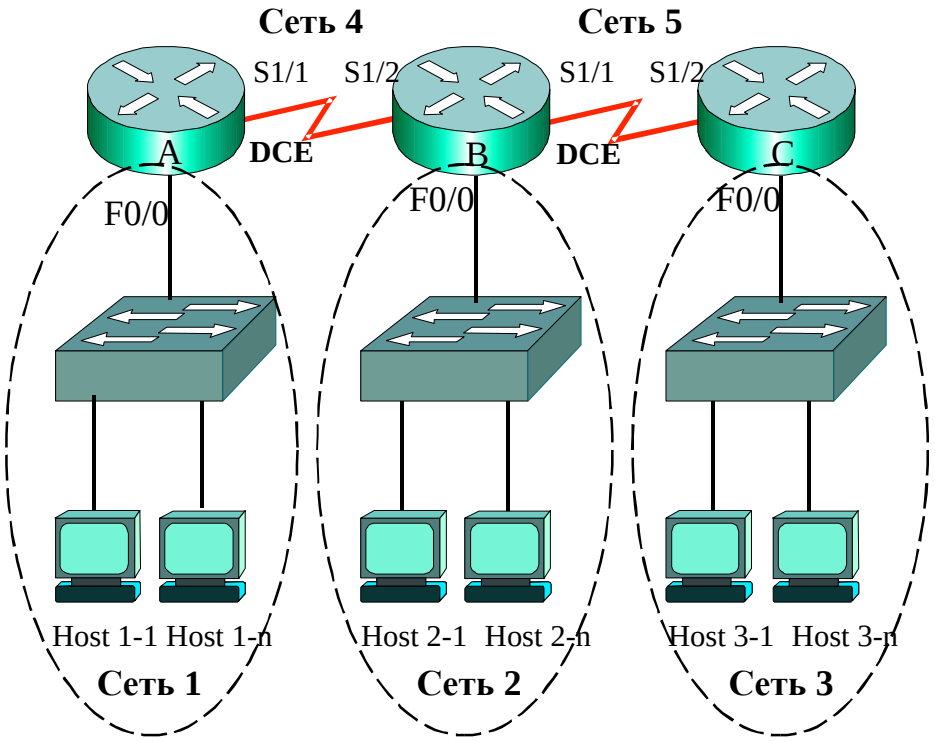
1. Протокол состояния канала Open Shortest Path First – OSPF предназначен для работы в больших гибких составных сетях и может работать с оборудованием разных фирм производителей.
2. Административное расстояние протокола OSPF равно 110. Протокол используется внутри определенной области, нулевая область (area 0) является главной или единственной.
3. Протокол создает таблицы маршрутизации на основе информации, хранящейся в специальной базе и в таблице данных соседних устройств.
4. Протокол OSPF не проводит периодический обмен объемными обновлениями (update) маршрутной информации, также как протокол EIGRP, и характеризуется быстрой сходимостью. Обмен маршрутной информацией производится только при возникновении изменений в сети.
5. Hello-пакеты используются, чтобы устанавливать и поддерживать отношения смежности (adjacency) между соседними устройствами.
6. Период рассылки Hello-пакетов протокола OSPF составляет 10 секунд. Обмен Hello-пакетами производится с использованием адресов 224.0.0.5 или 224.0.0.6 многоадресного режима.
7. Для подтверждения принятого пакета обновлений используется пакет подтверждения.
8. Каждый маршрутизатор копирует сообщение и модифицирует свое состояние связи, т.е. топологическую базу данных, которая содержит весь набор состояний соединений.
9. Для формирования путей свободных от маршрутных петель строится топологическое дерево с использованием алгоритма Dijkstra выбора первого кратчайшего пути.
10. В сетях с множественным доступом выбирается главный назначенный маршрутизатор (Designated Router - DR) и запасной (Backup Designated Router - BDR), что сокращает объем информации обновлений. Выбор DR и BDR происходит на основе идентификаторов маршрутизаторов.
11. Метрика протокола OSPF базируются на полосе пропускания. Алгоритм протокола рассчитывает суммарное значение метрики всех соединений.
12. Протокол OSPF поддерживает маски переменной длины, бесклассовую адресацию на основе префикса, обеспечивает маршрутизацию в топологии с разделенными сетями.

Вопросы по лекции 12

1. Какую информацию содержит пакет OSPF при обновлениях?
2. Каков период передачи пакетов Hello протокола OSPF?
3. Какая таблица строится на основе обмена пакетами Hello? Какая адресация используется при этом?
4. Когда протокол OSPF производит обмен маршрутной информацией?
5. Какая база данных содержит полную информацию о топологии сети?
6. Какие параметры учитывает метрика протокола OSPF?
7. Каков формат команд конфигурирования протокола OSPF?

Упражнения

Сконфигурируйте динамическую маршрутизацию OSPF нижеприведенной схемы с заданными в таблице адресами. Проведите проверку и отладку с использованием команд **show running-config**, **show ip route**, **ping**, **traceroute** и **tracert**.



Наименование	Адрес	Наименование	Адрес
Сеть 1 f0/0 Host 1-1 Host 1-*n*	10.1.10.0/28 10.1.10.1 10.1.10.2 10.1.10.*n*	Сеть 2 f0/0 Host 2-1 Host 2-*n*	172.16.20.0/27 172.16.20.1 172.16.20.2 172.16.20.*n*
Сеть 3 f0/0 Host 3-1 Host 3-*n*	192.168.30.0/26 192.168.30.1 192.168.30.2 192.168.30.*n*	Сеть 4 s1/1 s1/2	204.4.4.0/30 204.4.4.1 204.4.4.2
Сеть 5 s1/1 s1/2	205.5.5.0/30 200.5.5.1 200.5.5.2		

Проанализируйте таблицы маршрутизации. Посчитайте метрики маршрутов.

Контрольный тест по разделу 5

Задача 5.1
Вариант 1 Задачи 5.1

136. Протокол динамической маршрутизации RIP-2 задается по команде:

1. `Router(config)#`**`router rip-2`**
2. `Router(config)#`**`router rip version-2`**
3. `Router(config)#`**`router rip`**
   `Router(config-router)#`**`version 2`**
4. `Router(config)#`**`router`**
   `Router(config-router)#` **`rip version 2`**

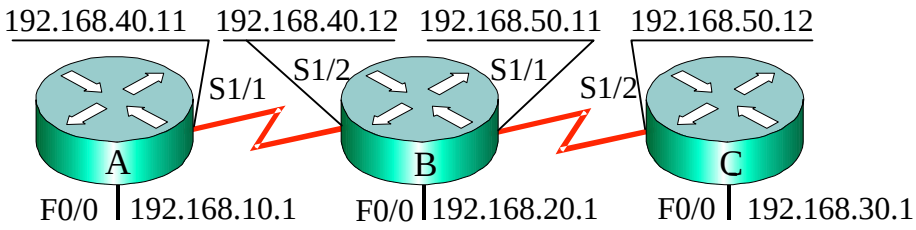
Вариант 2 Задачи 5.1

137. При конфигурировании протокола динамической маршрутизации RIP-2 наиболее коротким будет следующее описание непосредственно присоединенной сети с адресом 192.168.10.32/28:

```
Router(config-router)#network 192.168.10.0
Router(config-router)#network 192.168.10.32 0.0.0.15
Router(config-router)#network 192.168.10.32 255.255.255.240
Router(config-router)#network 192.168.10.32 255.255.255.240 area 0
```

Вариант 3 Задачи 5.1

138. При конфигурировании протокола динамической маршрутизации RIP-2 для нижеприведенной схемы отметить правильный вариант динамической маршрутизации:



1.
```
Router-A(config)#router rip-2
Router-A(config-router)#network 192.168.10.0
Router-A(config-router)#network 192.168.40.0
```

2.
```
Router-A(config)#router rip
Router-A(config-router)#version 2
Router-A(config-router)#network 192.168.10.0
Router-A(config-router)#network 192.168.40.0
```

3.
```
Router-A(config)#router rip version 2
Router-A(config-router)#network 192.168.10.0
Router-A(config-router)#network 192.168.40.0
```

4.
```
Router-A(config)#router rip
Router-A(config-router)#version 2
Router-A(config-router)#network 192.168.20.0
Router-A(config-router)#network 192.168.30.0
```

Задача 5.2
Вариант 1 Задачи 5.2

139. При использовании протокола динамической маршрутизации RIP-2 задается:
- Номер автономной системы
- Номер области (area)
- Номер процесса
- Ничего из вышеперечисленного

Вариант 2 Задачи 5.2

140. При использовании протокола маршрутизации RIP-2 в обновлениях передается:
- Адрес сети назначения
- Значение сетевой маски
- Адрес следующего перехода
- Номер автономной системы
- Номер области (area)
- Значение задержки пакета в маршрутизаторе

Вариант 3 Задачи 5.2

141. Максимальное число переходов на пути к адресату назначения протокола RIP-2 равно:

10, 15, 16, 24, 255

Задача 5.3
Вариант 1 Задачи 5.3

142. По умолчанию метрика протокола EIGRP определяется следующими параметрами: (выбрать два ответа)

Количеством переходов (hop count)
Шириной полосы пропускания (bandwidth)
Задержкой (delay)
Загрузкой (load)
Стоимостью (cost)

Вариант 2 Задачи 5.3

143. Hello-пакеты протокола EIGRP для поддержания отношения смежности (adjacency) между соседними устройствами передаются:

Периодически каждые 5 сек.
Периодически каждые 10 сек.
Периодически каждые 30 сек.
Периодически каждые 90 сек.
Не периодически, при изменениях в сети

Вариант 3 Задачи 5.3

144. Hello-пакеты протокола EIGRP для поддержания отношения смежности (adjacency) между соседними устройствами передаются:

С использованием широковещательных адресов 255.255.255.255 и без подтверждения доставки
С использованием многоадресного режима 224.0.0.10 и с подтверждением доставки
С использованием многоадресного режима 224.0.0.10 и без подтверждения доставки
С использованием многоадресного режима 224.0.0.5 и с подтверждением доставки
С использованием широковещательных адресов 255.255.255.255 и с подтверждением доставки

Задача 5.4
Вариант 1 Задачи 5.4

145. Пакеты обмена маршрутной информацией (Update) протокол EIGRP пересылает:

Периодически каждые 5 секунд
Периодически каждые 10 секунд
Периодически каждые 30 секунд
Периодически каждые 90 секунд
Не периодически, при изменениях в сети

Вариант 2 Задачи 5.4

146. Таблицы протокола EIGRP находятся между собой в следующих отношениях:

Таблица соседних устройств и таблица маршрутизации используются для создания таблицы топологии сети
Таблица соседних устройств и топологическая используются для создания таблицы маршрутизации

Таблица маршрутизации и топологическая используются для создания таблицы соседних устройств
Все три таблицы являются независимыми друг от друга

Вариант 3 Задачи 5.4

147.Административное расстояние протокола EIGRP составляет:

1, 90, 100, 110, 115, 120

Задача 5.5
Вариант 1 Задачи 5.5

148. При конфигурировании протокола EIGRP

```
Router_B(config)#router eigrp 30
Router_B(config-router)#network 192.168.1.32 0.0.0.31
Router_B(config-router)#network 200.5.5.4 0.0.0.3
Router_B(config-router)#network 200.5.5.8 0.0.0.3
Router_B(config-router)#network 210.10.10.20 0.0.0.3
```

команды **network** задают:

Адреса удаленных сетей назначения с маской
Адреса непосредственно присоединенных сетей с маской
Адреса сетей непосредственно присоединенных к соседнему маршрутизатору
Адреса локальных сетей с маской
Адреса глобальных сетей с маской

Вариант 2 Задачи 5.5

149. При конфигурировании протокола EIGRP

```
Router_B(config)#router eigrp 30
Router_B(config-router)#network 192.168.1.32 0.0.0.31
Router_B(config-router)#network 200.5.5.4 0.0.0.3
Router_B(config-router)#network 200.5.5.8 0.0.0.3
Router_B(config-router)#network 210.10.10.20 0.0.0.3
```

число 30 означает:

Номер сети назначения
Номер сети источника
Номер автономной системы
Номер порта
Номер области (area)

Вариант 3 Задачи 5.5

150. При конфигурировании протокола EIGRP

```
Router_B(config)#router eigrp 30
Router_B(config-router)#network 192.168.1.32 0.0.0.31
Router_B(config-router)#network 200.5.5.4 0.0.0.3
Router_B(config-router)#network 200.5.5.8 0.0.0.3
Router_B(config-router)#network 210.10.10.20 0.0.0.3
```

число 0.0.0.31 означает :

Количество локальных сетей в составной сети
Номер автономной системы непосредственно присоединенной сети
Адрес сети непосредственно присоединенной к соседнему маршрутизатору
Инверсную маску непосредственно присоединенной сети
Сетевую маску удаленной сети назначения

Задача 5.6
Вариант 1 Задачи 5.6

151. В строке таблицы маршрутизации

D 192.168.2.0/24 [90/21538560] via 210.10.10.22, 00:12:58, Serial1/0

число 21538560 в квадратных скобках означает:

Число переходов до сети назначения
Маршрут создан протоколом EIGRP
Маршрут создан администратором
Метрика пути до сети назначения
Сеть назначения недостижима

Вариант 2 Задачи 5.6

152. В строке таблицы маршрутизации

D 192.168.2.0/24 [90/21538560] via 210.10.10.22, 00:12:58, Serial1/0

запись via 200.10.10.22 означает: (выбрать два ответа)

Адрес сети назначения
Адрес выходного интерфейса маршрутизатора на пути к сети назначения
Адрес входного интерфейса соседнего маршрутизатора на пути к сети назначения
Адрес запасного преемника (feasible succcessor)
Адрес преемника (succcessor)

Вариант 3 Задачи 5.6

153. В строке таблицы маршрутизации

D 192.168.2.0/24 [90/21538560] via 210.10.10.22, 00:12:58, Serial1/0
запись Serial1/0 означает:

Выходной интерфейс маршрутизатора на пути к сети назначения
Входной интерфейс соседнего маршрутизатора на пути к сети назначения
Входного интерфейса маршрутизатора, с которого поступил пакет
Шлюз по умолчанию (next hop)

Задача 5.7
Вариант 1 Задачи 5.7

154. Метрика протокола OSPF определяется следующим параметром:

Количеством переходов (hop count)
Надежностью (reliability)

Задержкой (delay)
Загрузкой (load)
Стоимостью (cost)

Вариант 2 Задачи 5.7

155. Пакеты обмена маршрутной информацией протокол OSPF пересылает:

Периодически каждые 5 секунд
Периодически каждые 10 секунд
Периодически каждые 30 секунд
Периодически каждые 90 секунд
Не периодически, при изменениях в сети

Вариант 3 Задачи 5.7

156. Hello-пакеты протокола OSPF для поддержания отношения смежности (adjacency) между соседними устройствами передаются:

Не периодически, с использованием широковещательных адресов 255.255.255.255 и без подтверждения доставки
Периодически каждые 5 сек. с использованием многоадресного режима 224.0.0.10 и с подтверждением доставки
Периодически каждые 10 сек. с использованием многоадресного режима 224.0.0.5 и без подтверждения доставки
Периодически каждые 30 сек. с использованием многоадресного режима 224.0.0.5 и без подтверждения доставки
Периодически каждые 30 сек. с использованием широковещательных адресов 255.255.255.255 и с подтверждением доставки

Задача 5.8
Вариант 1 Задачи 5.8

157. При конфигурировании протокола OSPF

```
Router_B(config)#router ospf 1
Router_B(config-router)#network 192.168.1.32 0.0.0.31 area 0
Router_B(config-router)#network 200.5.5.4 0.0.0.3 area 0
Router_B(config-router)#network 200.5.5.8 0.0.0.3 area 0
Router_B(config-router)#network 210.10.10.20 0.0.0.3 area 0
```

команды **network** задают:

Адреса удаленных сетей назначения с маской
Адреса непосредственно присоединенных сетей с маской
Адреса сетей непосредственно присоединенных к соседнему маршрутизатору
Адреса локальных сетей с маской
Адреса глобальных сетей с маской

Вариант 2 Задачи 5.8

158. При конфигурировании протокола OSPF

```
Router_B(config)#router ospf 1
Router_B(config-router)#network 192.168.1.32 0.0.0.31 area 0
```

```
Router_B(config-router)#network 200.5.5.4 0.0.0.3 area 0
Router_B(config-router)#network 200.5.5.8 0.0.0.3 area 0
Router_B(config-router)#network 210.10.10.20 0.0.0.3 area 0
```

число 1 в первой строке означает:

Номер сети назначения
Номер процесса OSPF
Номер автономной системы
Номер порта
Номер области (area)

Вариант 3 Задачи 5.8

159. При конфигурировании протокола OSPF

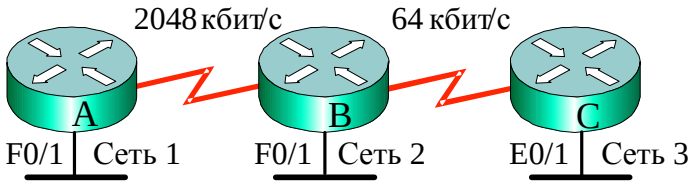
```
Router_B(config)#router ospf 1
Router_B(config-router)#network 192.168.1.32 0.0.0.31 area 0
Router_B(config-router)#network 200.5.5.4 0.0.0.3 area 0
Router_B(config-router)#network 200.5.5.8 0.0.0.3 area 0
Router_B(config-router)#network 210.10.10.20 0.0.0.3 area 0
```

число 0.0.0.3 означает:

Количество локальных сетей в составной сети
Номер автономной системы непосредственно присоединенной сети
Адрес сети непосредственно присоединенной к соседнему маршрутизатору
Инверсную маску непосредственно присоединенной сети
Сетевую маску удаленной сети назначения

Задача 5.9
Вариант 1 Задачи 5.9

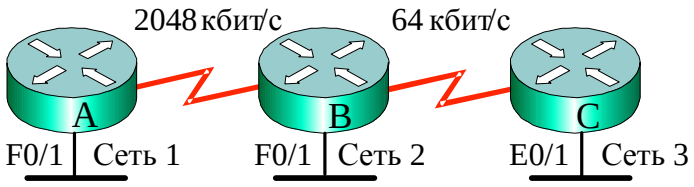
160. Метрика пути из Сети 1 в Сеть 2 (см. рисунок) составляет:



48, 49, 50, 1562, 1573, 1621

Вариант 2 Задачи 5.9

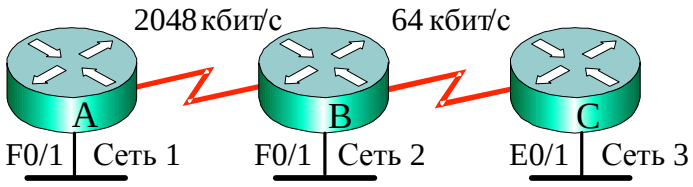
161. Метрика пути из Сети 2 в Сеть 3 (см. рисунок) составляет:



48, 49, 50, 1562, 1573, 1621

Вариант 3 Задачи 5.9

162. Метрика пути из Сети 3 в Сеть 1 (см. рисунок) составляет:



48, 49, 50, 1562, 1573, 1621

Задача 5.10
Вариант 1 Задачи 5.10

163. В строке таблицы маршрутизации

O 192.168.4.48 [110/2344] via 200.50.50.10, 00:00:10, Serial1/1

число 2344 в квадратных скобках означает:

Число переходов до сети назначения
Маршрут создан протоколом EIGRP
Маршрут создан администратором
Метрика пути до сети назначения
Сеть назначения недостижима

Вариант 2 Задачи 5.10

164. В строке таблицы маршрутизации

O 192.168.4.48 [110/2344] via 200.50.50.10, 00:00:10, Serial1/1

запись via 200.50.50.10 означает:
Адрес сети назначения
Адрес выходного интерфейса маршрутизатора на пути к сети назначения
Адрес входного интерфейса соседнего маршрутизатора на пути к сети назначения
Адрес запасного пути (feasible succcessor) к сети назначения
Адрес преемника (succcessor)

Вариант 3 Задачи 5.10

165. В таблице маршрутизации нижеприведенная запись означает:

O 192.168.4.48 [110/2344] via 200.50.50.10, 00:00:10, Serial1/1
[110/2344] via 200.10.10.18, 00:00:10, Serial1/0

До сети назначения имеется два равнозначных пути
Первая строка показывает основной, а вторая – запасной путь к сети назначения
Первая строка создана протоколом OSPF, а вторая – другим, с меньшим административным расстоянием
Путь к сети назначения лежит через входной интерфейс Serial1/1 (*succcessor*)
Путь к сети назначения лежит через входной интерфейс Serial1/0 (*succcessor*)

РАЗДЕЛ 6. ВОПРОСЫ БЕЗОПАСНОСТИ СЕТЕЙ НА МАРШРУТИЗАТОРАХ И КОММУТАТОРАХ

Лекция 13. СЕТЕВЫЕ ФИЛЬТРЫ

Краткая аннотация лекции: Рассмотрены принципы функционирования сетевых фильтров. Приведены примеры конфигурирования стандартных, расширенных, именованных списков доступа. Даны команды верификации и отладки сетевых фильтров.
Цель лекции: изучить основы защиты сетей путем управления потоком данных с помощью списков доступа.

Информационная безопасность телекоммуникационных сетей обеспечивается комплексом мер по их защите. Для защиты информации широко используются пароли, криптографирование передаваемой информации, устройства физической безопасности и другие аппаратные и программные средства. В настоящем разделе рассматриваются только некоторые методы и средства защиты сетей от несанкционированного доступа: сетевые фильтры (списки доступа), средства защиты портов коммутаторов, использование виртуальных локальных сетей. Однако эти меры весьма эффективны и применяются практически на всех сетях.

13.1. Функционирование списков доступа

Сетевой администратор должен иметь возможность управления трафиком, обеспечивая доступ к требуемым ресурсам зарегистрированным пользователям и запрещая несанкционированный доступ к сети. Эффективным средством фильтрации трафика являются **списки контроля доступа** (Access Control Lists – **ACL**). Их также называют **сетевые фильтры** или просто **списки доступа**. Списки доступа используются, чтобы **разрешать** (**permit**) или **запрещать** (**deny**) продвижение пакетов через маршрутизатор, т.е. разрешать или запрещать доступ информации из других локальных сетей или из Интернета в защищаемую сеть, а также удаленный доступ по командам Telnet.

Списки доступа ACL могут быть созданы для всех сетевых протоколов, функционирующих на маршрутизаторе, например, IP или IPX, и устанавливаются на интерфейсах маршрутизаторов. **Запрет или разрешение** сетевого трафика через интерфейс маршрутизатора реализуется на основании

анализа *совпадения* определенных *условий*. Для этого списки доступа представляются в виде последовательных записей, в которых анализируются используемые адреса и протоколы. Сетевые фильтры (списки доступа) создаются как для **входящих,** так и для **исходящих** пакетов на основании **анализируемых параметров (адреса источника**, **адреса назначения**, используемого **протокола** и **номера порта верхнего уровня)**, указанных в списке доступа ACL (рис. 13.1).

Списки доступа могут быть определены для каждого установленного на интерфейсе протокола и для каждого направления сетевого трафика (исходящего и входящего). Поэтому для входящего и исходящего трафиков через интерфейс создаются отдельные списки. Например, для двух интерфейсов маршрутизатора, сконфигурированных для трех протоколов (IP, AppleTalk и IPX), может быть создано 12 отдельных списков доступа (на каждом интерфейсе по 6 списков: 3 для входящего и 3 для исходящего трафика).

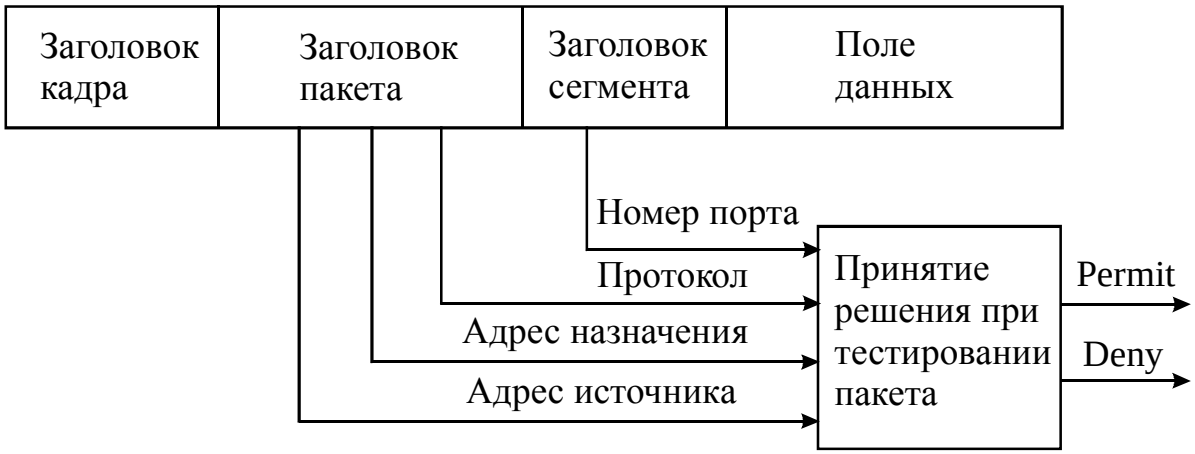


Рис. 13.1. Принятие решения при тестировании пакета

Списки доступа повышают гибкость сети. Например, списки, ограничивающие видео трафик, могут уменьшить нагрузку сети и повысить ее пропускную способность для передачи данных или аудио сигналов. Можно определить, какие типы трафика могут быть отправлены, а какие заблокированы в интерфейсах маршрутизатора, например, можно разрешить маршрутизацию электронной почте, но блокировать трафик Telnet. Можно использовать разрешение или запрет доступа различным типам файлов, таким как FTP или HTTP.

Если списки доступа не формируются на маршрутизаторе, то все проходящие через маршрутизатор пакеты, будут иметь доступ к сети.

Список доступа ACL составляется из **утверждений** (**условий**), которые определяют, следует ли пакеты принимать или отклонять во входных или выходных интерфейсах маршрутизатора. Программное обеспечение IOS Cisco проверяет пакет последовательно по каждому условию. Если условие, разрешающее продвижение пакета, расположено наверху списка, никакие условия, добавленные ниже его, не будут запрещать продвижение пакета. **Если в списке доступа необходимы дополнительные условия, то список целиком должен быть удален и создан новый с новыми условиями.**

Функционирование маршрутизатора по проверке соответствия принятого пакета требованиям списка доступа производится следующим образом. Когда кадр поступает на интерфейс, маршрутизатор проверяет MAC-адрес. Если адрес назначения соответствует адресу интерфейса, то маршрутизатор извлекает (декапсулирует) из кадра пакет и проверяет его на соответствие условиям списка ACL входного интерфейса. При отсутствии запрета или отсутствии списка доступа пакет инкапсулируется в новый кадр второго уровня модели OSI и отправляется интерфейсу следующего устройства.

Проверка условий (утверждений) списка доступа производится последовательно. Если текущее утверждение верно, пакет обрабатывается в соответствие с командами **`permit`** или **`deny`** списка доступа, остальная часть условий ACL не проверяется. Если все утверждения ACL неверны, то неявно заданная по умолчанию команда **`deny any`** (**запретить все остальное**) в конце списка не позволит передавать дальше по сети несоответствующие пакеты.

Существуют разные типы списков доступа: стандартные (standard ACLs), расширенные (extended ACLs), именованные (named ACLs). Когда список доступа конфигурируются на маршрутизаторе, каждый список должен иметь уникальный **идентификационный номер**. Это число идентифицирует тип созданного списка доступа и должно находиться в пределах определенного диапазона, заданного для этого типа списка (табл.13.1).

Таблица 13.1

Диапазоны идентификационных номеров списков доступа

Диапазон номеров	Название списка доступа
1-99	IP standard access-list
100-199	IP extended access-list
1300-1999	IP standard access-list (extended range)
2000-2699	IP extended access-list (extended range)
600-699	Appletalk access-list
800-899	IPX standard access-list
900-999	IPX extended access-list

Стандартные списки доступа (Standard access lists) – для принятия решения в IP пакете анализируется только адрес источника сообщения, чтобы фильтровать сеть.

Расширенные списки доступа (Extended access lists) проверяют как IP-адрес источника, так и IP-адрес назначения, поле протокола в заголовке пакета Сетевого уровня и номер порта в заголовке Транспортного уровня.

Таким образом, для каждого протокола, для каждого направления трафика и для каждого интерфейса может быть создан свой список доступа. Исходящие фильтры не затрагивают трафик, который идет из местного маршрутизатора.

Стандартные списки доступа рекомендуется устанавливать по возможности ближе к адресату назначения, а расширенные – ближе к источнику. То есть стандартные списки доступа должны блокировать устройство назначения и располагаться поближе к защищаемой сети, а расширенные списки устанавливаются ближе к источнику сообщений.

Список доступа производит фильтрацию пакетов по порядку, поэтому в строках списков следует задавать условия фильтрации, начиная от специфических условий до общих. Условия списка доступа обрабатываются последовательно от вершины списка к основанию, пока не будет найдено соответствующее условие. Если никакое условие не найдено, то тогда пакет отклоняется и уничтожается, поскольку **неявное условие `deny any`** (запретить все остальное) есть неявно в конце любого списка доступа. Не удовлетворяющий списку доступа пакет протокола IP будет отклонен и уничтожен, при этом отправителю будет послано сообщение протокола ICMP. Новые записи (линии) всегда добавляются в конце списка доступа.

13.2. Конфигурирование стандартных списков доступа

Конфигурирование списков доступа производится в два этапа:

1. **Создание списка доступа** в режиме глобального конфигурирования.
2. **Привязка списка доступа к интерфейсу** в режиме детального конфигурирования интерфейса.

Формат команды создания стандартного списка доступа следующий:

```
Router(config)#access-list {№} {permit или deny} {адрес источника}.
```

Списки доступа могут фильтровать как трафик, входящий в маршрутизатор (**in**), так и трафик, исходящий из маршрутизатора (**out**). Направление трафика указывается при привязке списка доступа к интерфейсу. Формат команды привязки списка к интерфейсу следующий:

```
Router(config-if)#{протокол} access-group {номер} {in или out}
```

После привязки списка доступа его содержимое не может быть изменено. Не удовлетворяющий администратора список доступа должен быть удален командой **no access-list** и затем создан заново.

Ниже приведены примеры конфигурирования стандартных списков доступа по защите Сети 1 (рис. 13.2).

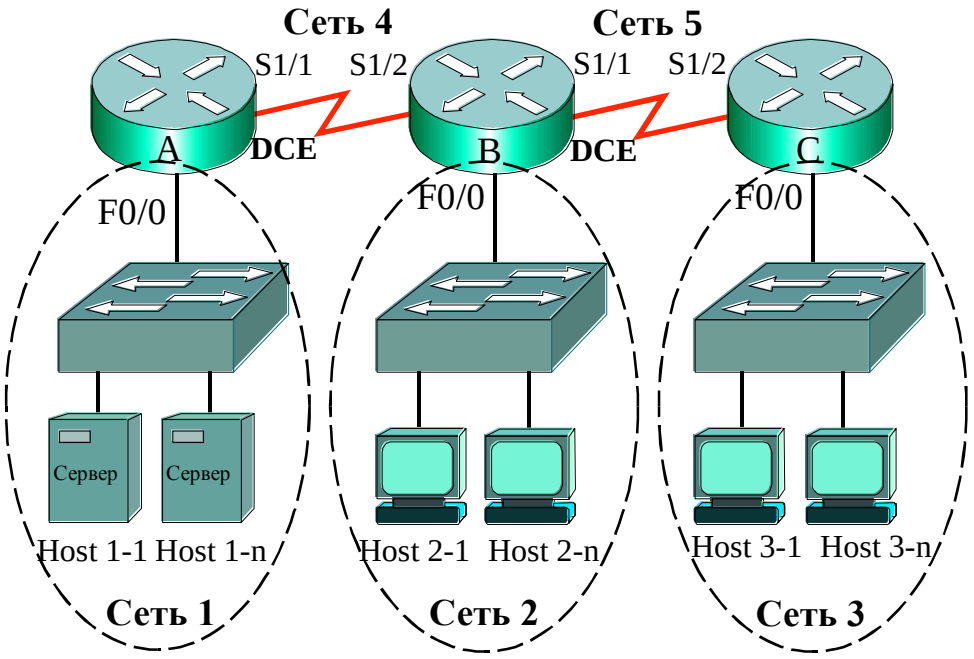


Рис. 13.2. Схема сети

Пример 1. Необходимо, чтобы серверы Сети 1 были доступны только узлу Host 2-1 Сети 2 с адресом 192.168.20.11, а все остальные узлы Сети 2 и Сети 3 не имели бы доступа в Сеть1. Список доступа следует установить на интерфейс F0/0 маршрутизатора Router_A. Номер списка доступа (10) выбирается из диапазона табл. 13.1. Адреса сетей, а также названия и адреса интерфейсов приведены в табл. 13.2.

Таблица 13.2

Адреса сетей и интерфейсов маршрутизаторов

	IP-адрес сети	Интерфейсы	IP-адрес интерфейса
Сеть 1	192.168.10.0/24	F0/0	192.168.10.1
Сеть 2	192.168.20.0/24	F0/0	192.168.20.1
Сеть 3	192.168.30.0/24	F0/0	192.168.30.1
Сеть 4	200.40.40.0/24	S1/1	200.40.40.11
		S1/2	200.40.40.12
Сеть 5	200.50.50.0/24	S1/1	200.50.50.11
		S1/2	200.50.50.12

Создание и установка списка доступа производится по командам:

```
Router_A(config)#access-list 10 permit 192.168.20.11
Router_A(config)#int f0/0
Router_A(config-if)#ip access-group 10 out
```

Согласно созданной конфигурации ко всем исходящим из маршрутизатора пакетам через интерфейс F0/0 будет применяться список доступа:

`permit 192.168.20.11` – присутствует в списке в явном виде,

`deny any` – присутствует неявно в конце каждого списка доступа.

Некоторые версии операционных систем IOS маршрутизаторов требуют в обязательном порядке использование инверсных масок WildCard при задании адресов узлов и сетей, либо расширения host при задании адресов узлов. Подобные дополнения рассмотрены в следующих примерах.

Пример 2. Серверы Сети 1 должны быть доступны всем узлам Сети 2 и узлу Host 3-1 Сети 3 с адресом 192.168.30.11, остальные узлы Сети 3 не должны иметь доступа. Список доступа установить на интерфейс F0/0 Router_A. В списке доступа имеются адреса сети и отдельного узла, поэтому необходимо использовать маску WildCard. Нулевые значения маски WildCard означают требование обработки соответствующих разрядов адреса, а

единичные значения – игнорирование соответствующих разрядов адреса при функционировании списка доступа. Таким образом, маска **0.0.0.0** предписывает анализ и обработку всех разрядов адреса, т.е. в этом случае будет обрабатываться адрес узла. Маска **0.0.0.255** показывает, что обрабатываться будет только сетевая часть адреса класса С.
Следовательно, список доступа будет следующим:

```
Router_A(config)#access-list 11 permit 192.168.30.11 0.0.0.0
Router_A(config)#access-list 11 permit 192.168.20.0 0.0.0.255
Router_A(config)#int f0/0
Router_A(config-if)#ip access-group 11 out
```

Согласно созданной конфигурации ко всем исходящим из маршрутизатора пакетам через интерфейс f0/0 будет применяться список доступа:
permit 192.168.30.11 0.0.0.0 – разрешение доступа узлу в Сеть 1,
permit 192.168.20.0 0.0.0.255 – разрешение доступа всем узлам Сети 2 в Сеть 1,
deny any – присутствует неявно в конце списка доступа.

Записи **192.168.30.11 0.0.0.0** полностью соответствует другой вариант – **host 192.168.30.11**, который также предписывает обрабатывать адрес только одного узла.

Пример 3. В Сети рис.13.2 необходимо установить список доступа, который:

1. блокирует рабочей станции 192.168.20.11 Сети 2 доступ в Сеть1;
2. блокирует рабочей станции 192.168.30.24 Сети 3 доступ в Сеть1;

Для этого создается список доступа:

```
Router_A(config)#access-list 12 deny host 192.168.20.11
Router_A(config)#access-list 12 deny host 192.168.30.24
Router_A(config)#access-list 12 permit any
Router_A(config)#int f0/0
Router_A(config-if)#ip access-group 12 out
```

Данный список блокирует доступ в Сеть 1 только двум рабочим станциям 192.168.20.11 и 192.168.30.24, а всем остальным – доступ разрешен. Если бы отсутствовала третья строка списка доступа, то ни одна станция из других сетей не могла бы попасть в Сеть 1.

13.3. Конфигурирование расширенных списков доступа

В отличие от стандартных списков доступа, где в качестве критерия фильтрации только один параметр – адрес источника, **расширенные списки используют несколько параметров**:

- адрес источника,
- адрес назначения,
- протокол,
- порт.

Формат команды создания расширенного списка доступа следующий:

```
Router(config)#access-list {номер} {permit или deny}
{протокол} {адрес источника} {адрес назначения} {порт}
```

В поле протокола задается имя или номер (0 – 255) протокола сети Интернет. Наиболее часто используются протоколы IP, TCP, UDP, OSPF, RIP и др. Поле порта используется либо для задания номера (0 – 65535), либо – имени портов, например, FTP или Telnet.

Формат команды привязки списка доступа к интерфейсу аналогичен команде стандартного списка:

```
Router(config-if)#{протокол} access-group {номер} {in или out}
```

Пример 4. В сети (рис. 13.2) необходимо:

1. разрешить одной рабочей станции 192.168.30.11 Сети 3 доступ к серверу с адресом 192.168.10.25 Сети 1 с адресом порта 8080;
2. разрешить всем рабочим станциям Сети 2 с адресом 192.168.20.0 доступ к тому же серверу;
3. разрешить всем рабочим станциям доступ ко всем Web-серверам Сети

Для этого создается список доступа:

```
Router_A(config)#access-list 110 permit tcp host
192.168.30.11 host 192.168.10.25 eq 8080
Router_A(config)#access-list 110 permit tcp 192.168.20.0
0.0.0.255 host 192.168.10.25 eq 8080
Router_A(config)#access-list 110 permit tcp any any eq WWW
Router_A(config)#int f0/0
Router_A(config-if)#ip access-group 110 out
```

Запись **any** (все) эквивалентна записи **0.0.0.0 255.255.255.255**, т.е. ни один бит адреса не должен анализироваться. Следовательно, в третьем условии Примера 4 записано требование, исключить фильтрацию по адресу источника и адресу назначения, т.е. запись **permit tcp any any** означает «разрешить доступ всем сегментам tcp ко всем узлам сети». Единственный критерий фильтрации – это **порт eq WWW.**

Запись **eq** означает требование анализа пакетов только с данным номером порта назначения. Вместо нее могла быть другая запись, например, **neq**, означающая требование анализа пакетов с другими номерами, за исключением данного. Запись **range** означает требование анализа пакетов с номерами портов в указанном диапазоне.

Пример 5. Необходимо в сети (рис.13.2) создать список доступа, чтобы:

1. блокировать рабочей станции 192.168.20.11 Сети 2 доступ по telnet в Сеть 1, но оставить доступ для другого сервиса;
2. блокировать рабочей станции 192.168.30.24 Сети 3 доступ по telnet в Сеть 1, но оставить доступ для другого сервиса;

Для этого создается список доступа:

```
Router_A(config)#access-list 115 deny tcp host
192.168.20.11 192.168.10.0 0.0.0.255 eq telnet
Router_A(config)#access-list 115 deny tcp host
192.168.30.24 192.168.10.0 0.0.0.255 eq telnet
Router_A(config)#access-list 115 permit ip any any
Router_A(config)#int f0/0
Router_A(config-if)#ip access-group 115 out
```

Удаление списков доступа производится с использованием отрицания **no.** Например, удаление списка доступа из предыдущего примера производится по команде:

```
RouterA(config)#no access-list 115
```

Именованные списки доступа

Именованные списки доступа позволяют за счет введения имени списка сократить затем объем записей при конфигурировании. Кроме того, снимаются ограничения в 99 стандартных и 100 номеров расширенных списков, поскольку имен можно придумать много. Именованный список доступа с именем **spisok** для вышеприведенного примера 4 будет выглядеть следующим образом:

```
Router_A(config)#access-list extended spisok
Router_A(config-ext-nac1)#permit tcp host 192.168.30.11
host 192.168.10.25 eq 8080
Router_A(config-ext-nac1)#permit tcp 192.168.20.0 0.0.0.255
host 192.168.10.25 eq 8080
Router_A(config-ext-nac1)#permit tcp any any eq WWW
Router_A(config-ext-nac1)#exit
Router_A(config)#int f0/0
Router_A(config-if)#ip access-group spisok out
```

Контроль списков доступа

Контроль списков доступа производится по командам **show**. Например, контроль любых списков доступа производится по команде:

```
RouterA#show access-list
Extended IP access list 110
permit tcp host 192.168.30.11 host 192.168.10.25 eq 8080
(34 matches)
permit tcp 192.168.20.11 0.0.0.255 host 192.168.10.25 eq
8080 (11 matches)
permit tcp any any eq WWW (29 matches)
```

Контроль IP-списков доступа производится по команде:

```
RouterA#show ip access-list
```

Списки доступа, установленные на интерфейсы, можно посмотреть по команде **show ip interface**, а также **show running-config**.

Краткие итоги лекции 13

1. Для защиты информации широко используются сетевые фильтры или списки доступа **(**Access Lists – ACL**)**.
2. Списки доступа могут использоваться, чтобы разрешать (permit) или запрещать (deny) продвижение пакетов через маршрутизатор.
3. Запрет или разрешение сетевого трафика через интерфейс маршрутизатора реализуется на основании анализа совпадения определенных условий.
4. В списке доступа ACL могут анализироваться адреса источника, адреса назначения, протокол и номера порта верхнего уровня.
5. Списки доступа могут быть определены для каждого установленного на интерфейсе протокола и для каждого направления сетевого трафика (исходящего и входящего).
6. Каждый список должен иметь уникальный идентификационный номер.
7. Стандартные списки доступа (Standard access lists) для принятия решения анализируют в IP пакете только адрес источника сообщения.
8. Расширенные списки доступа (Extended access lists) проверяют IP-адрес источника, IP-адрес назначения, поле протокола в заголовке пакета Сетевого уровня и номер порта в заголовке Транспортного уровня.
9. Стандартные списки доступа должны располагаться поближе к защищаемой сети.
10. Расширенные списки доступа должны быть установлены близко к источнику сообщений.
11. Условие `deny any` (запретить все остальное) есть неявно в конце любого списка доступа.
12. Создание списка доступа производится в режиме глобального конфигурирования. Формат команды создания стандартного списка доступа следующий:

```
Router(config)#access-list {№} {permit или deny} {адрес источника}.
```

13. Привязка списка доступа к интерфейсу производится в режиме детального конфигурирования интерфейса. Формат команды привязки списка к интерфейсу следующий:

```
Router(config-if)#{протокол} access-group {номер} {in или out}
```

14. Формат команды создания расширенного списка доступа следующий:

```
Router(config)#access-list {номер} {permit или deny}
{протокол} {адрес источника} {адрес назначения} {порт}
```

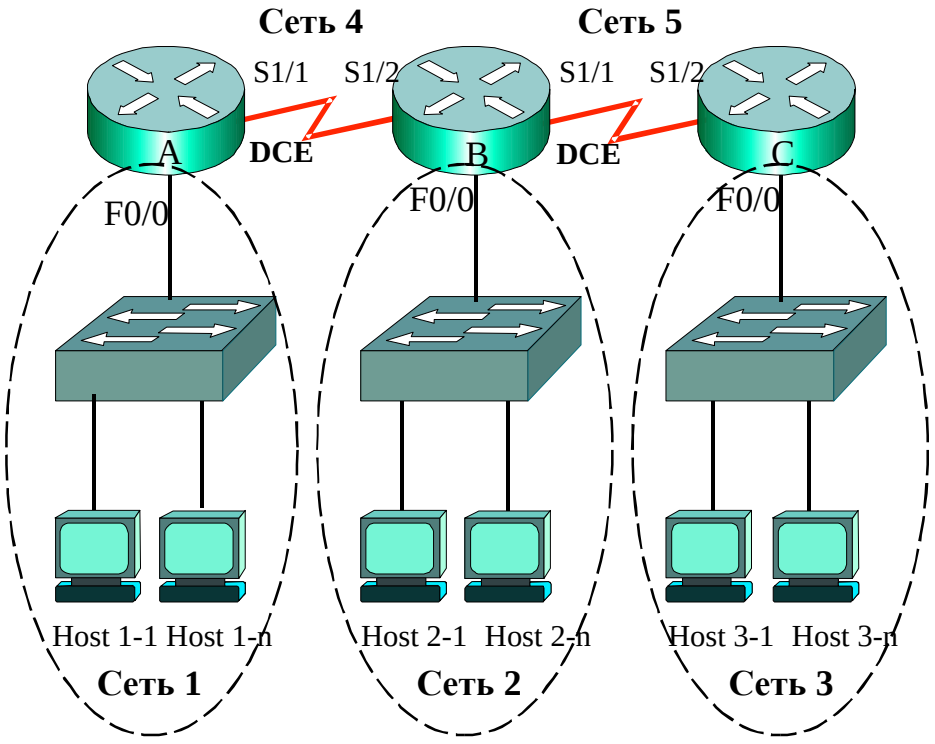
15. Именованные списки доступа позволяют за счет введения имени списка сократить затем объем записи при конфигурировании.

Вопросы по лекции 13

1. Для чего используются сетевые фильтры или списки доступа?
2. На основании чего формируется запрет или разрешение сетевого трафика через интерфейс маршрутизатора?
3. Какие параметры пакета могут анализироваться в списке доступа?
4. Где устанавливаются списки доступа?
5. Что анализируют стандартные списки доступа?
6. Что анализируют расширенные списки доступа?
7. Какое условие имеется неявно в конце любого списка доступа?
8. Для чего нужны идентификационные номера списков доступа?
9. Каков формат команды создания стандартного списка доступа?
10. Каков формат команды создания расширенного списка доступа?
11. Каков формат команды привязки списка к интерфейсу?
12. Какие достоинства имеют именованные списки доступа?

Упражнения

1. Сконфигурируйте список доступа для защиты Сети 1 нижеприведенной схемы от несанкционированного доступа всех узлов Сети 2 и одного узла Host 3-1 Сети 3. Адреса интерфейсов и узлов приведены в таблице.



Наименование	Адрес	Наименование	Адрес
Сеть 1 f0/0 Host 1-1 Host 1-*n*	10.1.10.0/24 10.1.10.1 10.1.10.11 10.1.10.1*n*	Сеть 2 f0/0 Host 2-1 Host 2-*n*	172.16.20.0/24 172.16.20.1 172.16.20.11 172.16.20.1*n*
Сеть 3 f0/0 Host 3-1 Host 3-*n*	192.168.30.0/24 192.168.30.1 192.168.30.31 192.168.30.3*n*	Сеть 4 s1/1 s1/2	204.4.4.0/24 204.4.4.1 204.4.4.2
Сеть 5 s1/1 s1/2	205.5.5.0/24 205.5.5.1 205.5.5.2		

2. Проведите проверку и отладку сети с использованием команд **show running-config**, **`show access-list`**, **`show ip access-list`**, **show ip interface, ping**, **traceroute** и **tracert**.

Лекция 14. БЕЗОПАСНОСТЬ КОММУТАТОРОВ

Краткая аннотация лекции: Приведены особенности конфигурирования коммутаторов, управления таблицей коммутации. Рассмотрены некоторые вопросы конфигурирования безопасности на коммутаторах.
Цель лекции: изучить вопросы конфигурирования коммутаторов.

14.1. Общие вопросы конфигурирования коммутаторов

В отличие от концентраторов коммутаторы делят сеть на домены коллизий и могут работать как в полудуплексном, так и в полнодуплексном режиме, т.е. могут посылать и получать данные одновременно, поэтому исключают коллизии в локальных сетях.

Новые коммутаторы имеют заданную при изготовлении конфигурацию по умолчанию. Эта конфигурация редко удовлетворяет потребности администраторов сети. Коммутаторы могут конфигурироваться и управляться из командной строки интерфейса (command-line interface - **CLI**). Устройства сети могут также конфигурироваться и управляться через базовый web интерфейс и browser.

При включении начинается процесс начальной загрузки (bootup) После того, как коммутатор загрузился, он может конфигурироваться, для чего следует ввести режим глобальный конфигурации и затем установить пароли.

1. После включения на экране появляется следующая информация:

```
1 user(s) now active on Management Console.
        User Interface Menu
     [M] Menus
     [K] Command Line
     [I] IP Configuration
Enter Selection:  K
      CLI session with the switch is open.
      To end the CLI session, enter [Exit].
```

Чтобы войти в CLI (Command Line Interface), нужно выбрать **K**.

Конфигурирование коммутатора похоже на конфигурирование маршрутизатора. Пользовательский режим User EXEC mode характеризуется приглашением в виде символа >. Команды, доступные в пользовательском режиме ограничены, они выполняют основные тесты и отображают основные

установки и параметры коммутатора. В таблице 14.1 приведено описание команд **show**, которые являются доступными в User EXEC mode.

Таблица 14.1

Команды **show**, доступные в пользовательском режиме конфигурирования

n/n	Команда	Описание
1	show version	Дает информацию о программных и аппаратных средствах
2	show flash	Отображает информацию о Флэш-памяти
3	show mac-address-table	Показывает содержимое таблицы коммутации MAC forwarding
4	show controllers ethernet -controller	Показывает отброшенные кадры, отсроченные кадры, ошибки установки, коллизии, и т.д.

Команда **enable** используется, чтобы войти в Привилегированный режим (Privileged EXEC mode) из пользовательского режима. Привилегированный режим характеризуется приглашением в виде символа (#). В этом режиме доступны следующие команды табл.14.2:

Таблица 14.2

Команды **show**, доступные в привилегированном режиме конфигурирования

n/n	Команда	Описание
1	show running-config	Отображает текущий конфигурационный файл коммутатора
2	show post	Отображает тест включения (POST)
3	show vlan	Показывает конфигурацию VLAN
4	show interfaces	Отображает статус и конфигурацию интерфейсов

Набор команд Привилегированного режима включает команду **configure**. Команда **configure** позволяет войти в другие режимы конфигурирования. Поскольку эти режимы используются, чтобы конфигурировать коммутатор, доступ в Привилегированный режим должен быть защищен паролем, чтобы предотвратить неправомочный доступ.

Первое, что необходимо сконфигурировать на любом коммутаторе – это пароли. Пароли можно устанавливать так же, как в маршрутизаторе, для чего нужно войти в привилегированный режим, используя команду **enable**:

```
Switch>enable
```

Второе, следует просмотреть текущую конфигурацию, используя команду **show running-configuration**

```
Switch#sh run
```

Третье, для входа в режим глобального конфигурирования используется команда **configuration terminal**

```
Switch#config t
Switch(config)#
```

Четвертое, необходимо ввести имя коммутатора, используя команду **hostname**, например:

```
Switch(config)#hostname Sw-A
Sw-A(config)#
```

Имена коммутатора, также как маршрутизатора, имеют значение только на локальном уровне.

Пятое, конфигурируется пароль на консоль:

```
Sw-A(config)#line con 0
Sw-A(config-line)#password cisco2
Sw-A(config-line)#login
```

Шестое, для защиты удаленного доступа конфигурируются пароли виртуальных линий 0-15:

```
Sw-A(config-line)#line vty 0 15
Sw-A(config-line)#password cisco3
Sw-A(configline)#login
```

Седьмое, устанавливаются пароли **enable password** или **enable secret password** на вход в привилегированный режим:

```
Sw-A(config)#enable password cisco4
Sw-_A(config)#enable secret cisco1
```

Enable secret password – более строгий пароль, который криптографируется по умолчанию и при установке заменяет пароль **enable password**. Если установлен **enable secret**, то нет необходимости устанавливать пароль привилегированного режима **enable password.**

Для просмотра текущей конфигурации на коммутаторе можно использовать команду **show running-config**:

```
Sw-A #sh run
```

```
Building configuration...
Current configuration:
enable secret 5 $1$FMFQ$wFVYVLYn2aXscfB3J95.w.
```

14.2. Конфигурирование интерфейсов коммутаторов, адресация

Коммутатор может работать по умолчанию без изменения базовой IP-конфигурации. Достаточно включить устройство и оно должно начать работать, точно так же, как это было при использовании концентратора. Однако для управления коммутатором при удаленном доступе к нему, при конфигурировании безопасности, а также при создании виртуальных локальных сетей (VLAN) коммутатором необходимо управлять, для чего задаются IP-адреса, маски, шлюзы, т.е. коммутатор конфигурируется.

Пример конфигурирования коммутатора приведен для схемы рис.14.1, где 3 конечных узла подключены к коммутатору Sw-A через концентратор.

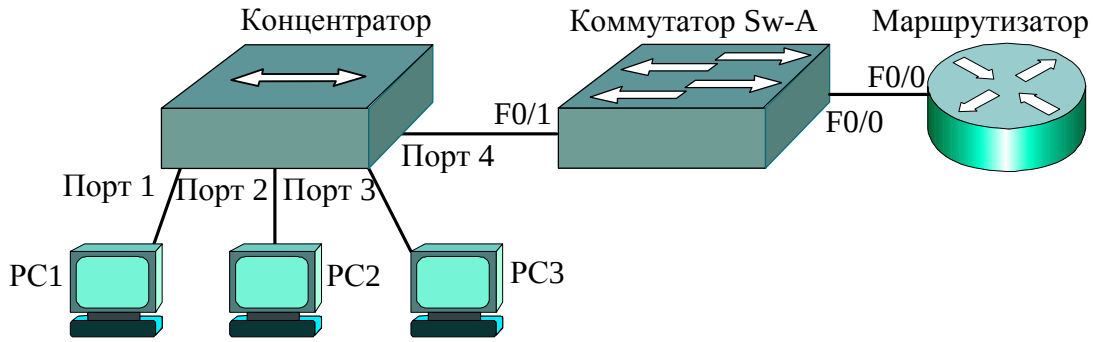


Рис.14.1. Схема сети с коммутатором

По умолчанию на коммутаторе не установлены ни **IP-адрес, ни шлюз по умолчанию**. Для управления коммутатором Catalist 2950 и более поздними образцами введен **интерфейс** виртуальной локальной сети **vlan 1**, на который устанавливается IP-конфигурация. Поэтому на указанном интерфейсе задается IP-адрес, маска сети или подсети, адрес шлюза по умолчанию (default-gateway).

Виртуальная локальная сеть vlan 1 по умолчанию является управляющей, на которую и выполняют атаки хакеры. Поэтому в качестве управляющей рекомендуется использовать виртуальную сеть с другим

номером, например vlan 101, на интерфейс которой устанавливается IP-адрес, например, 10.1.10.11/24. Этот адрес является шлюзом по умолчанию для компьютеров PC1, PC2, PC3. В свою очередь, для коммутатора Sw-A шлюзом будет являться интерфейс F0/0 маршрутизатора с адресом 10.1.10.1. Адреса конечных узлов, маски, а также адрес интерфейса vlan 101 коммутатора сведены в табл. 14.3

Таблица 14.3

Адреса сетей и интерфейсов маршрутизаторов

Устройство		Адрес	Маска	Шлюз
PC1	NIC	10.1.10.21	255.255.255.0	10.1.10.11
PC2	NIC	10.1.10.22	255.255.255.0	10.1.10.11
PC3	NIC	10.1.10.23	255.255.255.0	10.1.10.11
Sw-A	Vlan 101	10.1.10.11	255.255.255.0	10.1.10.1

Таким образом, конфигурирование указанных параметров позволяет реализовать доступ к коммутатору для управления с удаленного устройства, обеспечение безопасности коммутатора, создание виртуальных локальных сетей.

Конфигурирование коммутатора производится в следующей последовательности:

```
Sw-A(config)#vlan 101
Sw-A(config-vlan)#exit
Sw-A(config)#int vlan 101
Sw-A(config-if)#ip add 10.1.10.11 255.255.255.0
Sw-A(config-if)#no shutdown
Sw-A(config-if)#ip default-gateway 192.168.1.1
```

Чтобы изменить IP-адрес и заданный по умолчанию шлюз на коммутаторе, можно либо ввести новый адрес, либо удалить информацию командами глобальной конфигурации **no ip address** или **no ip default-gateway**.

Для верификации конфигурации используется команда **show interface vlan1** в привилегированном режиме:

```
Switch#show interface vlan1
```

Конфигурация коммутатора хранится в NVRAM, также как маршрутизатора. Текущую конфигурацию можно посмотреть по команде **show running-config**.

Для сохранения текущей конфигурации в **NVRAM** администратор может воспользоваться командой **copy running-config startup-config:**

```
Switch#copy run start
```

На коммутаторах Catalist 2950 дуплексный режим и скорость передачи установлены по умолчанию. Однако они могут быть установлены и вручную администратором, если до того дуплексный режим по каким-либо причинам был отменен:

```
Switch(config)#interface FastEthernet0/2
Switch(config-if)#duplex full
Switch(config-if)#speed 100
```

14.3. Управление таблицей коммутации

Коммутаторы изучают MAC-адрес источника кадра, полученного на входной интерфейс, и регистрирует его в таблице коммутации (см. Лекция 4). Кадры, которые имеют MAC-адрес назначения, зарегистрированный в таблице, переключаются только на соответствующий интерфейс без использования широковещательной передачи на все порты. Если в течение 300 секунд с какого либо узла нет передачи кадров, то MAC-адрес такого узла удаляется из таблицы. Не дожидаясь истечения заданного времени, администратор может вручную произвести очистку динамически созданных адресов путем использования команды **clear mac-address-table** в привилегированном режиме.

Таблица коммутации (таблица MAC-адресов) может формироваться, изменяться и дополняться в статическом режиме администратором. При этом повышается безопасность сети. Чтобы сконфигурировать статически MAC-адрес, на заданный интерфейс коммутатора используется команда:

```
Switch(config)#mac-address-table static <MAC-адрес
узла> vlan <имя vlan> interface FastEthernet <номер>
```

Ниже приведен пример конфигурирования некоторого коммутатора Switch, на котором уже были динамически сформированы три строки таблицы с интерфейсами FA0/7, FA0/8 и FA0/9. (Интерфейсы соответственно приписаны к виртуальным сетям vlan 2, vlan 3, vlan 4 – подробнее этот материал приведен в следующей лекции). Таблица коммутации отображается по команде:

```
Switch>sh mac-address-table

          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   2    0060.2f2e.9907    DYNAMIC     Fa0/7
   3    0060.2f2e.9908    DYNAMIC     Fa0/8
   4    0060.2f2e.9909    DYNAMIC     Fa0/9
```

Затем администратором статически конфигурируется новая запись:

```
Switch(config)#mac-address-table static 0030.A3E9.6623 vlan
2 Interface FastEthernet 0/2,
```

которая отображается в таблице коммутации (`Type – STATIC`):

```
Switch#sh mac-address-table

          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   2    0030.a3e9.6623    STATIC      Fa0/2
   2    0060.2f2e.9907    DYNAMIC     Fa0/7
   3    0060.2f2e.9908    DYNAMIC     Fa0/8
   4    0060.2f2e.9909    DYNAMIC     Fa0/9
```

Подобную информацию можно также увидеть по команде **`sh run`**:

```
Switch#sh run
...
mac-address-table static 0030.a3e9.6623 vlan 2
interface FastEthernet0/2
```

Чтобы удалить созданные статически MAC-адреса, нужно использовать следующую команду:

```
Switch(config)#no mac-address-table static <MAC-адрес узла>
interface FastEthernet <номер> vlan <номер>
```

14.4. Конфигурирование безопасности на коммутаторе

Порты коммутатора доступны через структурированную кабельную систему. Любой может подключиться к одному из портов напрямую или через концентратор (рис. 14.1), что является потенциальным пунктом входа в сеть неправомочного пользователя. При этом злоумышленник может сконфигурировать коммутатор так, чтобы он работал как концентратор, что позволяет анализировать весь трафик, проходящий через коммутатор. Поэтому необходимо обеспечивать **безопасность портов** (port security).

Статическое конфигурирование администратором MAC-адресов обеспечивает безопасность путем жесткой привязки адреса к интерфейсу, однако это достаточно сложно. Для обеспечения динамического режима безопасности, когда запись не удаляется автоматически после пяти минут молчания узла, используется ряд команд конфигурирования коммутатора. Например, динамический режим обеспечения безопасности на интерфейсе Fast Ethernet 0/7 конфигурируется следующей последовательностью команд:

```
Switch(config-if)#int f0/7
Switch(config-if)#switchport port-security
```

или последовательностью, используемой в виртуальных локальных сетях

```
Switch(config)#int f0/7
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
```

После ввода указанной последовательности команд таблица коммутации приобретает следующий вид:

```
Switch#sh mac-address-table
          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   2    0030.a3e9.6623    STATIC      Fa0/2
   2    0060.2f2e.9907    STATIC      Fa0/7
   3    0060.2f2e.9908    DYNAMIC     Fa0/8
   4    0060.2f2e.9909    DYNAMIC     Fa0/9
```

То есть автоматически обеспечивается статическая (постоянная) привязка MAC-адреса к интерфейсу коммутатора.

С целью повышения безопасности ограничивают число MAC-адресов узлов, которым разрешено присоединяться к данному интерфейсу коммутатора. Например, **число MAC-адресов на порт может быть ограничено до 1**. В этом случае первый MAC-адрес, динамически изученный коммутатором, считается безопасным адресом, кадры с другими MAC-адресами будут отвергаться.

```
Switch_A#config t
Switch_A(config)#int fa 0/7
Switch_A(config-if)#switchport port-security max 1
```

При увеличении максимального значения до *n* (**max** *n*) безопасными будут считаться первые *n* адресов кадров, поступивших в порт коммутатора.

Верификация режима **port security** конкретного интерфейса обеспечивается командой **show port security,** например:

```
Switch-A#sh port-security int f0/7

Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0060.2F2E.9907:2
Security Violation Count   : 0
```

Третья строка распечатки показывает **режим реагирования** системы на нарушения безопасности, который по умолчанию установлен в состояние «**Выключение**» (**Shutdown**). Нарушение безопасности происходит, когда станция, чей MAC-адрес отсутствует в таблице коммутации, пытается получить доступ к интерфейсу. При этом порт немедленно выключается и формируется сообщение о нарушении безопасности. Существуют еще два режима реагирования на нарушения безопасности: режим защиты (Protect) и режим ограничения (Restrict). В этих режимах пакеты с неизвестными исходящими MAC-адресами уничтожаются. При этом в режиме ограничения

формируется уведомление, а в режиме защиты – не формируется. Установить режим «Выключение» (если он не включен) можно по команде:

```
Switch_A(config-if)#switchport port-security violation shutdown
```

Для повышения безопасности рекомендуется выключить все неиспользуемые порты коммутатора по команде **Shutdown**. Ниже приведен пример фрагмента распечатки команды **sh run**, где показано, что неиспользуемый интерфейс FastEthernet0/10 – выключен.

```
Switch_A#sh run
!
interface FastEthernet0/7
 switchport access vlan 2
 switchport mode access
 switchport port-security
!
interface FastEthernet0/8
 switchport access vlan 3
 switchport mode access!
!
interface FastEthernet0/9
 switchport access vlan 4
 switchport mode access
!
interface FastEthernet0/10
 shutdown
!
interface FastEthernet0/11
!
```

Выключение режима безопасности **port security** обеспечивается формой **no** команды, по которой режим вводился.

Краткие итоги лекции 14

1. Коммутаторы делят сеть на домены коллизий.
2. При конфигурировании коммутатора используются четыре режима: пользовательский, привилегированный, глобального и детального конфигурирования.
3. Многие команды конфигурирования коммутатора аналогичны командам на конфигурирование маршрутизатора.
4. Коммутатором необходимо управлять, для чего задаются IP-адрес, маска, шлюз на интерфейс виртуальной локальной сети vlan 1.
5. Виртуальная локальная сеть vlan 1 по умолчанию является управляющей, на которую и выполняют атаки хакеры. Поэтому в качестве управляющей рекомендуется использовать виртуальную сеть с другим номером, например vlan 101.
6. Кадры, которые имеют MAC-адрес назначения, зарегистрированный в таблице коммутации, переключаются только на соответствующий интерфейс без использования широковещательной передачи на все порты, что повышает безопасность.
7. Формат команды статического конфигурирования MAC-адреса на заданный интерфейс следующий:

   Switch(config)#**mac-address-table static** <*MAC-адрес узла*> **vlan** <*имя vlan*> **interface FastEthernet** <*номер*>

8. Коммутаторы должны обеспечивать безопасность портов (port security).
9. Статическое конфигурирование администратором MAC-адресов обеспечивает безопасность путем жесткой привязки адреса к интерфейсу.
10. Обеспечение безопасности на интерфейсе конфигурируется командой **switchport port-security** в режиме конфигурирования интерфейса.
11. Число MAC-адресов на порт может быть ограничено до одного командой **switchport port-security max 1**.
12. Существуют различные режимы реагирования системы на нарушения безопасности.
13. Для повышения безопасности рекомендуется выключать все неиспользуемые порты коммутатора.

Вопросы по Лекции 14

1. Какие устройства делят сеть на домены коллизий?
2. Какие устройства делят сеть на широковещательные домены?
3. По каким командам конфигурируется IP-адрес и шлюз коммутатора?
4. По какой команде конфигурируется администратором новая запись в таблицу коммутации?
5. По какой команде можно удалить созданные записи таблицы коммутации?
6. По какой команде производится очистка таблицы коммутации?
7. Какие команды используются для установки дуплексного режима и скорости передачи?
8. По какой команде конфигурируется динамический режим обеспечения безопасности на интерфейсе?
9. По какой команде можно посмотреть содержимое таблицы коммутации?
10. Какие команды используются для верификации режима port security?

Упражнения

1. Смоделируйте сеть согласно рис.14.1, табл.14.3.
2. Сконфигурируйте необходимую информацию для управления коммутатором с удаленного устройства, а также пароли.
3. Припишите порт F0/1 коммутатора к виртуальной сети vlan 101:

```
Switch(config)#int f0/1
Switch(config-if)#switchport access vlan 101
```

4. С компьютера PC1 выполните удаленный доступ к коммутатору по команде PC1>**telnet 10.1.10.11**. Измените имя коммутатора, например, на Sw_A. Завершите сеанс удаленного доступа.
5. Проведите проверку таблицы коммутации. Смоделируйте дополнительные динамические записи в таблице коммутации.
6. Сконфигурируйте безопасность порта F0/1 коммутатора.

```
Switch(config-if)#switchport port-security max 1
Switch(config-if)#switchport port-security mac-address sticky
```

7. Выполнить команды **ping 10.1.10.11** последовательно с компьютеров PC1, PC2, PC3. Прокомментировать результаты.

Лекция 15. ВИРТУАЛЬНЫЕ ЛОКАЛЬНЫЕ СЕТИ

Краткая аннотация лекции: Приведены общие сведения о виртуальных локальных сетях, принципы организации транковых соединений. Рассмотрено конфигурирование виртуальных локальных сетей. Маршрутизация между сетями. Верификация и отладка.
Цель лекции: изучить основы создания виртуальных локальных сетей.

15.1. Общие сведения о виртуальных сетях

Безопасность телекоммуникационных сетей во многом определяется размерами широковещательных доменов, внутри которых может происходить несанкционированный доступ к конфиденциальной информации. В традиционных сетях деление на широковещательные домены реализуется маршрутизатором.

Виртуальные сети созданы, чтобы реализовать сегментацию сети на коммутаторах, т.е. на втором уровне модели OSI. Создание виртуальных локальных сетей (Virtual Local Area Networks – **VLAN**), которые представляют собой логическое объединение групп станций сети (рис. 15.1), является одним из основных методов защиты информации в сетях на коммутаторах.

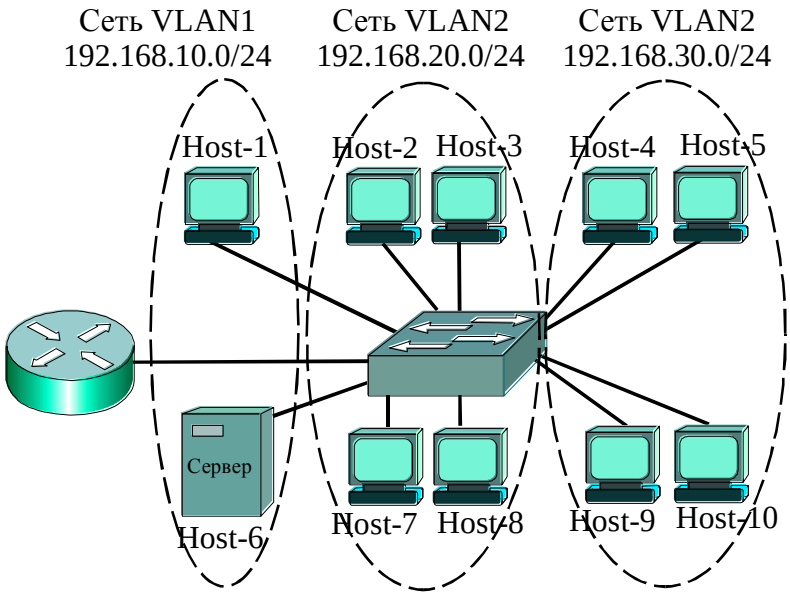


Рис. 15.1. Виртуальные локальные сети VLAN

Обычно VLAN группируются по функциональным особенностям работы, независимо от физического местоположения пользователей. Обмен данными происходит только между устройствами, находящимися в одной

сети VLAN. Обмен данными между различными VLAN производится только через маршрутизаторы.

Рабочая станция в виртуальной сети, например, Host-1 в сети VLAN1 (рис. 15.1), ограничена общением с сервером в той же самой VLAN1. Виртуальные сети логически сегментируют всю сеть на широковещательные домены так, чтобы пакеты переключались только между портами, которые назначены на ту же самую VLAN (приписаны к одной VLAN). Каждая сеть VLAN состоит из узлов, объединенных единственным широковещательным доменом, образованным приписанными к виртуальной сети портами коммутатора.

Поскольку каждая виртуальная сеть представляет широковещательный домен, то маршрутизаторы в топологии сетей VLAN (рис.15.1) обеспечивают фильтрацию широковещательных передач, безопасность, управление трафиком и связь между VLAN. Коммутаторы не обеспечивают трафик между VLAN, поскольку это нарушает целостность широковещательного домена VLAN. **Трафик между VLAN** обеспечивается маршрутизацией, т.е. **общение между узлами разных виртуальных сетей происходит только через маршрутизатор**.

Для нормального функционирования виртуальных сетей необходимо на коммутаторе сконфигурировать все виртуальные локальные сети и приписать порты коммутатора к соответствующей сети VLAN. Если кадр должен пройти через коммутатор и MAC-адрес назначения известен, то коммутатор только продвигает кадр к соответствующему выходному порту. Если MAC-адрес неизвестен, то происходит широковещательная передача во все порты широковещательного домена, т.е. внутри виртуальной сети VLAN, кроме исходного порта, откуда кадр был получен. **Широковещательные передачи снижают безопасность информации.**

Управление виртуальными сетями VLAN реализуется через первую сеть VLAN1 и сводится к управлению портами коммутатора. Сеть VLAN1 получила название **сеть по умолчанию** (**default VLAN**). По крайней мере, один порт должен быть в VLAN 1, чтобы управлять коммутатором. Все другие порты на коммутаторе могут быть назначены другим сетям VLAN. Поскольку данная информация известна всем, то хакеры пытаются атаковать, в первую очередь, именно эту сеть. Поэтому на практике администраторы изменяют номер сети по умолчанию, например, на номер VLAN 101.

Каждой виртуальной сети при конфигурировании должен быть назначен IP-адрес сети или подсети с соответствующей маской, для того чтобы виртуальные сети могли общаться между собой. Например, VLAN1 (рис.15.1) может иметь адрес 192.168.10.0/24, VLAN2 – адрес 192.168.20.0/24, VLAN3 – адрес 192.168.30.0/24. Каждому хосту необходимо задать IP-адрес из диапазона адресов соответствующей виртуальной сети, например, host-1 – адрес 192.168.10.1, host-2 – адрес 192.168.20.1, host-3 – адрес 192.168.20.2, host-7 – адрес 192.168.20.3, host-10 – адрес 192.168.30.4.

Идентификаторы виртуальных сетей (VLAN1, VLAN2, VLAN3 и т.д.) могут назначаться из нормального диапазона 1 – 1005, в котором номера 1002 – 1005 зарезервированы для виртуальных сетей технологий Token Ring и FDDI. Существует также расширенный диапазон идентификаторов 1006 – 4094. Однако для облегчения управления рекомендуется, чтобы сетей VLAN было не более 255 и сети не расширялись вне Уровня 2 коммутатора.

Таким образом, сеть VLAN является широковещательным доменом, созданным одним или более коммутаторами. На рис. 15.2, три виртуальных сети VLAN созданы одним маршрутизатором и тремя коммутаторами. При этом существуют три отдельных широковещательных домена (сеть VLAN1, сеть VLAN2, сеть VLAN3). Маршрутизатор управляет трафиком между сетями VLAN, используя маршрутизацию Уровня 3.

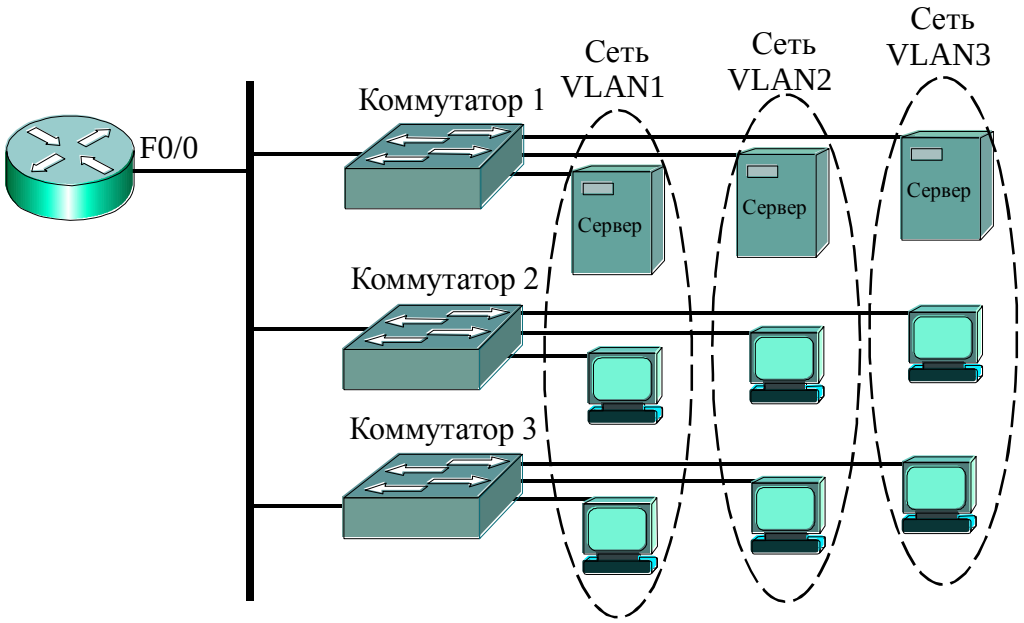


Рис. 15.2. Три виртуальных сети VLAN

Если рабочая станция сети VLAN1 захочет послать кадр рабочей станции в той же самой VLAN1, адресом назначения кадра будет MAC-адрес рабочей станции назначения. Если же рабочая станция сети VLAN1 захочет переслать кадр рабочей станции сети VLAN2, кадры будут переданы на MAC-адрес интерфейса F0/0 маршрутизатора. То есть, маршрутизация производится через IP-адрес интерфейса F0/0 маршрутизатора.

Для выполнения своих функций в виртуальных сетях коммутатор должен поддерживать таблицы коммутации (продвижения) для каждой VLAN. Для продвижения кадров производится поиск адреса в таблице только данной VLAN. Если адрес источника ранее не был известен, то при получении кадра коммутатор добавляет этот адрес в таблицу.

При построении сети на нескольких коммутаторах необходимо выделить дополнительные порты для объединения виртуальных сетей, узлы которых подключены к разным коммутаторам (рис. 15.3). Дополнительных пар портов двух коммутаторов должно быть выделено столько, сколько создано сетей VLAN.

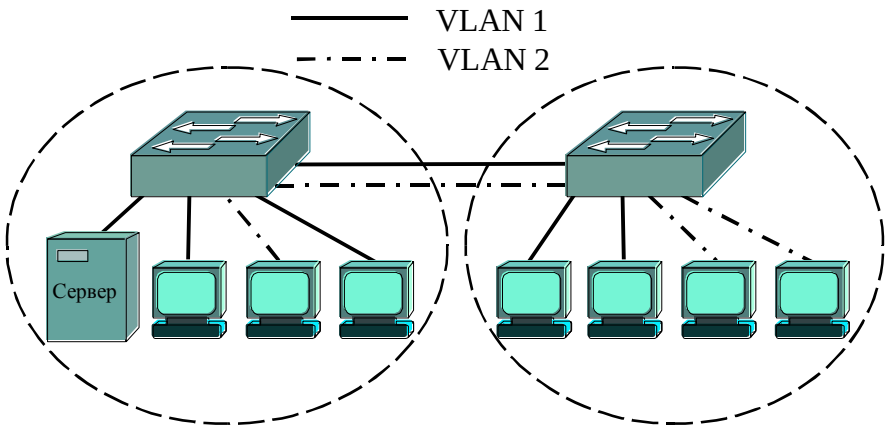


Рис. 15.3. Объединение виртуальных сетей двух коммутаторов

Поскольку кадры данных могут быть получены коммутатором от любого устройства, присоединенного к любой виртуальной сети, то при обмене данными между коммутаторами в заголовок кадра добавляется **уникальный идентификатор** кадра – **тег** (tag) виртуальной сети, который определяет VLAN каждого пакета. **Стандарт IEEE 802.1Q**, определяющий формирование виртуальных сетей, предусматривает введение **поля меток** в заголовок кадра, содержащего два байта (рис. 15.4).

3 бита	1 бит	12 бит
Приоритет	CFI	VLAN ID

Рис. 15.4. Формат тега виртуальной сети

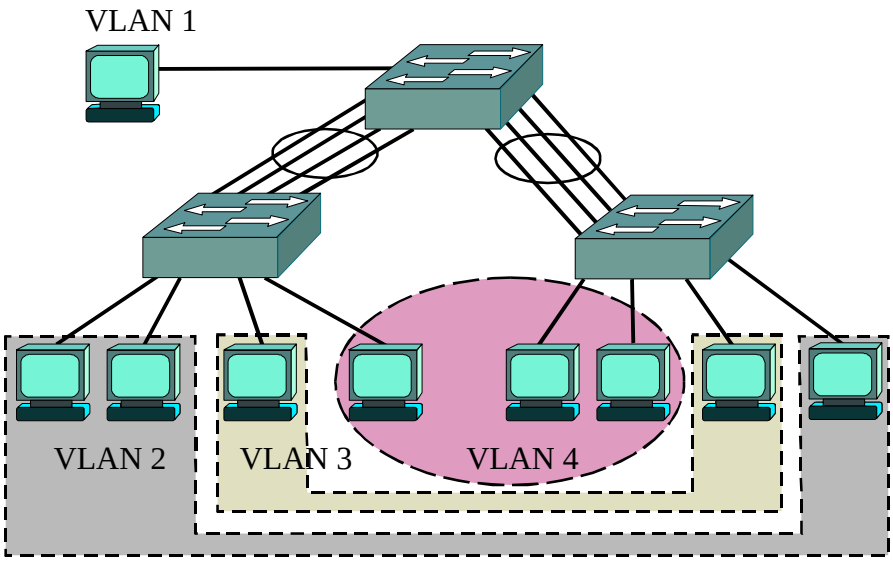
Из них 12 двоичных разрядов используются для адресации VLAN, что позволяет помечать до 4096 виртуальных сетей и соответствует нормальному и расширенному диапазону идентификаторов VLAN. Еще три разряда этого поля позволяют задавать 8 уровней приоритета передаваемых сообщений, т.е. позволяют обеспечивать качество (QoS) передаваемых данных. Наивысший приоритет уровня 7 имеют кадры управления сетью, уровень 6 – кадры передачи голосового трафика, 5 – передача видео. Остальные уровни обеспечивают передачу данных с разным приоритетом. Единичное значение поля CFI показывает, что виртуальная сеть является Token Ring.

Пакет отправляется коммутатором или маршрутизатором, базируясь на идентификаторе VLAN и MAC-адресе. После достижения сети назначения идентификатор VLAN (tag) удаляется из пакета коммутатором, а пакет отправляется присоединенному устройству. **Маркировка пакета** (Packet tagging) обеспечивает механизм управления потоком данных.

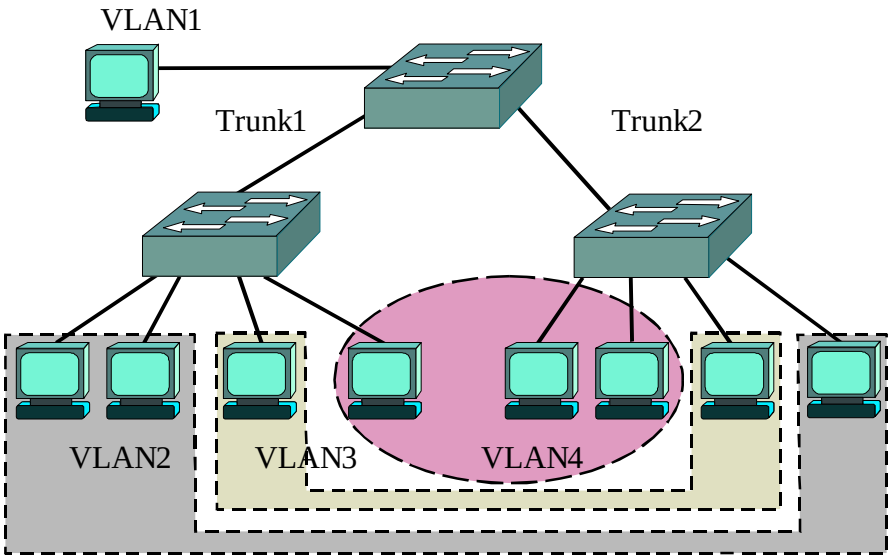
Транковые соединения

Согласно принципу, представленному на рис. 15.3, в виртуальных локальных сетях для соединения нескольких коммутаторов между собой задействуют несколько физических портов. Совокупность физических каналов между двумя устройствами (рис. 15.5 а) может быть заменена одним агрегированным логическим каналом (рис. 15.5 б), получившим название **транк** (**Trunk**). Транк – это канал, передающий кадры множества виртуальных локальных сетей, магистральный канал. Транковые соединения используются и для подключения маршрутизатора к коммутатору (рис. 15.2). При этом на интерфейсе маршрутизатора формируются несколько субинтерфейсов (по количеству виртуальных сетей). Пропускная способность агрегированного логического канала должна быть равна сумме

пропускных способностей физических каналов. Транки используют и для подключения высокоскоростных серверов.



а)



б)

Рис. 15.5. Транковые соединения коммутаторов

На практике используются статические и динамические VLAN. Динамические VLAN создаются через программное обеспечение управления сети. Однако динамические VLAN широко не используется. Наибольшее распространение получили статические VLAN. Входящие в сеть устройства автоматически становятся членами VLAN порта, к которому присоединены. Для статического конфигурирования используется интерфейс командной линии CLI.

15.2. Конфигурирование виртуальных сетей

Конфигурационный файл в виде базы данных **vlan.dat**, хранится во флэш-памяти коммутатора. Каждая VLAN должна иметь уникальный адрес Уровня 3 или выделенный ей адрес подсети. Это позволяет маршрутизаторам переключать пакеты между виртуальными локальными сетями.

Статическое конфигурирование виртуальных сетей сводится к назначению портов коммутатора на каждую виртуальную локальную сеть VLAN, что может непосредственно конфигурироваться на коммутаторе через использование командной строки CLI. Таким образом, при статическом конфигурировании каждый порт приписывается к какой-то виртуальной сети. Статически сконфигурированные порты поддерживают назначенную конфигурацию до тех пор, пока не будут изменены вручную. **Пользователи** подключены к портам коммутатора на **уровне доступа** (access layer). **Маркировка** (Frame tagging) используется, чтобы обмениваться данными, передаваемыми между коммутаторами.

По умолчанию управляющей сетью является первая сеть VLAN 1, однако ей может быть назначен другой номер, причем, сеть VLAN 1 – будет Ethernet сетью, и ей принадлежит IP-адрес коммутатора.

Ниже рассмотрено конфигурирование коммутатора для виртуальной локальной сети (рис. 15.6).

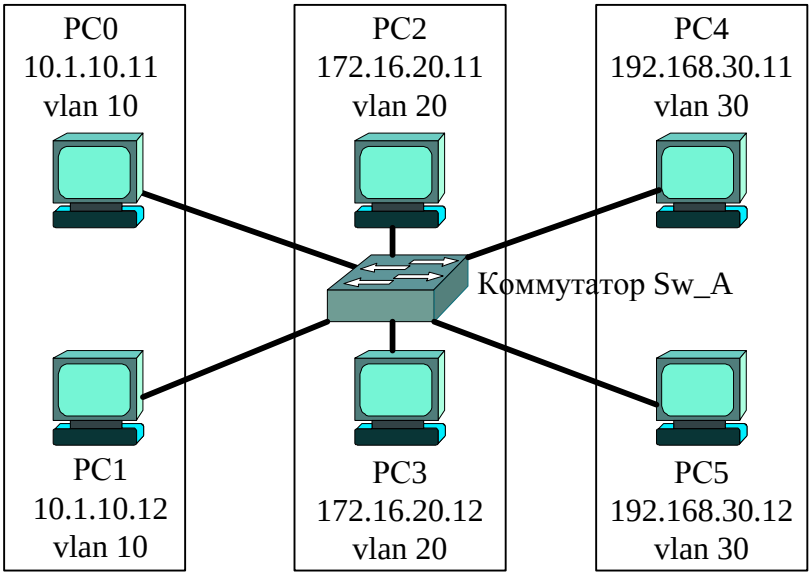


Рис. 15.6. Виртуальная локальная сеть

Примеры конфигурирования даны для коммутаторов серии 2950 и последующих модификаций.

Состояние виртуальных сетей и интерфейсов коммутатора Cisco Catalyst серии 2950-24 с именем **Sw_A** можно посмотреть по следующей команде:

```
Sw_A#sh vlan brief

VLAN  Name                Status    Ports
----  ----------------    --------  -------------------------------
1     default             active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                    Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                    Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                    Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                    Fa0/21, Fa0/22, Fa0/23, Fa0/24
1002 fddi-default         active
1003 token-ring-default   active
1004 fddinet-default      active
1005 trnet-default        active
```

Из распечатки команды `Sw_A#sh vlan brief` следует, что все 24 интерфейса FastEthernet приписаны к сети по умолчанию VLAN 1, других активных виртуальных сетей нет, за исключением 1002 – 1005, зарезервированных для сетей token-ring и fddi.

Создание виртуальных сетей может производиться двумя способами:

1) в режиме глобального конфигурирования;
2) из привилегированного режима конфигурирования по команде **vlan database.**

Примеры конфигурирования трех виртуальных локальных сетей (рис.15.6) vlan 10, vlan 20, vlan 30 приведены ниже:

При первом способе используются следующие команды:

```
Sw-A(config)#vlan 10
Sw-A(config-vlan)#vlan 20
Sw-A(config-vlan)#vlan 30
```

По второму способу:

```
Sw-A#vlan database
Sw-A(vlan)#vlan 10
Sw-A(vlan)#vlan 20
Sw-A(vlan)#vlan 30
```

Программисты Cisco рекомендуют использовать первый способ создания виртуальных локальных сетей.

После создания виртуальных сетей vlan 10, vlan 20, vlan 30 они становятся активными, что можно посмотреть по команде **sh vlan brief**:

```
Sw-A#sh vlan brief

VLAN Name                 Status             Ports
---- -------------------  -------- -------------------------------
1    default              active   Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                   Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                   Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                   Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                   Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                   Fa0/21, Fa0/22, Fa0/23, Fa0/24
10   VLAN0010             active
20   VLAN0020             active
30   VLAN0030             active
1002 fddi-default         active
1003 token-ring-default   active
1004 fddinet-default      active
1005 trnet-default        active
```

При желании можно также сформировать название VLAN по команде **vlan** *№* **name** *имя*, например:

```
Switch2950(config-vlan)#vlan 30 name VLAN30 или
Switch2950(vlan)#vlan 3 name VLAN3
```

Указанные операции не являются обязательными, они служат только для удобства чтения распечаток.

На следующем этапе необходимо назначить виртуальные сети на определенные интерфейсы (приписать интерфейсы к созданным виртуальным сетям), используя пару команд **switchport mode access**, **switchport access vlan** *№*. Ниже приведен пример указанных операций для сети рис.15.6.

```
Sw-A(config)#int f0/1
Sw-A(config-if)#switchport mode access
Sw-A(config-if)#switchport access vlan 10
Sw-A(config-if)#int f0/2
Sw-A(config-if)#switchport mode access
Sw-A(config-if)#switchport access vlan 10
Sw-A(config-if)#int f0/3
```

```
Sw-A(config-if)#switchport mode access
Sw-A(config-if)#switchport access vlan 20
Sw-A(config-if)#int f0/4
Sw-A(config-if)#switchport mode access
Sw-A(config-if)#switchport access vlan 20
Sw-A(config-if)#int f0/5
Sw-A(config-if)#switchport mode access
Sw-A(config-if)#switchport access vlan 30
Sw-A(config-if)#int f0/6
Sw-A(config-if)#switchport mode access
Sw-A(config-if)#switchport access vlan 30
```

Если при конфигурировании нескольких портов режим не изменяется, то команда **switchport mode access** может использоваться один раз для первого интерфейса. Верификацию полученной конфигурации можно произвести с помощью команд **show vlan** или **show vlan brief**, например:

```
Sw-A#sh vlan
VLAN Name                 Status        Ports
---- -----------------  --------    -----------------------------
1    default              active          Fa0/7, Fa0/8, Fa0/9, Fa0/10,
                                          Fa0/11, Fa0/12, Fa0/13, Fa0/14,
                                          Fa0/15, Fa0/16, Fa0/17, Fa0/18,
                                          Fa0/19, Fa0/20, Fa0/21, Fa0/22,
                                          Fa0/23, Fa0/24
10   VLAN0010             active          Fa0/1, Fa0/2,
20   VLAN0020             active          Fa0/3, Fa0/4,
30   VLAN0030             active          Fa0/5, Fa0/6,
1002 fddi-default         active
1003 token-ring-default   active
1004 fddinet-default      active
1005 trnet-default        active

VLAN Type  SAID    MTU  Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2
---- ----- ------  ----  ------ ------ -------  ---- -------- ------ -----
1    enet  100001   1500  -      -      -      -    -        0      0
10   enet  100010   1500  -      -      -      -    -        0      0
20   enet  100020   1500  -      -      -      -    -        0      0
30   enet  100030   1500  -      -      -      -    -        0      0
1002 enet  101002   1500  -      -      -      -    -        0      0
1003 enet  101003   1500  -      -      -      -    -        0      0
1004 enet  101004   1500  -      -      -      -    -        0      0
1005 enet  101005   1500  -      -      -      -    -        0      0
```

Из распечатки следует, что команда **show vlan** дает больше информации, чем **show vlan brief**.

Кроме того, конфигурацию конкретной виртуальной сети, например VLAN2, можно также просмотреть с помощью команд **show vlan id 2** или по имени **show vlan name VLAN2**, если оно задано.

Конфигурационный файл коммутатора должен быть скопирован в энергонезависимую память коммутатора по команде

```
Sw-A#copy running-config startup-config
```

Он может быть также скопирован на сервер TFTP с помощью команды **copy running-config tftp**. Параметры конфигурации можно посмотреть с помощью команд **show running-config** или **show vlan**.

Удаление виртуальной сети, например vlan 10, выполняется с помощью формы **no** команды:

```
Sw-A(config)#no vlan 10
```

или

```
Switch#vlan database
Switch(vlan)#no vlan 10
```

Когда виртуальная локальная сеть удалена, все порты, приписанные к этой VLAN, становятся бездействующими. Однако порты останутся связанными с удаленной виртуальной сетью VLAN пока не будут приписаны к другой виртуальной сети или не будет восстановлена прежняя.

Для того, чтобы отменить неверное назначение интерфейса на виртуальную сеть, например, ошибочное назначение виртуальной сети vlan 20 на интерфейс F0/2, используется команда:

```
Sw-A(config)#int f0/2
Sw-A(config-if)#no switchport access vlan 20
```

Также можно было бы просто приписать интерфейс f0/2 к другой виртуальной сети, например, к vlan 10:

```
Sw-A(config)#int f0/2
Sw-A(config-if)#switchport mode access
Sw-A(config-if)#switch access vlan 10
```

На конечных узлах (хостах) сети рис. 15.6 установлена следующая конфигурация:

Таблица 15.1

Конфигурация конечных узлов виртуальных локальных сетей

VLAN №	Узел	Адрес узла	Маска	Шлюз
Vlan 10	PC0 PC1	10.1.10.11 10.1.10.12	255.255.255.0	10.1.10.1
Vlan 20	PC2 PC3	172.16.20.11 172.16.20.12	255.255.255.0	172.16.20.1
Vlan 30	PC4 PC5	192.168.30.11 192.168.30.12	255.255.255.0	192.168.30.1

Таким образом, каждая виртуальная локальная сеть имеет свой IP-адрес.

Проверка работоспособности сети производится по командам ping, (tracert). Она показывает, что, например, PC0 имеет соединение с PC1:

```
PC0>ping 10.1.10.11

Pinging 10.1.10.11 with 32 bytes of data:

Reply from 10.1.10.11: bytes=32 time=82ms TTL=128
Reply from 10.1.10.11: bytes=32 time=80ms TTL=128
Reply from 10.1.10.11: bytes=32 time=73ms TTL=128
Reply from 10.1.10.11: bytes=32 time=70ms TTL=128

Ping statistics for 10.1.10.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 70ms, Maximum = 82ms, Average = 76ms
```

но PC0 не может обмениваться сообщениями с узлами других VLAN:

```
PC0>ping 172.16.20.11

Pinging 172.16.20.11 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.16.20.11:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

или

```
PC0>ping 192.168.30.12

Pinging 192.168.30.12 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.30.12:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Если к сети присоединить дополнительный узел PC6, адрес которого 192.168.30.101, т.е. адрес его сети совпадает с адресом сети vlan 30, но узел PC6 не приписан ни к одной из виртуальных сетей, то он не сможет реализовать соединения с узлами существующих виртуальных сетей:

15.3. Маршрутизация между виртуальными локальными сетями

Поскольку каждая виртуальная локальная сеть представляет собой широковещательный домен, т.е. сеть со своим IP-адресом, то для связи между сетями необходима маршрутизация Уровня 3. Поэтому к коммутатору необходимо присоединить маршрутизатор (рис.15.7).

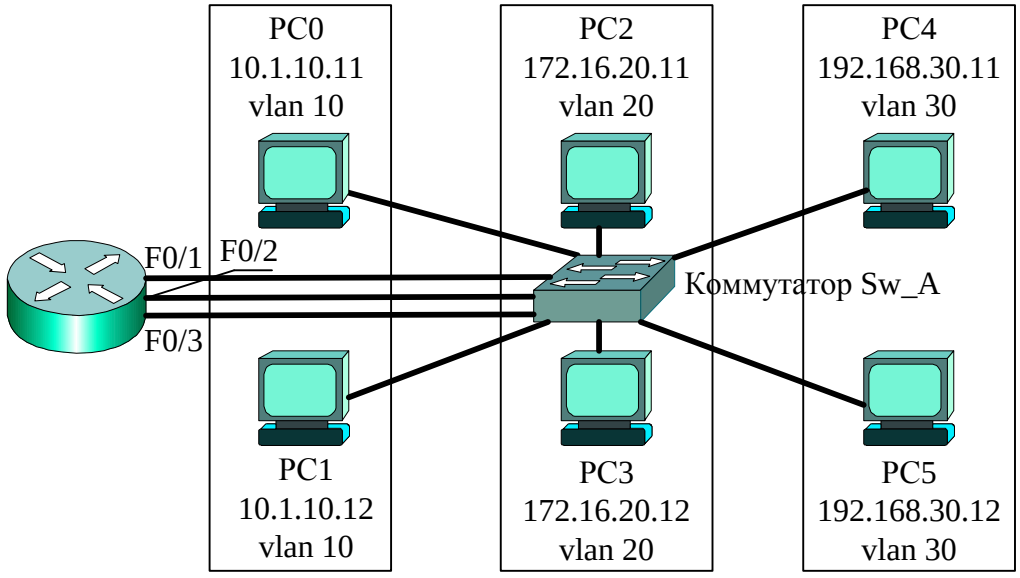


Рис.15.7. Связь между сетями через маршрутизатор

Для соединения с маршрутизатором в схеме дополнительно задействованы три интерфейса коммутатора Sw_A: F0/11, F0/12, Ff0/13.При этом порт F0/11 приписан к сети vlan 10, порт F0/12 – к vlan 20, порт F0/13 – к vlan 30.

```
Sw_A(config)#int f0/11
Sw_A(config-if)#switchport access vlan 10
Sw_A(config-if)#int f0/12
Sw_A(config-if)#switchport access vlan 20
Sw_A(config-if)#int f0/13
Sw_A(config-if)#switchport access vlan 30
```

На маршрутизаторе используются три интерфейса F0/1, F0/2, F0/3 (по числу виртуальных сетей), которые сконфигурированы следующим образом:

```
Router>ena
Router#conf t
Router(config)#int f0/1
Router(config-if)#ip add 10.1.10.1 255.255.255.0
Router(config-if)#no shut
Router(config-if)#int f0/2
Router(config-if)#ip add 172.16.20.1 255.255.255.0
Router(config-if)#no shut
Router(config)#int f0/3
Router(config-if)#ip add 192.168.30.1 255.255.255.0
Router(config-if)#no shut
```

По команде **sh ip route** можно посмотреть таблицу маршрутизации:

```
Router#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/24 is subnetted, 1 subnets
C       10.1.10.0 is directly connected, FastEthernet0/1
     172.16.0.0/24 is subnetted, 1 subnets
C       172.16.20.0 is directly connected, FastEthernet0/2
C    192.168.30.0/24 is directly connected, FastEthernet0/3
```

Из таблицы маршрутизации следует, что все три сети (10.1.10.0, 172.16.20.0, 192.168.30.0) являются непосредственно присоединенными и, следовательно, могут обеспечивать маршрутизацию между сетями. «Прозвонка» с узла 10.1.10.11 узлов сетей 172.16.20.0, 192.168.30.0 дает положительный результат.

Защита межсетевых соединений через маршрутизатор может быть реализована с помощью сетевых фильтров (списков доступа), которые рассмотрены в Лекции 13.

Недостатком такого метода организации межсетевых соединений является необходимость использования дополнительных интерфейсов коммутатора и маршрутизатора, число которых равно количеству виртуальных сетей. От этого недостатка свободно **транковое** соединение, когда совокупность физических каналов между двумя устройствами может быть заменена одним агрегированным каналом.

Конфигурирование транковых соединений

При транковом соединении коммутатора и маршрутизатора три физических канала между ними (рис. 15.7) заменяются одним агрегированным каналом (рис. 15.8).

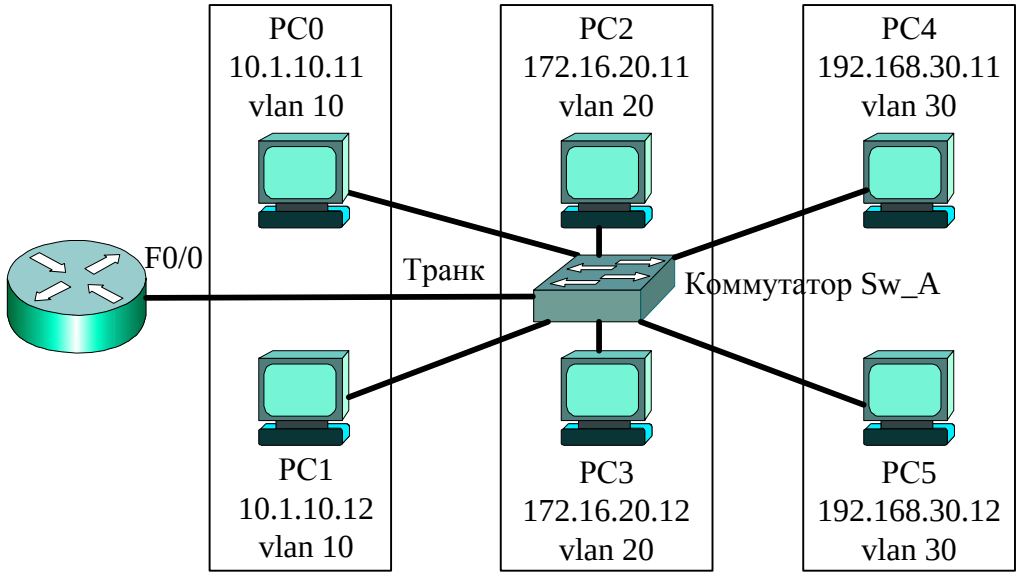


Рис. 15.8. Транковое соединение коммутатора и маршрутизатора

Для создания транкового соединения на коммутаторе задействован интерфейс F0/10, а на маршрутизаторе – F0/0.

Конфигурирование коммутатора будет следующим:

```
Sw_A>ena
Sw_A#conf t
Sw_A(config)#vlan 10
Sw_A(config-vlan)#vlan 20
Sw_A(config-vlan)#vlan 30
Sw_A(config-vlan)#int f0/1
Sw_A(config-if)#switchport mode access
Sw_A(config-if)#switchport access vlan 10
Sw_A(config-if)#int f0/4
Sw_A(config-if)#switchport access vlan 10
Sw_A(config-if)#int f0/2
Sw_A(config-if)#switchport access vlan 20
Sw_A(config-if)#int f0/5
Sw_A(config-if)#switchport access vlan 20
Sw_A(config-if)#int f0/3
Sw_A(config-if)#switchport access vlan 30
Sw_A(config-if)#int f0/6
Sw_A(config-if)#switchport access vlan 30
Sw_A(config-if)#int f0/10
Sw_A(config-if)#switchport mode trunk
Sw_A(config-if)#^Z
```

По команде **sh int f0/10 switchport** можно посмотреть состояние интерфейса:

```
Sw_A#sh int f0/10 switchport
Name: Fa0/10
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
 . . .
Sw_A#
```

Из распечатки следует, что порт F0/10 находится в режиме Trunk.

Конфигурирование маршрутизатора сводится к тому, что на его интерфейсе F0/0 формируются субинтерфейсы F0/0.10, F0/0.20, F0/0.30. На указанных субинтерфейсах задается протокол Dot 1q для виртуальных сетей 10, 20, 30. Последовательность команд необходимо завершить включением интерфейса **no shut**.

```
Router>ena
Router#conf t
Router(config-if)#int f0/0.10
Router(config-subif)#encapsulation dot1q 10
Router(config-subif)#ip add 10.1.10.1 255.255.255.0
Router(config-subif)#int f0/0.20
Router(config-subif)#encapsulation dot1q 20
Router(config-subif)#ip add 172.16.20.1 255.255.255.0
Router(config-subif)#int f0/0.30
Router(config-subif)#encapsulation dot1q 30
Router(config-subif)#ip add 192.168.30.1 255.255.255.0
Router(config-subif)#int f0/0
Router(config-if)#no shut
```

Результат конфигурирования проверяется по команде **sh ip route**:

```
Router#sh ip route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/24 is subnetted, 1 subnets
C    10.1.10.0 is directly connected, FastEthernet0/0.10
     172.16.0.0/24 is subnetted, 1 subnets
C    172.16.20.0 is directly connected, FastEthernet0/0.20
C       192.168.30.0/24 is directly connected,
FastEthernet0/0.30
Router#
```

Из таблицы маршрутизации следует, что сети 10.1.10.0, 172.16.20.0, 192.168.30.0 являются непосредственно присоединенными. Поэтому маршрутизатор способен обеспечить маршрутизацию между сетями.

Краткие итоги лекции 15

1. Виртуальная локальная сеть VLAN состоит из узлов, объединенных единственным широковещательным доменом, образованным приписанными к виртуальной сети портами коммутатора.
2 Для функционирования VLAN необходимо на коммутаторе сконфигурировать все виртуальные локальные сети и приписать порты коммутатора к соответствующей сети.
8. Трафик между VLAN обеспечивается маршрутизацией, т.е. общение между узлами разных виртуальных сетей происходит только через маршрутизатор.
9. Управление виртуальными сетями VLAN реализуется через первую сеть VLAN1 и сводится к управлению портами коммутатора. Администраторы обычно изменяют номер сети по умолчанию для повышения безопасности.
10. Каждой виртуальной сети при конфигурировании должен быть назначен IP-адрес сети или подсети с соответствующей маской и шлюзом.
11. При построении сети на нескольких коммутаторах необходимо выделить дополнительные порты для объединения портов разных коммутаторов, приписанных к одноименным виртуальным сетям.
12. При обмене данными между коммутаторами в заголовок добавляется уникальный идентификатор кадра – тег (tag) виртуальной сети, который определяет членство VLAN каждого пакета.
13. Маркировка (Frame tagging) используется для обмена информацией сетей VLAN между коммутаторами.
14. Совокупность физических каналов между двумя устройствами может быть заменена одним агрегированным логическим каналом, получившим название транк (Trunk).
15. Транк – это канал, передающий кадры множества виртуальных локальных сетей, магистральный канал.
16. При транковых соединениях на интерфейсе маршрутизатора формируются несколько субинтерфейсов (по количеству виртуальных сетей).
17. Конфигурирование виртуальных сетей сводится к назначению портов коммутатора на каждую виртуальную локальную сеть VLAN.
18. Приписать интерфейсы к созданным виртуальным сетям) можно, используя пару команд **switchport mode access, switchport access vlan №.**
19. Для создания транкового соединения на интерфейсе коммутатора используется команда **switchport mode trunk**.
20. Состояние виртуальных сетей и интерфейсов коммутатора можно посмотреть по команде **sh vlan brief**.

Вопросы по лекции 15

1. Для чего создаются виртуальные локальные сети? Их достоинства?
2. Как связываются между собой VLAN и порты коммутатора?
3. Как обеспечивается общение между узлами разных виртуальных сетей?
4. Как обеспечивается управление виртуальными локальными сетями?
5. Можно ли построить VLAN на нескольких коммутаторах? Как это сделать?
6. Для чего служит идентификатор кадра (tag)? Где он размещается?
7. Что такое транк? Как он создается на коммутаторе и маршрутизаторе?
8. Какие команды используются для назначения VLAN на интерфейсы?
9. Какие команды используются для создания транковых соединений?
10. Какие команды используются для верификации VLAN?

Упражнения

1. Сконфигурируйте две виртуальных локальных сети на двух коммутаторах, используя транковые соединения.
2. Обеспечьте межсетевое взаимодействие.

Контрольный тест по разделу 6

Задача 6.1
Вариант 1 Задачи 6.1

166. Сетевые фильтры (списки доступа) создаются:

Только для входящих пакетов
Только для исходящих пакетов
Для входящих и исходящих пакетов
Для транзитных пакетов
Для пакетов, предназначенных удаленным сетям

Вариант 2 Задачи 6.1

167. Стандартный список доступа анализирует следующие параметры:

IP-адрес источника
IP-адрес назначения
Номер порта верхнего уровня
Маску подсети
MAC-адрес источника и назначения

Вариант 3 Задачи 6.1

168. Расширенный список доступа анализирует следующие параметры: (выбрать 3 ответа)

IP-адреса источника и назначения
MAC-адрес источника и назначения
Протокол
Номер порта верхнего уровня
Маску подсети

Задача 6.2
Вариант 1 Задачи 6.2

169. Запись в списке доступа

```
Router_A(config)#access-list 11 permit 192.168.30.11 0.0.0.0
```

Разрешает доступ к конечному узлу 192.168.30.11 защищаемой сети
Запрещает доступ к конечному узлу 192.168.30.11 защищаемой сети
Разрешает доступ конечному узлу 192.168.30.11 к защищаемой сети
Запрещает доступ конечному узлу 192.168.30.11 к защищаемой сети

Вариант 2 Задачи 6.2

170. Запись в списке доступа

```
Router_A(config)#access-list 11 permit host 192.168.30.15
```

Разрешает доступ к хосту 192.168.30.15 защищаемой сети
Запрещает доступ к хосту 192.168.30.15 защищаемой сети
Разрешает доступ хосту 192.168.30.15 к защищаемой сети
Запрещает доступ хосту 192.168.30.15 к защищаемой сети

Вариант 3 Задачи 6.2

171. Запись в строке конфигурации

```
Router_A(config-if)#ip access-group 12 out
```

Определяет группу из 12 списков доступа
Определяет доступ группы из хостов к сети
Устанавливает список доступа 12 на интерфейс для входящего трафика
Устанавливает список доступа 12 на интерфейс для исходящего трафика

Задача 6.3
Вариант 1 Задачи 6.3

172. Запись в строке списка доступа

```
Router_A(config-ext-nac1)#permit tcp host 192.168.30.11 host
192.168.10.25 eq 8080
```

принадлежит:

Стандартному именованному списку доступа
Стандартному не именованному списку доступа
Расширенному не именованному списку доступа
Расширенному именованному списку доступа

Вариант 2 Задачи 6.3

173. Запись в строке списка доступа

```
Router_A(config-ext-nac1)#permit tcp host 192.168.30.11 host
192.168.10.25 eq 8080
```

означает:

Узлу 192.168.30.11 разрешен доступ к узлу 192.168.10.25 по Telnet
Узлу 192.168.30.11 запрещен доступ к узлу 192.168.10.25 по Telnet
Узлу 192.168.10.25 разрешен доступ к узлу 192.168.30.11 по протоколу 8080
Узлу 192.168.10.25 запрещен доступ к узлу 192.168.30.11 по протоколу 8080
Узлу 192.168.30.11 разрешен доступ к узлу 192.168.10.25 по протоколу 8080

Вариант 3 Задачи 6.3

174. Запись в строке списка доступа

```
Router_A(config)#access-list 115 permit ip any any
```

означает:

Стандартный список доступа 115 разрешает всем IP пакетам доступ ко всем узлам сети
Расширенный список доступа 115 разрешает всем IP пакетам доступ ко всем узлам сети
Стандартный список доступа 115 запрещает всем IP пакетам доступ ко всем узлам сети
Расширенный список доступа 115 запрещает всем IP пакетам доступ ко всем узлам сети

Задача 6.4
Вариант 1 Задачи 6.4

175. Чтобы не показывать по команде `Switch-AB#sh run`
все пароли в открытом тексте, необходимо использовать следующую команду:

```
Switch(config)#enable samara secret
```

```
Switch(config)#enable password samara
Switch(config)#service password-encryption
Switch(config)#enable secret samara
Switch(config)#service encryption-password
```

Вариант 2 Задачи 6.4

176. Удаленный доступ к виртуальным линиям коммутатора по команде Telnet при использовании пароля «samara» будет разрешен при следующем наборе команд:

1. ```
   Switch(config-line)#config telnet
   Switch(config-line)#line vty 0 5
   Switch(config-line)#password samara
   ```

2. ```
   Switch(config)#line vty 0 4
   Switch(config)#password samara
   ```

3. ```
   Switch(config)#line vty 0 4
   Switch(config-line)#password samara
   Switch(config-line)#login
   ```

4. ```
   Switch(config-line)#config telnet
   Switch(config-line)#password samara
   Switch(config-line)#login
   ```

Вариант 3 Задачи 6.4

177. При вводе последовательности команд

```
Switch_A(config-line)# line console 0
Switch_A(config-line)# password samara
Switch_A(config-line)# login
```

будет получен следующий результат:

Паролем «samara» защищен удаленный доступ к коммутатору
Паролем «samara» защищен вход в привилегированный режим коммутатора
Паролем «samara» защищен режим глобального конфигурирования
Паролем «samara» защищен режим детального конфигурирования линий
Паролем «samara» защищен консольный порт коммутатора

Задача 6.5
Вариант 1 Задачи 6.5

178. Для управления коммутатором Catalist 2950 конфигурация (IP-адрес, маска сети или подсети, адрес шлюза по умолчанию) устанавливается по умолчанию:

На любой интерфейс
На интерфейс vlan 1
На интерфейс f0/0
На последовательный интерфейс s0/0
На линию console 0

Вариант 2 Задачи 6.5

179. Если на порт F0/1 коммутатора со следующей конфигурацией

```
Switch_A(config)#int f0/1
Switch_A(config-if)#switchport port-security
Switch_A(config-if)#switchport port-security mac-adress 00aa-1234-5b6d
Switch_A(config-if)#switchport port-security maximum 1
```

поступит кадр с MAC-адресом источника 00aa-1234-5bef, то:

Кадр будет уничтожен и будет сформировано уведомление
Кадр будет уничтожен и уведомление сформировано не будет
Кадр не будет уничтожен, MAC-адрес будет включен в таблицу коммутации
Интерфейс f0/1 будет выключен

Вариант 3 Задачи 6.5

180. В командной строке

```
Switch_A(config-if)#switchport port-security max 1
```

число 1 означает, что:

Только один конечный узел может быть подключен к интерфейсу
Только одна сеть может быть подключена к интерфейсу
К интерфейсу не подключен статически ни один конечный узел
К интерфейсу подключена динамически одна сеть
На интерфейсе задан один пароль

Задача 6.6
Вариант 1 Задачи 6.6

181. Режим реагирования системы на нарушения безопасности «Выключение» (**Shutdown**) вводится по команде:

```
Switch_A(config-if)#shutdown
Switch_A(config-if)#switchport port-security violation shutdown
Switch_A(config)# shutdown
Switch_A(config)#switchport port-security violation shutdown
```

Вариант 2 Задачи 6.6

182. Для повышения безопасности неиспользуемые порты коммутатора рекомендуется:

+ Выключить по команде **Shutdown**
Выключить по команде **switchport port-security violation shutdown**
Перевести в пассивное состояние
Перевести в активное состояние

Вариант 3 Задачи 6.6

183. Выберите режим конфигурирования, линии и интерфейсы, которые должны быть защищены паролем, чтобы ограничить доступ к коммутатору: (выбрать три ответа)

+ VTY line
+ console interface
Ethernet interface
secret EXEC mode
+ privileged EXEC mode
switch configuration mode

Задача 6.7
Вариант 1 Задачи 6.7

184. Для входа в режим создания VLAN на коммутаторе используется следующие команды: (выбрать два ответа)

```
Switch#config vlan
Switch#vlan database
Switch(config)#config vlan
Switch(config)#vlan database
Switch(config)#vlan (номер)
Switch(config)#database vlan (номер)
```

Вариант 2 Задачи 6.7

185. После удаления одной из виртуальных локальных сетей приписанные к ней порты будут иметь следующий статус:

Порты перейдут в пассивное состояние
Порты административно выключены
Порты будут связанными с удаленной сетью, пока не будут переназначены другой виртуальной сети
Порты удаленной сети будут автоматически переназначены сети VLAN1.

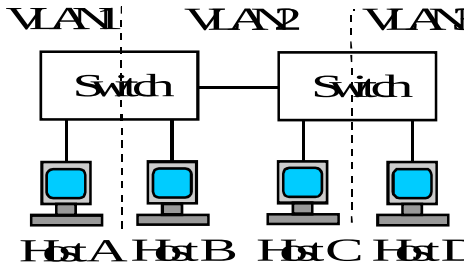
Вариант 3 Задачи 6.7

186. По умолчанию управляющей сетью является:

+ Первая сеть VLAN 1
Сеть, которой назначили IP-адрес
Сеть расширенного диапазона идентификаторов VLAN
Сеть, определенная стандартом 802.1Q

Задача 6.8
Вариант 1 Задачи 6.8

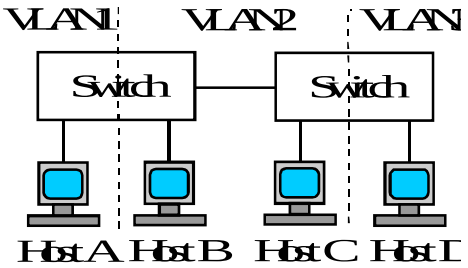
187. Посланный конечным узлом Host C (см. рис.) ARP-запрос может увидеть узел:



Host A
Host B
Host A и Host B
Host A и Host D
Host B и Host D
Host A, Host B и Host D

Вариант 2 Задачи 6.8

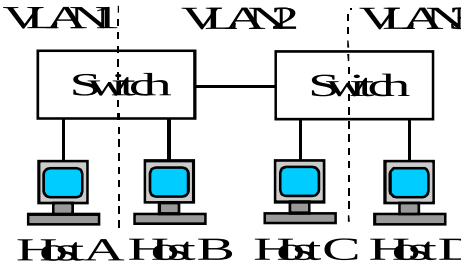
188. Сколько широковещательных доменов существует в сети (см. рис.)?



1, 2, 3, 4, 5

Вариант 3 Задачи 6.8

189. С какими узлами может общаться Host B в сети (см. рис.):



Host A
Host D
Host C
Host A и Host C
Host A и Host D
Host C и Host D
Host A, Host C и Host D

Задача 6.9
Вариант 1 Задачи 6.9

190. Для назначения порта VLAN2 на коммутаторе используется последовательность команд:

```
1.Switch#vlan database
  Switch(vlan)#vlan 2
  Switch(vlan)#vlan 2 trunk

2.Switch(config)#int fa 0/2
  Switch(config-if)#switchport mode access
  Switch(config-if)#switchport access vlan 2

3.Switch(config)#vlan database
  Switch(config)#vlan 2
  Switch(config)#vlan 2 name VLAN2

4.Switch(config)#int fa 0/2
  Switch(config-if)#switchport mode trunk
  Switch(config-if)#switchport access vlan 2
```

Вариант 2 Задачи 6.9

191. Для назначения порта trunk на коммутаторе используется последовательность команд:

1. Switch#**vlan database**
   Switch(vlan)#**vlan 2**
   Switch(vlan)#**vlan 2 trunk**
2. Switch(config)#**int fa 0/2**
   Switch(config-if)#**switchport mode access**
   Switch(config-if)#**switchport access vlan 2 trunk**
3. Switch(config)#**vlan database**
   Switch(config)#**vlan 2 trunk**
   Switch(config)#**vlan 3 name VLAN3**
4. Switch(config)#**int fa 0/2**
   Switch(config-if)#**switchport mode trunk**

Вариант 3 Задачи 6.9

192. На маршрутизаторе для создания соединения trunk коммутатора с маршрутизатором используется следующая последовательность команд:

1. Router(config-subif)#**int f0/0.30**
   Router(config-subif)#**encapsulation dot1q 30**
2. Router(config-if)#**int f0/0.30**
   Router(config-if)#**encapsulation dot1q 30**
3. Router(config- subif)#**int f0/0**
   Router(config- subif)#**encapsulation dot1q**
4. Router(config- subif)#**int f0/0**
   Router(config- subif)#**encapsulation dot1q**

Задача 6.10
Вариант 1 Задачи 6.10

193. Если не используется транковое соединение, то для организации межсетевых соединений необходимо:

Использовать дополнительные интерфейсы коммутатора и маршрутизатора, число которых равно количеству виртуальных сетей
Использовать дополнительно по одному интерфейсу коммутатора и маршрутизатора
Дополнительных интерфейсов не требуется

Вариант 2 Задачи 6.10

194. В транковых соединениях:

Несколько физических каналов заменяются одним агрегированным
Используется несколько агрегированных интерфейсов
Физический канал с полосой пропускания 100 Мбит/с заменяется каналом с полосой пропускания 1 Гбит/с
В агрегированном логическом канале выделяется несколько физических

Вариант 3 Задачи 6.10

195. Маршрутизацию между виртуальными локальными сетями обеспечивает:

Транковое соединение между коммутаторами
Транковое или обычное соединение между коммутаторами
Транковое или обычное соединение между коммутатором и маршрутизатором
Только обычное соединение между коммутатором и маршрутизатором

Задача 6.11
Вариант 1 Задачи 6.11

196. По какой команде удобно посмотреть активные виртуальные сети и приписанные к ним интерфейсы? (выбрать два ответа)

```
Sw_A#sh ip route
Sw_A#sh vlan brief
Sw_A#sh brief
Sw_A#sh vlan
Sw_A#sh int
```

Вариант 2 Задачи 6.11

197.Для чего назначают имена виртуальным локальным сетям?

Для ускорения процесса продвижения пакетов через коммутатор
Для повышения безопасности сетей
Для удобства чтения распечаток
Без них невозможно конфигурировать VLAN

Вариант 3 Задачи 6.11

198. Параметры виртуальных локальных сетей определяются стандартом:
IEEE 802.1
IEEE 802.2
IEEE 802.1Q
IEEE 802.2Q
IEEE 802.3Q

РАЗДЕЛ 7. ГЛОБАЛЬНЫЕ СЕТИ

Лекция 16. ТЕХНОЛОГИИ ГЛОБАЛЬНЫХ СЕТЕЙ

Краткая аннотация лекции: рассмотрены основные принципы и сетевые технологии, используемые при построении глобальных сетей.
Цель лекции: изучить принципы функционирования сетевых технологий, используемых при построении глобальных сетей.

16.1. Общие сведения о глобальных сетях

Локальные сети (LAN) функционируют в пределах ограниченного географического пространства (в пределах комнаты, этажа, здания или группы близко расположенных зданий). Глобальные сети (WAN) обеспечивают связь между далеко расположенными локальными сетями, удаленными пользователями. Сети WAN должны переносить различные типы трафика (голос, видео и данные) с требуемым качеством обслуживания.

Технологии глобальных сетей отличаются по предоставляемым услугам, быстродействию, стоимости услуг и оборудования. Услуги транспортной сети WAN пользователям предоставляют провайдеры. Часть оборудования сети размещается у провайдера, другая часть – у пользователя. Оборудование, размещаемое у пользователя, называется оборудованием помещения клиента (customer premises equipment - **CPE**). Клиент имеет либо собственное оборудование CPE, либо арендует его у поставщика услуг. Оборудование CPE по кабелю соединяется с ближайшим центральным офисом (central office - **CO**) поставщика услуг. Эту систему кабелей часто называют местной петлей (**local loop**), или "последней милей" (**last-mile**).

Глобальные сети можно классифицировать на сети с коммутацией пакетов, с коммутацией каналов и сети с выделенными линиями (рис.16.1).

Рис.16.1. Классификация глобальных сетей

Сети на основе **выделенных линий** связи экономически дороги, поскольку не всегда загружены полностью. Разделяемая общая линия в сетях с коммутацией каналов и пакетов позволяет снизить экономические затраты.

Сети с **коммутацией каналов** создавались для телефонных сетей общего пользования. Для повышения производительности их магистралей были разработаны технологии PDH, SDH. Сети были предназначены для равномерного потокового трафика. Поэтому при появлении компьютерных сетей потребовались новые сетевые технологии.

Сети с **коммутацией пакетов**, предназначенные для эластичного (пульсирующего) трафика, в последнее время получили широкое развитие, поскольку они обеспечивают более рентабельную технологию глобальных сетей по сравнению с технологией сетей с коммутацией каналов, предназначенных для равномерного (потокового) трафика.

При создании мультисервисных сетей, передающих все виды трафика (аудио сигналы, видеоинформацию, данные) сети с коммутацией каналов играют роль транспорта для сетей с коммутацией пакетов. По оптической транспортной сети (ОТС) или сети SDH передаются данные в виде пакетов переменной длины.

Сети с коммутацией пакетов могут быть с **предварительным соединением** (connection-oriented) или без предварительного соединения (connectionless), т.е. **дейтаграммные сети**. В дейтаграммных сетях, например Интернет, каждый промежуточный коммуникационный узел (коммутатор или маршрутизатор) должен обрабатывать **многоразрядный адрес**, чтобы решить, какому следующему узлу передать полученный пакет.

В сетях с предварительным соединением сначала определяется маршрут, по которому будет передаваться совокупность пакетов. Каждое соединение маршрута помечается **короткими идентификаторами**, которые хранятся в таблице коммутации. Обработка идентификаторов требует значительно меньше времени, чем обработка многоразрядных адресов и занимает меньше объем памяти. Проложенный маршрут через ряд физически существующих каналов получил название виртуального канала (Virtual Circuit – **VC**). Виртуальный канал может быть всегда доступным, т.е. постоянным (Permanent Virtual Circuit – PVC) или создаваемым на время, т.е. коммутируемым (Switched Virtual Circuit – SVC).

Ряд технологий, используемых в глобальных сетях, представлен в табл. 16.1.

Таблица 16.1

Технологии глобальных сетей

<table>
<tr><td colspan="2">Сетевой уровень</td><td colspan="2">IP</td><td rowspan="2">Коммутация пакетов</td></tr>
<tr><td colspan="2">Канальный уровень</td><td>Ethernet, FR, ATM, MPLS</td><td>HDLC, PPP</td></tr>
<tr><td rowspan="3">Физич-ий уровень</td><td>Выделенные каналы</td><td colspan="2">SDH, OTN</td><td rowspan="3">Коммутация каналов</td></tr>
<tr><td>Выделенные волны</td><td colspan="2">λ – DWDM, CWDM</td></tr>
<tr><td>Выделенные волокна</td><td colspan="2">Оптические волокна</td></tr>
</table>

Интернет-протокол IP является самым распространенным сетевым протоколом, функционирующем на третьем (сетевом) уровне модели OSI. Протокол IP применяется для построения как локальных, так и глобальных сетей, обеспечивая связь между разнородными далеко расположенными корпоративными и локальными сетями, а также удаленными пользователями. IP-адресация позволяет обращаться к любым адресатам внутри всемирной сети Интернет, для чего необходимо задать IP-адрес источника сообщения и IP-адрес назначения. Интернет представляет сеть с коммутацией пакетов. В многоуровневой модели глобальных сетей (табл. 16.1) протокол IP расположен на верхнем уровне. Остальные уровни обеспечивают услуги для IP-протокола.

Канальный уровень модели OSI представлен в модели технологий глобальных сетей (табл. 16.1) технологиями коммутации пакетов (Ethernet, Frame Relay, ATM, MPLS), а также технологиями соединений точка-точка (HDLC, PPP). Технологии Frame Relay, ATM, использующие виртуальные каналы, вытесняются новыми технологиями MPLS и Carrier Ethernet.

К физическому уровню модели OSI относятся технологии коммутации каналов, которые выполняют роль транспорта для технологий коммутации пакетов. Это технологии PDH, SDH, технологии спектрального уплотнения по длине волны λ – DWDM, CWDM, а также технология дальнейшего их развития – оптические транспортные сети - ОТС (**OTN**). Другие технологии коммутации каналов (ISDN, технологии телефонных сетей общего пользования) в глобальных сетях с коммутацией пакетов используются все реже и поэтому в модели табл.16.1 не отражены.

Выделенные линии могут быть представлены выделенными волокнами, выделенными волнами, выделенными каналами. Оптические волокна выделяются крупными операторами с разветвленной кабельной системой другим операторам и провайдерам. Выделенные волны (λ) предоставляются провайдерам и администраторам корпоративных сетей. Отдельные каналы PDH, SDH выделяются для корпоративных и локальных сетей.

Интернет образован совокупностью сетей операторов и провайдеров фиксированнеой и мобильной связи, соединенных с локальными сетями, сетями доступа и отдельными пользователями (рис.16.2).

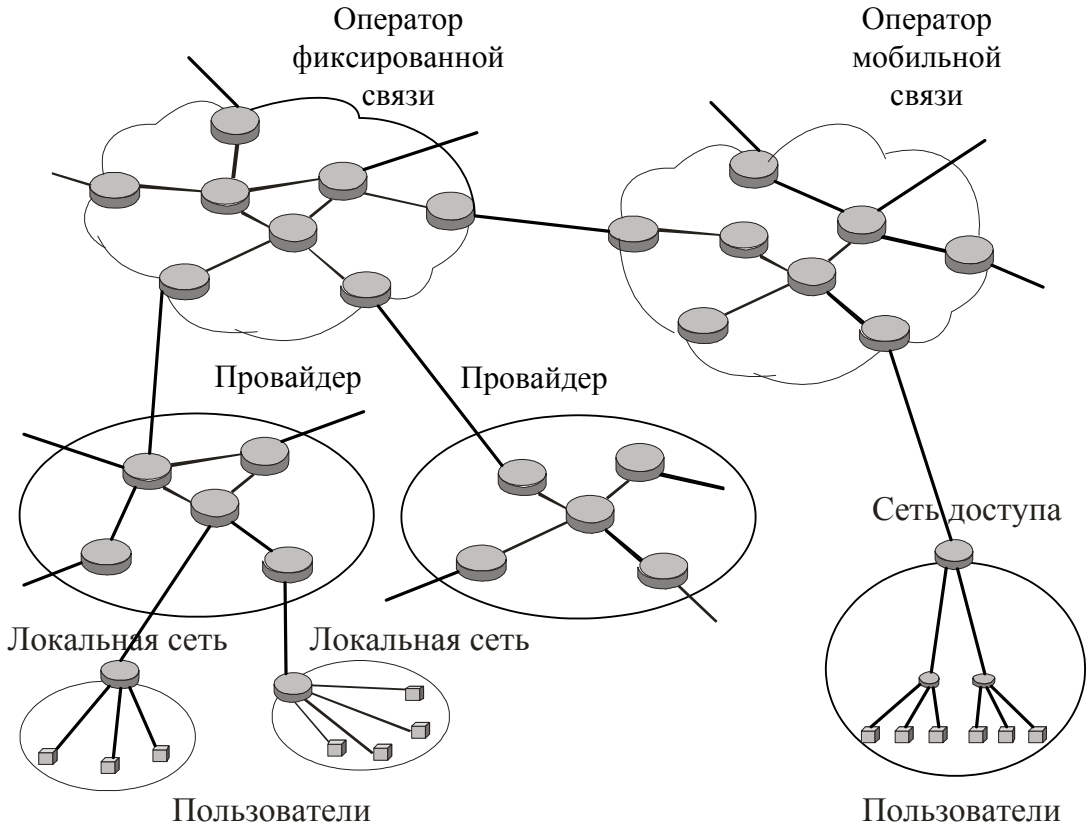


Рис.16.2. Схематичное изображение сети Интернет

Устройства клиента, которые подготавливают данные и передают их по локальной петле в сеть провайдера, называют терминальным оборудованием (data terminal equipment – DTE), например, маршрутизатор. Устройства, которые соединяют центральный офис провайдера (CO) с локальной петлей, называют канальным оборудованием (data communications equipment – DCE). Интерфейс DTE/DCE использует различные протоколы физического уровня, которые определяют скорость передачи, используемый код и электрические параметры, например, протоколы V.35, EIA/TIA-232. Оборудование DCE

обеспечивает провайдер, который предоставляет услуги для DTE, доступные через модем для аналоговых линий связи или через устройство согласования с каналом (channel service unit/data service unit - CSU/DSU) для цифровых линий, которое может быть встроено в интерфейс маршрутизатора.

Таким образом, присоединение маршрутизаторов, которые относятся к терминальному оборудованию DTE, через выделенный канал, например, PDH или SDH, к сети провайдера реализуется через аппаратуру DSU/CSU устройства DCE (рис.16.3).

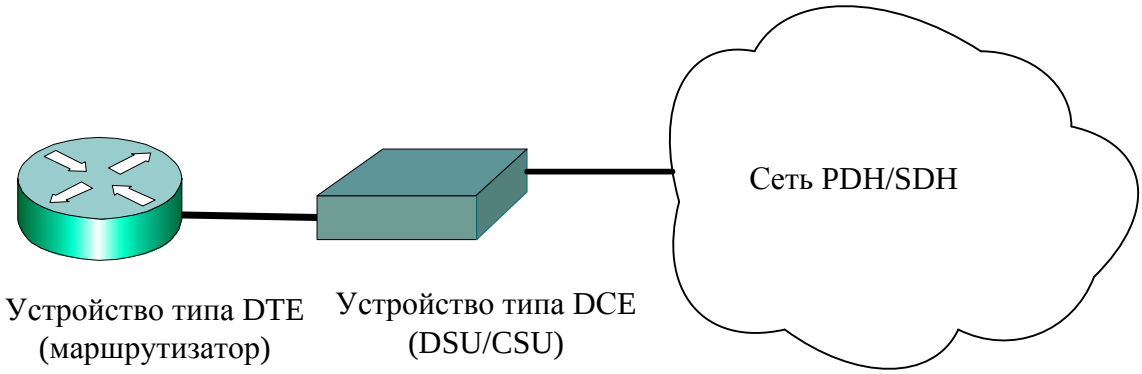


Рис.16.3. Соединение маршрутизатора с глобальной сетью

В тех случаях, когда устройство DCE встроено в порт маршрутизатора, его необходимо сконфигурировать.

При непосредственном соединении маршрутизаторов друг с другом, как например, на рис.16.4, один из интерфейсов должен быть типа DCE, а второй – остается DTE.

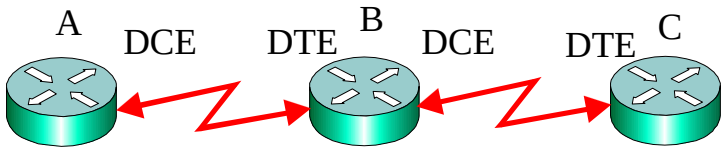


Рис.16.4. Непосредственное соединение маршрутизаторов

Глобальные сети строятся либо с использованием маршрутизаторов (рис.16.5), либо коммутаторов, например в сетях Frame Relay, либо коммутаторов-маршрутизаторов в сетях MPLS (рис.16.6).

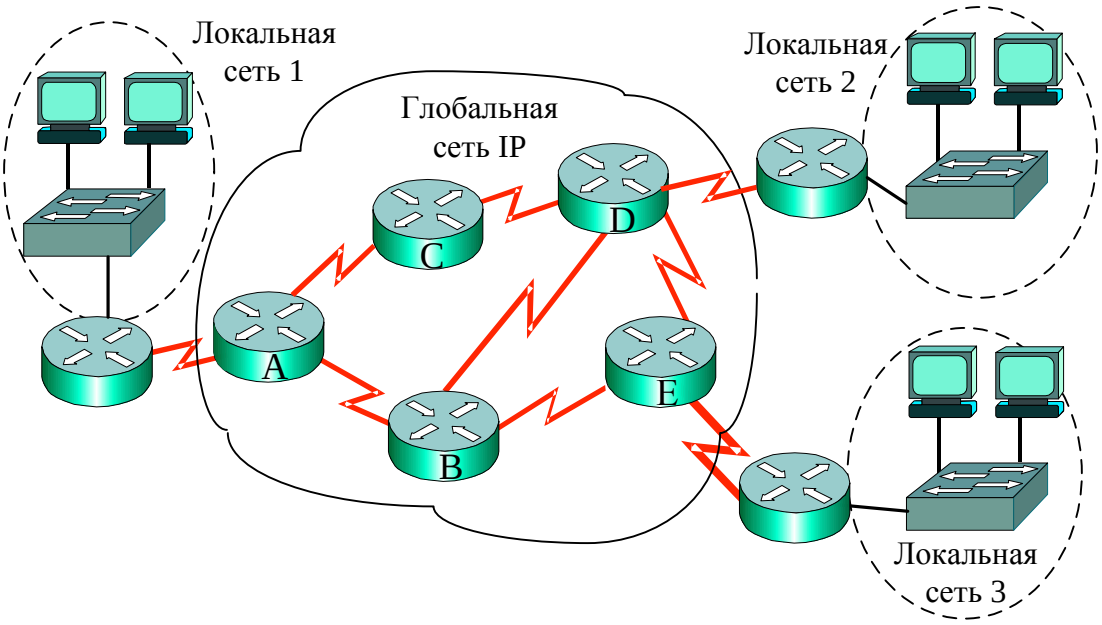


Рис. 16.5. Глобальная сеть IP на базе маршрутизаторов

Маршрутизаторы (рис. 16.5) содержат интерфейсы как локальных (интерфейсы Ethernet), так и глобальных сетей (интерфейсы serial). В простейшем случае глобальная IP-сеть образуется путем соединения последовательных интерфейсов маршрутизаторов выделенными линиями, при этом реализуются соединения «точка-точка». Эти линии представляют собой либо физически выделяемые волокна кабелей связи, либо отдельные волны λ, либо цифровые каналы сетей PDH/SDH.

Коммутаторы-маршрутизаторы (рис.16.6) обладают свойствами, как коммутаторов, так и маршрутизаторов.

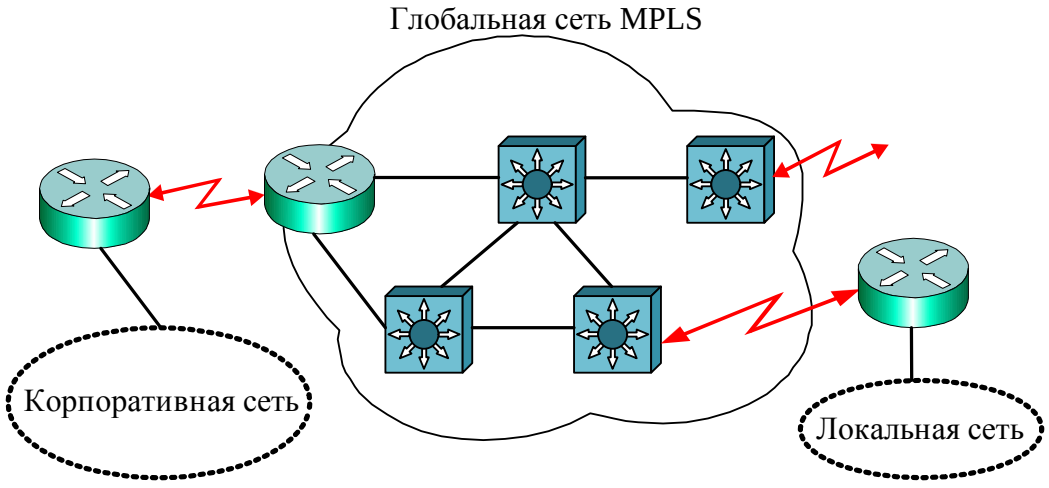


Рис.16.6. Глобальная сеть MPLS на базе коммутаторов-маршрутизаторов

Коммутаторы-маршрутизаторы имеют достаточно много портов и характеризуются высокой производительностью, как всякие коммутаторы, а также характеризуются широкими функциональными возможностями, прежде всего функцией маршрутизации, как всякие маршрутизаторы.

При передаче информации по глобальной сети пакеты проходят через целый ряд промежуточных устройств (коммутаторов, маршрутизаторов). В каждом из них производится обработка полученного пакета и продвижение его на выходной интерфейс. Промежуточное устройство при обработке пакета задействует программно-аппаратные средства не всех семи уровней модели OSI, а только нижних. Если IP-сеть непосредственно использует услуги выделенных каналов, то в промежуточных устройствах функционируют средства трех нижних уровней модели OSI (рис.16.7).

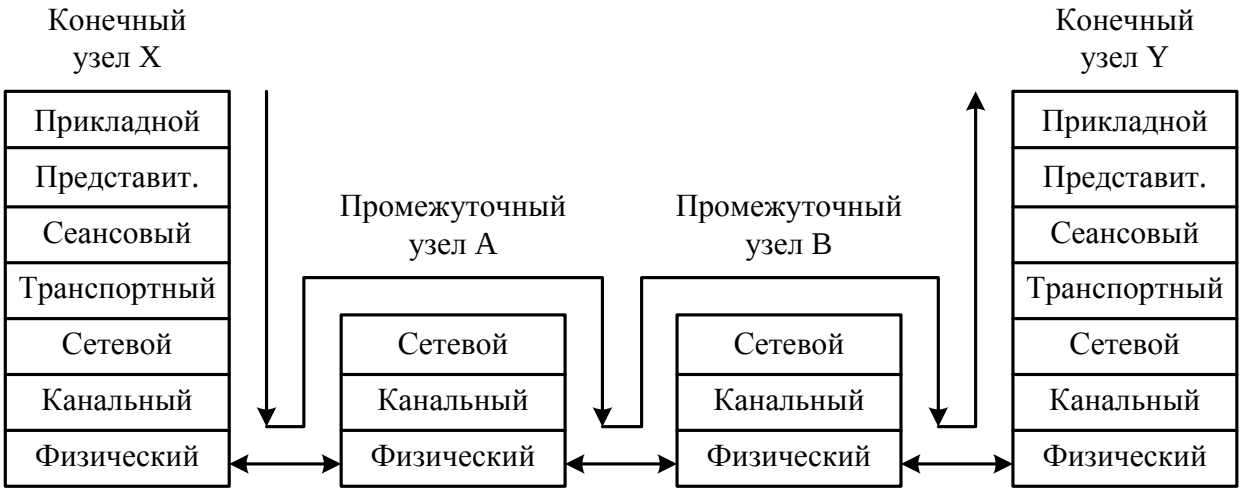


Рис.16.7. Три нижних уровня модели OSI в глобальных сетях

В сетевых технологиях с использованием виртуальных каналов (Frame Relay, ATM, MPLS) в процессе формирования канала используются средства трех нижних уровней модели OSI. Однако когда канал уже сформирован, то используются средства только двух нижних уровней (рис.16.8), что ускоряет процесс продвижения пакетов, т.е. уменьшается задержка пакетов в промежуточных устройствах.

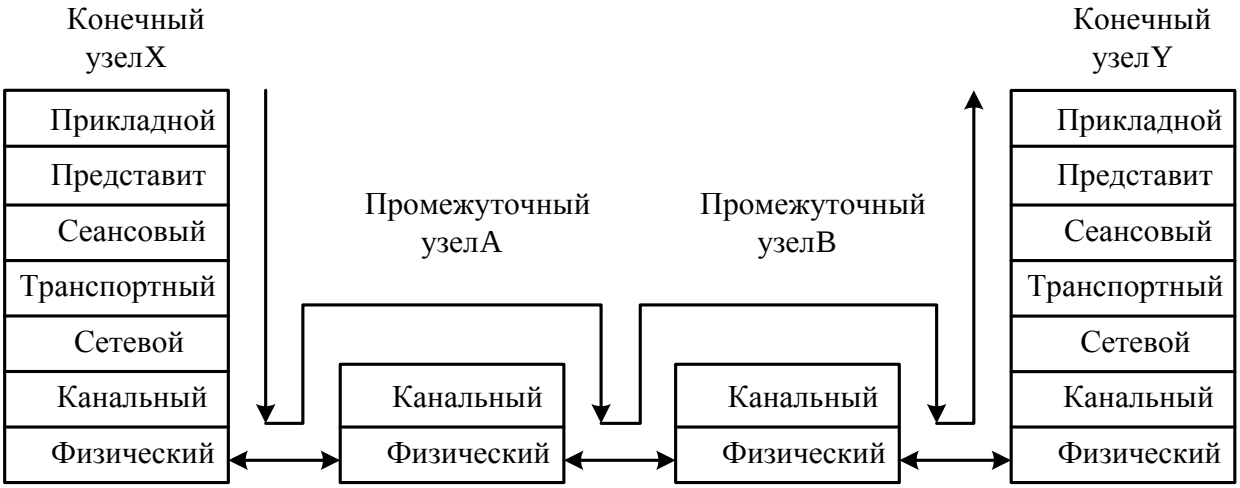


Рис.16.8. Два нижних уровня модели OSI в глобальных сетях

16.2. Протоколы соединений «точка-точка»

Передача сообщений между маршрутизаторами в IP-сети на основе выделенных каналов происходит при инкапсуляции пакета в кадр канального уровня. Протоколы, работающие на этом уровне (табл. 16.1), должны обеспечивать управление передачей, согласование параметров обмена, необходимые проверки для защиты сети на данном уровне. Кроме того, Ethernet и совместимые с ним протоколы обеспечивают физическую адресацию (MAC-адреса). В соединениях «точка-точка», характерных для структуры глобальной IP-сети (рис.16.5), нет необходимости задания физических адресов, поскольку интерфейсы непосредственно соединены друг с другом. Поэтому широко используются два протокола: высокоуровневого управления соединением (High-level Data Link Control – **HDLC**) и протокол точка-точка (Point-to-Point Protocol – **PPP**), в которых адреса задаются формально.

Протокол HDLC

Протокол HDLC установлен по умолчанию на всех устройствах Cisco, использующих выделенные линии и коммутируемые каналы глобальных сетей. Формат кадра протокола HDLC приведен на рис.16.9. Поле флага длиной в 1 байт – 01111110 используется в качестве разделителя кадров. При передаче данных после каждых пяти единиц вставляется 0. На приемной

стороне протокол удаляет вставленные нулевые биты. Поэтому, если на приемной стороне будет получено 6 единиц подряд, то это будет означать прием флага (нового кадра).

Флаг	Адрес	Контроль	Данные	Конт. сумма	Флаг
01111110	11111111				01111110
	Заголовок				

Рис.16.9. Формат кадра протокола HDLC

Поле адреса длиной 1 – 2 байта может содержать уникальный, групповой или широковещательный адрес. В соединениях «точка-точка» обычно используются широковещательные адреса 11111111. Поле контроля показывает, какая информация передается: управляющие кадры, информационные данные или универсальные (ненумерованные) кадры. Адрес и поле контроля образуют **заголовок** кадра. Длина поля контрольной суммы (FCS) составляет 2 – 4 байта.

Версия протокола HDLC фирмы Cisco в заголовке содержит дополнительно идентификатор протокола сетевого уровня, пакет которого инкапсулирован в поле данных кадра (рис.16.10). Это обеспечивает поддержку множества протоколов сетевого уровня (IP, IPX …). Например, при использовании протокола IP в поле контроля содержится шестнадцатеричное число 0×0800. В поле данных кадра канального Уровня 2 инкапсулируется пакет сетевого уровня.

Флаг	Адрес	Контр.	Протокол	Данные	Конт. сум.	Флаг
01111110	11111111		0×0800			01111110

Рис.16.10. Формат кадра протокола HDLC Cisco

Протокол HDLC представляет собой стек протоколов канального уровня для глобальных сетей:

- LAP-B – для сетей X.25;
- LAP-D – для сетей ISDN;
- LAP-M – для сетей, использующих модемы;
- LAP-F – для сетей Frame Relay.

По умолчанию на синхронных последовательных интерфейсах устройств Cisco сконфигурирован протокол HDLC, который обеспечивает надежную доставку данных по ненадежным линиям. Если на конфигурируемом устройстве протокол HDLC был удален, то его можно восстановить на соответствующем интерфейсе по команде:

```
Router(config-if)#encapsulation hdlc
```

Проверить установленный протокол, например, на интерфейсе **serial 0/1**, можно по команде:

```
Router#show interfaces serial 0/1.
```

Протокол PPP

Когда в сети на основе выделенных каналов функционирует оборудование различных фирм производителей, то передача сообщений между маршрутизаторами по выделенным линиям глобальных сетей производится с использованием **протокола «точка-точка»** (Point-to-Point Protocol – **PPP**). В отличие от HDLC протокол PPP поддерживает аутентификацию при установлении соединения.

Функции протокола PPP охватывают физический и канальный уровни, а также позволяют устанавливать взаимоотношения с сетевым уровнем. На физическом уровне могут использоваться синхронные и асинхронные соединения через RS-232-C, V.35 или другие интерфейсы DTE/DCE, которые определяют скорость передачи данных.

В рамках протокола PPP функционируют протоколы управления соединением (Link Control Protocol – **LCP**) и управления сетью (Network Control Protocols – **NCP**). На канальном уровне функционирует протокол LCP, который настраивает параметры соединения «точка-точка» канального уровня, тестирует и завершает соединение. Параметры соединения устанавливаются в процессе переговоров между узлами. Это могут быть значения MTU, режим аутентификации, сжатия данных, контроля ошибок.

Режим аутентификации может использовать протокол аутентификации по паролю (Password Authentication Protocol – **PAP**) или более строгий

протокол аутентификации по квитированию вызова (Challenge Handshake Authentication Protocol – **CHAP**).

Набор протоколов управления сетью (Network Control Protocols – **NCP**) позволяет взаимодействовать с различными протоколами сетевого уровня (IP Control Protocol, Appletalk Control Protocol, Novell IPX Control Protocol).

В протоколе PPP сохранен формат кадра протокола HDLC, но в поле данных размещены дополнительные поля заголовка. В отличие от протокола HDLC протокол PPP не обеспечивает процедуры надежной передачи данных и управления потоком. Однако протокол PPP дополнен процедурой принятия параметров соединения (качество линий, размер кадров, тип аутентификации, протокол сетевого уровня). Формат кадра протокола PPP приведен на рис.16.11.

Флаг	Адрес	Контр.	Протокол	Данные	Конт. сум.
01111110	11111111				

Рис.16.11. Формат кадра протокола PPP

Поле флага аналогично протоколу HDLC – 01111110 используется в качестве разделителя кадров. Достаточно одного флага в начале кадра. Поле адреса всегда содержит широковещательный адрес 11111111. Поле контроля длиной в один байт (00000011) обеспечивает передачу ненумерованных кадров. Поле протокола идентифицирует протокол сетевого уровня, пакет которого инкапсулирован в поле данных кадра. Максимальный размер поля данных по умолчанию составляет 1500 байт.

Протокол управления соединением (LCP) устанавливает сессию между взаимодействующими узлами, поддерживает ее и завершает. **На этапе установления соединения** инициирующий сессию узел посылает запрос (LCP Configure-Request) с предлагаемыми параметрами конфигурации. Второй узел в ответ либо подтверждает конфигурацию(LCP Configure-Ack), либо отвергает ее. После чего задается режим аутентификации.

Специфическая информация служебных пакетов LCP заключена в поле данных кадра протокола PPP (рис.16.11).

В поле данных кадра протокола PPP помещаются:

- поле кода (Code) длиной в один байт определяет тип пакета LCP, например, запрос конфигурации, подтверждение или отклонение конфигурации.
- поле идентификатора (Identifier) длиной в один байт определяет совпадение пакетов запроса и ответа;
- поле длины (Length) занимает 2 байта и задает общий размер пакета LCP;
- поле данных (Data) переменной длины определяется кодом.

В поле данных могут размещаться конфигурационные опции, такие как тип аутентификации (по паролю PAP или по квитированию вызова CHAP), тип сжатия данных и др.

Затем в работу включается протокол NCP. В настоящем конспекте лекций из сетевых протоколов рассматривается только протокол IP. Поэтому в рамках протокола NCP речь идет только о протоколе IP Control Protocol (IPCP). На этапе установления соединения инициирующий сессию узел посылает запрос об алгоритме сжатия информации и об IP-адресе. Последовательный порт может иметь отдельный IP-адрес или набор IP-адресов для подканалов синхронных транспортных модулей STM (для виртуальных контейнеров).

На этапе передачи данных протокол LCP поддерживает соединение и проводит его отладку (тестирует качество соединения), посылая и принимая служебные кадры (Echo-Request, Echo-Reply). После передачи данных сетевого уровня LCP протокол переходит к этапу завершения соединения.

На этапе завершения сессии узлы обмениваются пакетами запроса на завершение (LCP Terminate-Request) и подтверждения (LCP Terminate-Ack).

Конфигурирование параметров протокола PPP

При конфигурировании протокола PPP необходимо предварительно на маршрутизаторе сконфигурировать маршрутизирующий протокол (RIP, OSPF, EIGRP). Затем на последовательном интерфейсе маршрутизатора установить протокол PPP по команде:

```
Router(config-if)#encapsulation ppp
```

Конфигурирование типа сжатия производится по команде:

```
Router(config-if)#compress [predictor | stac]
```

Проверить установленный протокол, например, на интерфейсе **serial 0/1**, можно по команде:

```
Router#show interfaces serial 0/1.
```

Кроме того, по этой команде можно посмотреть состояние LCP и NCP.

16.3. Многопротокольная коммутация на основе меток

Технология многопротокольной коммутации по меткам (Multi Protocol Label Switching – **MPLS**) объединила технологию сетей виртуальных каналов с технологией сетей TCP/IP. Многопротокольная технология MPLS поддерживает не только стек TCP/IP, но и другие стеки протоколов, например IPX/SPX. Эта технология использует принципы сетей с виртуальными каналами (Frame Relay, ATM) для быстрой коммутации пакетов в многопротокольных сетях, что обеспечивает построение магистральных сетей, имеющих высокую скорость обработки трафика и возможность организации дополнительных сервисов.

В качестве узлов сети MPLS применяются коммутаторы-маршрутизаторы, которые коммутируют пакеты по меткам (Label Switching Router – **LSR**). При формировании меток используются технологии Сетевого уровня, а при передаче пакетов – технологии Канального уровня. Поэтому коммутатор-маршрутизатор LSR наделен качествами как работающего на сетевом уровне маршрутизатора с широкими функциональными возможностями, так и коммутатора канального уровня с высоким быстродействием. Метка передается в составе пакета, ее значение уникально для каждого участка пути между узлами сети MPLS. Маршрутизатор LSR определяет и поддерживает топологию сети с помощью протоколов маршрутизации (OSPF, BGP и др.), а продвижение пакетов по сети одного провайдера производится с использованием виртуальных каналов.

Обмен метками между LSR позволяет сформировать внутри сети MPLS пути с коммутацией по меткам (Label Switching Path – **LSP**). Для этого коммутаторы-маршрутизаторы, которые далее обозначаются как обычные маршрутизаторы, (рис.16.12) строят таблицы продвижения по меткам (табл.16.2). Построением таблиц занимается протокол распределения меток

(Label Distribution Protocol – **LDP**) в процессе формирования виртуальных каналов, которые являются путями коммутации по меткам LSP. Прокладка виртуальных каналов производится на основе таблиц маршрутизации с использованием многоразрядных IP-адресов, а передача данных ведется на основе таблиц продвижения с использованием коротких номеров меток, что повышает производительность маршрутизатора LSR.

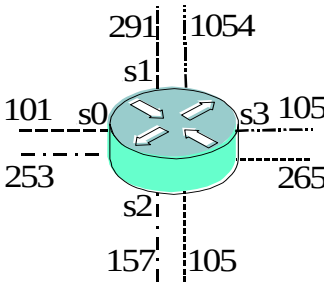


Рис.16.12. Коммутатор-маршрутизатор LSR

Таблица 16.2

Таблица продвижения по меткам коммутатора-маршрутизатора LSR

Входной интерфейс	Метка	Выходной интерфейс (Next Hop)	Действия
s0	101	s1	291
s0	253	s2	157
s3	265	s2	105

Получая пакет, маршрутизатор LSR по номеру интерфейса, на который пришел пакет, и по значению привязанной к пакету метки определяет выходной интерфейс. Старое значение метки заменяется новым, которое содержится в поле «выходная метка» таблицы, и пакет отправляется к следующему устройству.

Таблица 16.2 содержит описание входного интерфейса маршрутизатора LSR с соответствующей меткой виртуального соединения и описание выходного интерфейса с новой меткой виртуального пути. В таблице новая метка обозначена полем «Действия». Адрес виртуального пути может быть иерархическим, поэтому используется стек меток. Поле «Действия» отображает не только номер метки, но и команды по введению или удалению метки более высокого уровня, т.е. по перемещению стека меток. Также как в таблицах маршрутизации в поле «Выходной интерфейс» может задаваться либо условное обозначение выходного интерфейса маршрутизатора LSR, для

которого построена таблица, либо входной интерфейс следующего коммутирующего по меткам маршрутизатора (Next Hop) на пути пакета.

На границе сети MPLS функционируют **пограничные коммутирующие по меткам маршрутизаторы** (Label switch Edge Routers – **LER**), которые принимают от внешних IP-сетей стандартные пакеты с IP-адресами, добавляют к ним соответствующие метки и направляют пакеты по сформированному виртуальному пути через промежуточные маршрутизаторы LSR (рис.16.13).

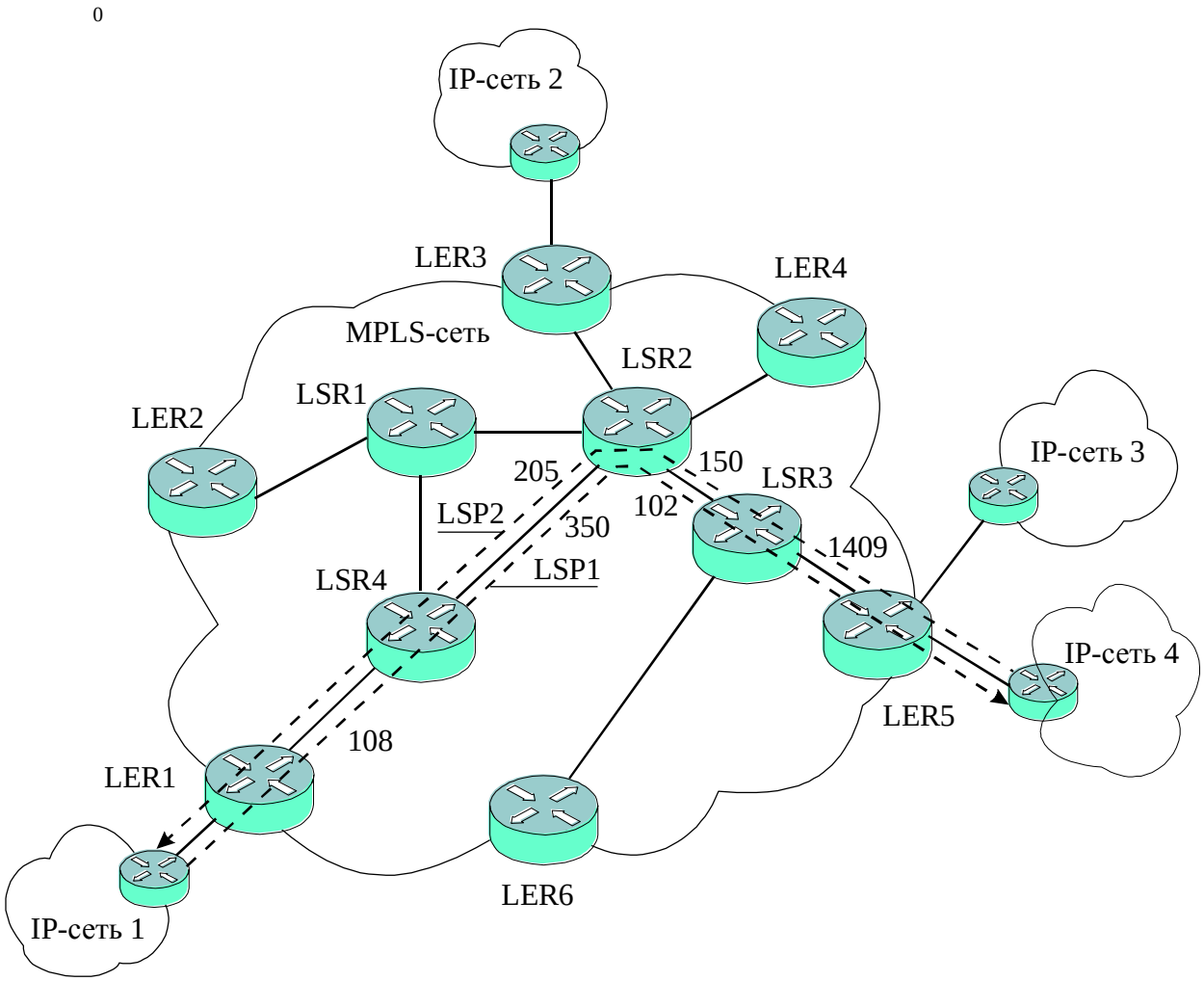


Рис.16.13. IP-сеть на основе MPLS

Внутри сети MPLS продвижение пакетов осуществляется по меткам, что ускоряет процесс передачи. Виртуальные пути коммутации по меткам, например, пути LSP1, LSP2, являются однонаправленными, поэтому один и тот же маршрут в разных направлениях (LSP1, LSP2) помечен двумя разными наборами меток. При продвижении пакета с входного интерфейса маршрутизатора на выходной номер метки изменяется. При выходе пакета из

сети MPLS метка должна быть удалена, чтобы передавать пакет дальше в стандартной форме по заданному IP-адресу. Для ускорения продвижения пакетов метку удаляет не пограничный маршрутизатор LER, а последний маршрутизатор LSR сети MPLS при передаче пакета пограничному маршрутизатору. Например, на виртуальном пути LSP1 удаление метки производит LSR3, удаление метки на виртуальном пути LSP2 производит маршрутизатор LSR4. Номер метки имеет не глобальное, а локальное значение на двухточечном соединении.

Виртуальные пути прокладываются заранее. При появлении в таблице маршрутизации новой записи маршрутизатор запускает процесс прокладки нового виртуального пути к вновь появившейся сети. Например, если в таблице маршрутизатора LSR4 появилась новая IP-сеть 5 с адресом 131.1.22.0, то LSR4 посылает запрос протокола распределения меток LDP маршрутизатору LSR1 (рис.16.14, табл.16.3). В запросе указывается IP-адрес сети, к которой нужно проложить новый виртуальный путь LSP1.

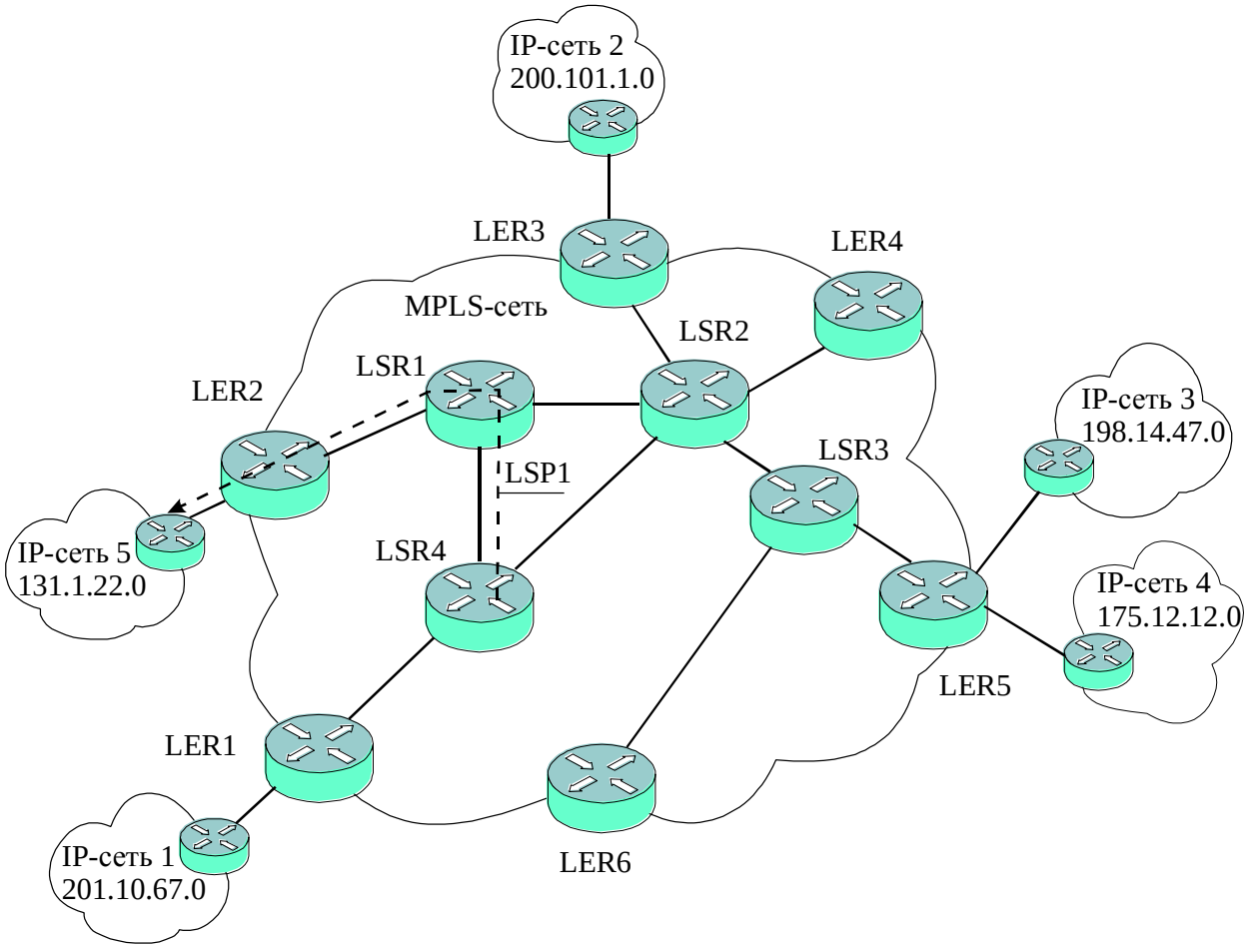


Рис.16.14. Формирование виртуального пути с помощью протокола LDP

Таблица 16.3

Пример таблицы маршрутизации LSR4

Сеть	Адрес	Шлюз (Next Hop)
IP-сеть 5	131.1.22.0	LSR1
IP-сеть 1	201.10.67.0	LER1
IP-сеть 2	200.101.1.0	LSR2
IP-сеть 3	198.14.47.0	LSR2
IP-сеть 4	175.12.12.0	LSR2

Если маршрутизатор LSR1 определяет, что в его таблице продвижения также нет виртуального пути к IP-сети 5, то он передает запрос следующему маршрутизатору в соответствии с его таблицей маршрутизации, т.е. маршрутизатору LER2. Поскольку LER2 является пограничным, то он посылает ответ маршрутизатору LSR1, который в свою очередь передает ответ маршрутизатору LSR4. При этом протокол распределения меток LDP назначает номера меток виртуальным соединениям. В дальнейшем передача пакетов данных в IP-сеть 5 будет производиться не на основе таблицы маршрутизации, а на основе таблицы продвижения. Таким образом, запросы, ответы, таблицы продвижения и номера меток формируются с помощью протокола распределения меток LDP.

Если пути к некоторым сетям, например, к IP-сети 3 с адресом 198.14.47.0 и к IP-сети 4 с адресом 175.12.12.0, в пределах MPLS-сети совпадают, то маршрутизаторы создают объединенные (агрегированные) пути к таким сетям. Агрегированные маршруты образуют класс эквивалентности перенаправления/форвардинга (FEC). Все пакеты определенного FEC, входящие в сеть через определенный узел, будут следовать по единому маршруту. Таким образом, принадлежность пакета определенному FEC определяется, когда пакет попадает в пограничный маршрутизатор. Пакет помечается меткой раньше, чем продвигается на выходной интерфейс. При вхождении пакета в MPLS-сеть через разные маршрутизаторы, он помечается разными метками.

В технологии MPLS используются кадры разных технологий канального уровня: PPP, Ethernet, Frame Relay, ATM. В эти кадры помещается IP-пакет с заголовком MPLS. Заголовок MPLS содержит 32 двоичных разряда, из которых 20 разрядов занимает поле номера метки, 8

разрядов – поле время жизни TTL, дублирующее соответствующее поле заголовка IP-пакета, 3 разряда – поле класса сервиса CoS для передаваемого типа трафика, 1 разряд – признак S дна стека меток (рис.16.15). Заголовок MPLS помещается между заголовком кадра PPP, Ethernet, Frame Relay и заголовком IP-пакета.

Заголовок MPLS

Рис.16.15. Формат заголовка MPLS

Поскольку внутри сети MPLS нет необходимости анализировать заголовки сетевого уровня, то маршрутизаторы можно заменить коммутаторами, которые идентифицируют метку и производят ее замену при продвижении пакетов, что повышает быстродействие.

Продвижение кадра внутри маршрутизатора сети MPLS производится на основе меток, а не на основе технологий канального уровня, например, Ethernet. Поэтому при продвижении кадра отпадает необходимость изменения MAC-адресов источника и назначения в кадре, следовательно, отпадает необходимость обращения к ARP-таблице и необходимость широковещательных ARP-запросов. Все это существенно ускоряет процесс передачи пакета по сети.

Один и тот же путь или отрезок пути можно пометить разными метами для разных видов трафика. Это дает возможность строить развитую систему приоритетов и создавать эффективную систему управления качеством QoS.

Краткие итоги лекции 16

1. Глобальные сети (WAN) обеспечивают связь между далеко расположенными локальными сетями, удаленными пользователями.
2. Услуги транспортной сети WAN пользователям предоставляют провайдеры.
3. "Последняя миля" (last-mile) или местная петля (local loop) – это система кабелей, которая соединяет оборудование помещения клиента (CPE) с центральным офисом (**CO**) поставщика услуг.
4. В сетях с предварительным соединением сначала определяется маршрут, по которому будет передаваться совокупность пакетов. Каждое соединение маршрута помечается короткими идентификаторами, которые хранятся в таблице коммутации.
5. Обработка идентификаторов требует значительно меньше времени, чем обработка многоразрядных адресов и занимает меньше объем памяти.
6. Технологии коммутации каналов выполняют роль транспорта для технологий коммутации пакетов.
7. Протокол высокоуровневого управления соединением (HDLC) установлен по умолчанию на всех устройствах Cisco. Поле адреса длиной 1 – 2 байта может содержать уникальный, групповой или широковещательный адрес.
8. Поле адреса протокола точка-точка (PPP) содержит широковещательный адрес 11111111. Протокол PPP поддерживает аутентификацию при установлении соединения.
9. Режим аутентификации протокола PPP может использовать аутентификацию по паролю (PAP) или более строгую аутентификацию по квитированию вызова (CHAP).
10. Технология многопротокольной коммутации по меткам (MPLS) объединила технологию сетей виртуальных каналов с технологией сетей TCP/IP.
11. Коммутаторы-маршрутизаторы (LSR) коммутируют пакеты по меткам. При формировании меток используются технологии Сетевого уровня, а при передаче пакетов – технологии Канального уровня.
12. На границе сети MPLS функционируют пограничные коммутирующие по меткам маршрутизаторы (Label switch Edge Routers – LER), которые принимают от внешних IP-сетей стандартные пакеты с IP-адресами, добавляют к ним соответствующие метки и направляют пакеты по сформированному виртуальному пути через промежуточные маршрутизаторы LSR.

Вопросы по лекции 16

1. Какие функции выполняют глобальные сети?
2. Кто предоставляет пользователям (клиентам) услуги транспортирования сообщений?
3. Что такое «последняя миля» или местная (локальная) петля?
4. Чем характеризуются сети с предварительным соединением (сети на основе виртуальных каналов)?
5. Как адресуются сообщения при использовании протокола HDLC?
6. Как адресуются сообщения при использовании протокола PPP?
7. Каковы дополнительные возможности протокола PPP по сравнению с протоколом HDLC?
8. В чем особенности технологии многопротокольной коммутации по меткам (MPLS)?
9. Какие маршрутизаторы используются на гаранице и внутри сети MPLS?
10. Как создаются таблицы продвижения по меткам коммутатора-маршрутизатора LSR?
11. Какие параметры содержит таблица маршрутизации и таблица продвижения по меткам?

Упражнения

1. Смоделируйте составную распределенную сеть согласно рис.13.2.
2. Определите, какой протокол используется на соединениях между коммутаторами (HDLC или PPP). Измените протокол на другой.

13. Проверьте функционирование сети.
14. Изобразите формат заголовка MPLS. Объясните назначение полей.

Контрольный тест по разделу 7

Задача 7.1
Вариант 1 Задачи 7.1

199. Услуги транспортирования сообщений пользователям (клиентам) предоставляет:

Оборудование помещения клиента (customer premises equipment - CPE)
Система оборудования местной петлей (local loop), или "последней милей" (last-mile)
Провайдеры (Internet Service Provider – ISP)
Терминальное оборудование (data terminal equipment – DTE)

Вариант 2 Задачи 7.1

200. Маршрутизаторы по умолчанию относятся к оборудованию типа:

Терминальному (data terminal equipment – DTE)
Канальному (data communications equipment – DCE)
Устройству согласования с каналом (channel service unit/data service unit - CSU/DSU)
Интерфейсу выделенного канала

Вариант 3 Задачи 7.1

201. Оборудование CPE является:

Оборудованием помещения клиента
Оборудованием центрального офиса провайдера
Оборудованием местной петли (local loop), или
Оборудованием "последней милей" (last-mile)

Задача 7.2
Вариант 1 Задачи 7.2

202. На стадии формирования канала в технологиях Frame Relay, ATM, MPLS используются средства:

Всех семи уровней модели OSI
Трех нижних уровней модели OSI
Трех верхних уровней модели OSI
Двух нижних уровней модели OSI

Вариант 2 Задачи 7.2

203. На стадии передачи данных в сетях Frame Relay, ATM, MPLS используются средства:

Всех семи уровней модели OSI
Трех нижних уровней модели OSI
Трех верхних уровней модели OSI
Двух нижних уровней модели OSI

Вариант 3 Задачи 7.2

204. Три нижних уровня модели OSI в технологиях Frame Relay, ATM, MPLS используются:

На стадии передачи данных
В автопереговорах
На стадии формирования канала
На стадии аутентификации

Задача 7.3
Вариант 1 Задачи 7.3

205. В соединениях «точка-точка» широко используются протоколы: (2 ответа)

Многопротокольной коммутации по меткам (MPLS)
Высокоуровневого управления соединением (HDLC)
Протокол точка-точка (PPP)
Асинхронного режима передачи(ATM)
Протоколы сетей трансляции кадров (Frame Relay)

Вариант 2 Задачи 7.3

206. Протокол точка-точка (PPP) в поле адреса кадра использует комбинацию:

00000000
01111110
10101011
11111111

Вариант 3 Задачи 7.3

207. Протокол точка-точка (PPP) использует аутентификацию: (2 ответа)

по паролю (PAP)
по протоколу управления сетью (NCP)
по квитированию вызова (CHAP)
по протоколу управления соединением (LCP)

Задача 7.4
Вариант 1 Задачи 7.4

208. Внутри сети MPLS функционируют маршрутизаторы:

LSP
LSR
LDP
LER

Вариант 2 Задачи 7.4

209. На границе сети MPLS функционируют маршрутизаторы:

LSP
LSR
LDP
LER

Вариант 3 Задачи 7.4

210. Построением таблиц сети MPLS занимается протокол:
LSP
LSR
LDP
LER

Задача 7.5
Вариант 1 Задачи 7.5

211. В сети MPLS создаются: (2 ответа)

таблица продвижения по меткам
таблица маршрутизации
таблица топологии
таблица соседних устройств

Вариант 2 Задачи 7.5

212. Продвижение кадра внутри маршрутизатора сети MPLS производится:

на основе технологий канального уровня
на основе технологий сетевого уровня
на основе технологий транспортного уровня
на основе меток

Вариант 3 Задачи 7.5

213. Заголовок MPLS помещается:

между заголовком кадра PPP, Ethernet, Frame Relay и заголовком IP-пакета:
перед заголовком кадра PPP, Ethernet, Frame Relay
после заголовка IP-пакета:
в поле трейлера кадра

Заключение

Среди проблем в области сетевых технологий важное место занимают подготовка и переподготовка кадров, а также обеспечение информационной безопасности. Это обусловлено повсеместным переходом аналоговых и цифровых АТС на использование сетей с пакетной коммутацией, а также ростом угроз несанкционированного доступа. В связи с переходом на сети с пакетной коммутацией, в настоящее время происходит интенсивная переподготовка кадров, работающих в области телекоммуникаций. Требования знания основ создания защищенных сетей работодатели предъявляют и к поступающим на работу студентам.

Существующая в настоящее время система защиты информации при передаче по сети не в полной мере удовлетворяет требованиям по защите от несанкционированного доступа. Поэтому происходит постоянный поиск путей и способов создания аппаратно-программных средств и комплексов в рамках системы обеспечения информационной безопасности. Знание и учет особенностей построения и функционирования сети, конкретных стандартов и протоколов является основой успешного решения этой задачи.

Автор надеется, что материал настоящего учебного пособия представлен в доступной форме, что облегчит читателям задачу овладения технологиями современных сетей. Слушатели курсов и студенты, освоившие технологии виртуальных локальных сетейи обеспечение безопасности коммутаторов, а также конфигурирование сетевых фильтров (списков доступа), смогут эффективно создавать защищенные сети, как локальные, так и распределенные.

Список литературы

1. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. СПб: Питер, 2011 – 944 с.
2. Гольдштейн Б.С., Соколов Н.А., Яновский Г.Г. Сети связи: Учебник для ВУЗов. СПб.:БХВ-Петербург, 2010 – 400 с.
3. Гордиенко В.Н., Крухмалев В.В., Моченов А.Д., Шарафутдинов Р.М. Оптические телекоммуникационные системы. Учебник для вузов /. Под ред. В.Н. Гордиенко. – М.: Горячая линия – Телеком, 2011 – 368 с.
4. Программа сетевой академии Cisco CCNA 1 и 2. Вспомогательное руководство. М.: Издательский дом «Вильямс», 2005. – 1168 с.
5. Программа сетевой академии Cisco CCNA 3 и 4. Вспомогательное руководство. М.: Издательский дом «Вильямс», 2006. – 1000 с.
6. Васин Н.Н. Сети и системы передачи информации на базе коммутаторов и маршрутизаторов. Конспект лекций. – Самара: ГОУ ВПО ПГУТИ, 2010. – 362 с.
7. Васин Н.Н. Основы сетевых технологий на базе коммутаторов и маршрутизаторов. – М.: Интернет-Университет Информационных технологий: БИНОМ, 2011. – 270 с

Глоссарий
Ключевые термины лекции 1

Глобальные вычислительные сети - ГВС **(**Wide Area Network **- WAN)** – функционируют на широком географическом пространстве.
Дейтаграммные сети (технология IP) – характеризуются отсутствием предварительного соединения конечных узлов и подтверждения приема сообщения.
Инкапсуляция – процесс обрамление единицы данных заголовками со служебной информацией.
Канальный уровень (Data Link) 2 – формирует кадры данных и задает физические адреса устройств.
Коммутация – процесс формирования маршрута, по которому передается сообщение; продвижение данных с входного интерфейса на выходной.
Коммутатор – устройство, реализующее процесс коммутации.
Локальные сети передачи данных - ЛВС (Local Area Network - **LAN**) – функционируют на ограниченном географическом пространстве (в здании, аудитории).
Маршрутизатор – устройство реализующее процесс маршрутизации.
Маршрутизация – процесс выбора оптимального маршрута.
Межуровневый интерфейс – определяет взаимодействие уровней модели сети между собой.
Метрика – критерий выбора оптимального маршрута.
Протокол – правила, по которым происходит обмен данными между программно-аппаратными средствами, находящимися на одном уровне модели сети.
Сеансовый (Session Layer) уровень 5 – устанавливает сеанс связи двух конечных узлов.
Сетевой уровень (Network Layer) 3 – адресует сообщение, задавая логические IP-адреса, определяет маршрут, по которому передается пакет данных.
Сети с коммутацией каналов – канал создается до передачи сообщения.
Сети с коммутацией пакетов (сообщений) – все возможные маршруты (каналы) созданы заранее, маршрутизаторы выбирают оптимальный.
Сигнал – физический процесс, изменение информационного параметра которого отображает и переносит сообщение.
Сообщение – форма представления информации, удобная для передачи на расстояние.
Таблица маршрутизации – содержит маршруты ко всем доступным сетям, позволяет выбрать оптимальный маршрут.
Телекоммуникационная сеть – комплекс аппаратных и программных средств передачи сообщений с заданными параметрами качества. Образуется совокупностью абонентов и узлов, соединенных линиями (каналами) связи.
Транспортный уровень (Transport Layer) 4 – обеспечивает надежную доставку пакетов, из длинного сообщения формирует сегменты.

Уровень 6 Представления (Presentation Layer) – изменяет форму представления данных, производит шифрацию и сжатие данных.
Уровень 7 Приложений (Application Layer) – оперирует наиболее общей единицей данных – сообщением.
Физический уровень 1 (Physical**) –** реализует передачу последовательности битов по соответствующей физической среде (электрический или оптический кабель, радиоканал) через соответствующий интерфейс.

Ключевые термины лекции 2

Контроль потока – обеспечивает управление скоростью передачи данных путем изменения размера скользящего окна (Window), которое указывает, сколько байт данных может быть передано за одну порцию.
Модель «клиент – сервер» – клиент запрашивает информацию, пересылая запрос выделенному серверу (upload), который в ответ на запрос посылает (download) файл, принимаемый клиентом.
Номер порта – идентифицирует приложения верхнего уровня модели OSI.
Номер последовательности (Sequence Number) – номер первого байта в сегменте, используемого, чтобы гарантировать объединение частей (порций) данных в корректном порядке в устройстве назначения;
Подтверждение (**acknowledgment**) – после получения порции данных узел назначения посылает источнику квитанцию подтверждения (квитирование), что обеспечивает надежность передачи данных.
Приложения прикладного уровня – обеспечивают интерфейс (сопряжение) человека с сетью
Протокол передачи гипертекстовой информации (Hypertext Transfer Protocol – **HTTP**) – отображает данные на Web-страницах, используя текст, графику, звук и видео. Его основным приложением является Web-браузер.
Протокол Telnet – обеспечивает виртуальное соединение пользователя с удаленными сетевыми устройствами
Протокол динамического назначения адресов узлов (Dynamic Host Configuration Protocol – **DHCP**) – позволяет автоматизировать процесс назначения IP-адресов рабочим станциям из диапазона, предоставленного администратору провайдером.
Протокол передачи файлов (Fail Transfer Protocol – **FTP**) – позволяет передавать файлы от одного узла другому
Протоколы передачи электронной почты (Simple Mail Transfer Protocol – **SMTP**, Post Office Protocol – **POP**, Internet Messaging Access Protocol – **IMAP**).
Протоколы IP, UDP – являются протоколами **дейтаграммного типа** без предварительного соединения, которые обеспечивают доставку сообщения через сеть без гарантий, т.е. доставка не надежная.
Протокол, ориентированный на предварительное соединение (**TCP**) – обеспечивает контроль потока и надежность доставки.

Размер скользящего окна (**Window**) – определяет, сколько байтов данных передается в одной порции неподтвержденных данных.
Службы сервиса – используют программные средства протоколов, чтобы подготовить информацию для передачи по сети.
Сеть peer-to-peer – связанные через сеть конечные узлы разделяют общие ресурсы (принтеры, файлы) без выделенного сервера.
Система доменных имен (Domain Name System – DNS), используется, чтобы переводить имена сайтов или доменов в числовые значения IP адреса.

Ключевые термины лекции 3

Беспроводные локальные сети (Wireless LAN – **WLAN**) – определяются стандартом IEEE 802.11 (Wi-Fi).
Волоконно-оптического кабель – характеризуется отсутствием перекрестных помех и электромагнитных помех от внешних источников.
Конечный узел (host) – компьютер, принтер, IP телефон.
Консольный кабель – используется при конфигурировании коммутатора или маршрутизатора для их соединения с последовательным COM-портом компьютера.
Кроссовый кабель – используется для соединения одноименных устройств между собой (например, коммутатора с коммутатором или концентратором).
Логическая топология – показывает, как по сети передаются определенные единицы информации.
Прямой кабель – используется для соединений маршрутизатора с коммутатором, коммутатора (концентратора) с компьютерами или серверами
Симметричные кабели UTP – обеспечивают передачу сигналов на расстояние до 100 м.
Топология кольцо (ring) – сигналы передаются в одном направлении от узла к узлу.
Топология звезда (star) – требует применения центрального устройства.
Топология шина (bus) – характеризуется тем, что передачу данных в данный момент времени может вести только один узел.
Физическая топология – представляет собой наиболее общую структуру сети и отображает схему соединения сетевых элементов кабелями связи.

Ключевые термины лекции 4

Коллизия – возникает при одновременной передаче данных двумя станциями в сети с множественным доступом к среде, когда сигналы двух передающих узлов накладываются друг на друга.
MAC-адрес – содержит 48 двоичных разрядов и представляется в шестнадцатеричной системе. В локальных сетях адресация узлов производится на основе MAC-адресов.

Подуровень LLC – реализует связь с протоколами сетевого уровня и определяет логические процедуры передачи кадров по сети.
Подуровень MAC – определяет особенности доступа к физической среде при использовании различных технологий локальных сетей.
Продвижение кадра – передача кадра с входного интерфейса на выходной порт, к которому подключен узел назначения.
Производительность коммутатора – скорость фильтрации кадров, скорость продвижения кадров, пропускная способность, длительность задержки передачи кадра.
Протокол охватывающего дерева (STP) – используется, чтобы избежать маршрутных (коммутационных) петель.
Процедура LLC1 – без установления соединения и подтверждения; используется при дейтаграммном режиме передачи данных.
Процедура LLC2 – с установлением соединения перед началом передачи данных и подтверждением.
Процедура LLC3 – без установления соединения, но с подтверждением.
Спецификация технологии MAC-уровня – определяет среду физического уровня и основные параметры передачи.
Фильтрация кадров – удаление кадра из буфера порта, когда адресат назначения и источник находятся в одном сегменте.

Ключевые термины лекции 5

Fast Ethernet – характеризуется скоростью передачи данных до 100 Мбит/с, стандарт сетей Fast Ethernet – 802.3u.
Gigabit Ethernet, – характеризуется скоростью передачи данных 1 Гбит/с, стандарт сетей Gigabit Ethernet – 802.3z, 802.3ab.
10Gigabit Ethernet, – характеризуется скоростью передачи данных 10 Гбит/с, стандарт сетей **10**Gigabit Ethernet – 802.3z, 802.3ae.
Скрэмблирование – способ исключения в передаваемых данных длинных последовательностей нулей.
Спецификация 100Base-TX – использует две витых пары UTP 5 категории.
Спецификация 100Base-T4 – использует 4 витые пары категории UTP 3.
Спецификация 100Base-FX – предусматривает работу по двум волокнам оптического многомодового кабеля.
Спецификации 1000Base-SX и **1000Base-LX** определены стандартом 802.3z и предусматривают работу по волокнам оптического кабеля.
Уровень логического кодирования Fast Ethernet – избыточные коды 4B/5B или 8B/6T.
Уровень логического кодирования Gigabit Ethernet – код 8B/10B.
Уровень физического кодирования Fast Ethernet – коды NRZI для оптической среды и MLT-3 для симметричных кабелей.

Ключевые термины лекции 6

Агрегированный адрес объединяет несколько отдельных адресов в один общий.
Адрес 127.0.0.1 предназначен для **самотестирования**, узел проверяет, установлен ли протокол TCP/IP.
Бесклассовые протоколы маршрутизации передают в обновлениях маршрутизации IP-адреса и соответствующие маски.
Версия IPv6 использует для адресации 128 двоичных разрядов.
Глобальная (распределенная, составная) сеть (WAN) образуется путем объединения нескольких локальных сетей с помощью устройств и протоколов сетевого Уровня 3 семиуровневой эталонной модели OSI.
Два стека протоколов устанавливаются на интерфейсах устройств, чтобы поддерживать оба протокола IPv4 и IPv6, причем, IPv6 является привилегированным.
Идентификатор интерфейса задает адрес узла (интерфейса) в сети.
Интерфейсы маршрутизаторов обеспечивают как локальные, так и глобальные соединения.
Логический адрес узла в IP-сетях версии **IPv4** содержит 32 двоичных разряда.
Логическое умножение сетевого адреса узла на маску дает адрес сети
Маршрутизация – процесс выбора оптимального пути пакета.
Маски переменной длины (VLSM) позволяют создавать подсети разного размера, гибко задавая границы между полем адреса сети и полем адреса узла.
Многоадресный (multicast) класс адресации D.
Префикс – общая часть адреса, образованная старшими разрядами, одинаковая для всех узлов сети.
Протокол динамического конфигурирования узлов Dynamic Host Configuration Protocol (**DHCP**) позволяет узлу динамически без участия администратора получать IP-адрес.
Стандартная маска адреса класса A имеет 8 единиц в старших разрядах и 24 нуля в младших.
Стандартная маска адреса класса B имеет 16 единиц в старших разрядах и 16 нулей в младших.
Стандартная маска адреса класса c имеет 24 единицы в старших разрядах и 8 нулей в младших.
Старшие разряды адреса IPv4 являются номером сети**, младшие разряды –** номером узла в сети.
Транслятор сетевых адресов NAT переводит частный адрес в общественный.
Транслятор сетевых адресов PAT один общедоступный адрес комбинирует с набором номеров порта узла источника.
Частными адреса блокируется маршрутизатором.

Ключевые термины лекции 7

Адрес следующего перехода (next hop**)** – сетевой адрес входного интерфейса следующего маршрутизатора на пути к адресату назначения.
Главные функции маршрутизаторов: **выбор наилучшего пути** для пакетов к адресату назначения; **продвижение** (коммутация) принятого пакета с входного интерфейса на соответствующий выходной интерфейс.
Интерфейсы (порты) маршрутизатора **имеют уникальные адреса**.
Конфигурационный файл (Configuration File) – содержит команды и параметры для управления потоком трафика, проходящим через маршрутизатор. Конфигурационный файл используется для выбора сетевых протоколов и протоколов маршрутизации, которые определяют наилучший путь для пакетов к адресуемой сети.
Маршрутизатор ретранслирует пакет, продвигая его с входного интерфейса на выходной, для чего использует сетевую часть адреса назначения, обращаясь к таблице маршрутизации.
Маршрутизаторы – являются наиболее распространенными устройствами межсетевого взаимодействия сетей, подсетей и отдельных пользователей.
Метрика – критерий, на основе которого маршрутизатор выбирает доступный и наиболее рациональный маршрут к адресату назначения.
Протокол разрешения адресов (**ARP) –** реализует процесс нахождения MAC-адреса по известному сетевому адресу (IP-адресу).
Протоколы маршрутизации (**routing protocol**) –позволяют маршрутизаторам автоматически обмениваться информацией о сетевой топологии друг с другом.
Распределенная, составная, глобальная WAN сеть объединяет несколько локальных сетей посредством **маршрутизаторов** (routers).
Сетевые IP-адреса узла назначения и узла источника содержит заголовок пакета.
Таблицы маршрутизации создаются и поддерживаются либо статически (администратором), либо динамически, за счет использования **протоколов маршрутизации**. Основными параметрами являются номер (**адрес**) **сети назначения** и адрес **следующего перехода (next hop)**.
Терминальное оборудование (**DTE**), к которому относится и маршрутизатор, соединяется с сетью провайдера через **канальное коммуникационное оборудование** (**DCE**).
Технологии объединяемых маршрутизатором сетей могут быть различными.
Шлюз по умолчанию (Default gateway) – это интерфейс, через который все пакеты из локальной сети будут передаваться в удаленные сети.

Ключевые термины лекции 8

Автономная система – совокупность сетей, представленных набором маршрутизаторов под общим административным управлением.
Бесклассовая маршрутизация (classless routing) – информация о маске подсети включается в обновления (update).
Время жизни (TTL) ограничивает количество маршрутизаторов, через которые может пройти пакет.
Динамическая маршрутизация – маршрутная информация формируется протоколами маршрутизации в ходе обмена обновлениями (модификациями) между маршрутизаторами.
Загрузка (Load) – загрузка определяется количеством информации, загружающей сетевые ресурсы (маршрутизаторы и каналы).
Задержка (Delay) – это длительность времени прохождения пакета от источника до адресата назначения.
Идентификационный номер пакета – единый для всех фрагментов при фрагментации.
Извещение о состоянии соединения (**LSA**) – передается всем соседним маршрутизаторам, когда происходят изменения в маршрутах или каналах.
Количестве переходов (hop count) – метрика расстояния на пути от узла источника к адресату назначения.
Маршрутизации на основе классов (classful routing) – не включает информацию о маске подсети в модификацию (update).
Маршрутизирующие (routing) **протоколы** сетевого уровня создают и поддерживают таблицы маршрутизации. Они **разделяют сетевую информацию** между маршрутизаторами.
Метод мгновенных обновлений (triggered update) – рассылка модификаций производится сразу, как только маршрутизатор обнаружит какие-либо изменения в сети, не дожидаясь окончания периода обновления.
Метрика – критерий наиболее рационального пути в сеть назначения.
Надежность (Reliability) – надежность определяется интенсивностью ошибок на каждом сетевом соединении.
Обновления маршрутной информации или **модификации** (updates) реализуются путем связи и обмена между маршрутизаторами.
Поле смещения данных задает смещение в байтах поля данных этого пакета от начала общего поля данных исходного не фрагментированного пакета.
Поле типа сервиса позволяет в мультисервисных сетях организовать систему приоритетов, т.е. **систему качества обслуживания QoS**.
Полоса пропускания (Bandwidth) – способность соединения передавать данные с некоторой скоростью.
Принцип расщепления горизонта (split horizon) – метод борьбы с маршрутными петлями, согласно которому нельзя посылать информацию маршрутизатору об изменениях в сети в обратном направлении.
Протокол маршрутизации RIP – протокол вектора расстояния, использует в качестве метрики число переходов на пути к адресату назначения.

Протоколы вектора расстояния (distance-vector) определяют расстояние и направление, т.е. вектор некоторого соединения в составной сети.
Протокол Routing Information Protocol (**RIP**) использует в качестве метрики число переходов (hop count) на пути к адресату назначения. Максимальное значение метрики не может превышать 15.
Протоколы состояния канала (link-state) создают полную картину топологии сети и вычисляют кратчайший путь ко всем сетям назначения. Наиболее известным является протокол Open Shortest Path First (**OSPF**).
Сетевые (routed) **протоколы** определяют формат пакета, логические адреса узла источника и назначения, прокладывают маршрут пакета на основе имеющихся таблиц маршрутизации.
Сети без предварительного соединения отправителя и получателя сообщения (connectionless) передают пакеты (дейтаграммы) с использованием протокола IP.
Сети с предварительным соединением отправителя и получателя (connection-oriented) производят подтверждение принятых данных.
Статическая маршрутизация – маршрутная информация конфигурируется сетевым администратором.
Стоимость (Cost) –это обобщенный параметр затрат на передачу пакета к адресату назначения.
Сходимость (конвергенция) – это процесс согласования между всеми маршрутизаторами сети информации о доступных маршрутах.
Таблица маршрутизации хранит адреса всех доступных сетей назначения.
Фрагментация пакета – разбиение пакета большого размера на более мелкие

Ключевые термины лекции 9

Включение интерфейса производится по команде **no shutdown**, а **выключение** – командой **shutdown**.
Защита паролем виртуальных линий **vty 0 4** служит для организации удаленного доступа по протоколу Telnet.
Команда clock rate задает скорость передачи данных в битах в секунду
Команда configure terminal – служит для перехода в режиме глобального конфигурирования.
Команда copy running-cofig startup-config производит сохранение созданного конфигурационного файла.
Команда enable – служит для перехода в привилегированный режим.
Команда interface в глобальном режиме конфигурации используется, чтобы войти в режим детального конфигурирования интерфейса.
Команда service password-encryption – распространяет режим криптографирования на все виды паролей.
Команда show running-configuration – можно посмотреть все параметры и установки маршрутизатора, она выполняется из привилегированного режима.

Команды enable secret и **enable password** используются для защиты паролем входа в привилегированный режим.
Консольный порт – служит для прямого подключения маршрутизатора к компьютеру для конфигурирования.
Конфигурационный файл (startup configuration) –хранится в NVRAM.
Пользовательский режим (user mode) – используется для просмотра ограниченного количества состояний устройства, а также для перехода в привилегированный режим.
Привилегированный режим (privileged mode) – используется для просмотра всех установок устройства, а также для перехода в режим глобального конфигурирования.
Режим ROM monitor – выполняет процесс начальной загрузки и обеспечивает диагностику аппаратных средств.
Режим Boot ROM – позволяет записывать операции во флэш-память и модифицировать операционную систему Cisco IOS.
Режим setup – создания конфигурационного файла в процессе диалога.
Установка IP-адреса интерфейса производится следующей командой:
`Router_A(config-if)#` **`ip address`** *адрес маска*

Ключевые термины лекции 10

Административное расстояние –определяет источник задаваемого маршрута. Меньшее административное расстояние означает более надежный источник.
Динамическая маршрутизация – создается протоколом маршрутизации.
Количество переходов (hop count) – метрика протокола **RIP.**
Команда ip classless используется, чтобы маршрутизатор не уничтожал пакеты с неизвестными ему подсетями назначения, а отправлял эти пакеты по маршруту умолчания.
Команда ip route – используется для конфигурирования статической маршрутизации и содержит: адрес сети назначения, сетевую маску и адрес входного интерфейса следующего маршрутизатора на пути к адресату.
Команда no ip route – удаляет статический маршрут.
Команда show ip route – используется для проверки таблиц маршрутизации.
Команда show running-config – одна из основных команд отладки сети.
Статическая маршрутизация – создается администратором вручную.

Ключевые термины лекции 11

Алгоритм DUAL вычисляет маршруты свободные от маршрутных петель.
Баланс маршрутов – пакеты поочередно посылаются адресату через разные соединения при наличии нескольких маршрутов с одинаковой метрикой.
Дочерняя сеть – подсеть родительской сети.

Маска wildcard-mask – получается путем инвертирования обычной маски.
Номер автономной системы – должен быть одинаковым на всех маршрутизаторах, использующих протокол **Enhanced IGRP**.
Обновления (update) маршрутной информации протокола RIP не передают значения маски подсетей. Они передаются периодически каждые 30 сек.
Пакеты Hello протокола EIGRP служат для контроля связи с соседними маршрутизаторами.
Преемник (successor) – адрес следующего перехода (next hop) или шлюз, в терминах протокола EIGRP.
Протокол EIGRP в качестве метрики по умолчанию использует параметры полосы пропускания и задержки, характеризуется быстрой сходимостью (конвергенцией) и отсутствием маршрутных петель.
Протокол EIGRP поддерживает **Таблица топологии, Таблицу соседних устройств** и **Таблицу маршрутизации.**
Протокол RIPv2 поддерживает маски переменной длины VLSM и бесклассовую междоменную маршрутизациюCIDR
Родительская сеть – сеть одного из классов (A, B, C) со стандартной маской.
Таблица соседних устройств – содержит адреса входных интерфейсов соседних маршрутизаторов, типы собственных выходных интерфейсов, значение текущего времени и другую информацию.
Таблица топологии фиксирует любые изменения топологии, которые затем используются в таблице маршрутизации.

Ключевые термины лекции 12

Административное расстояние протокола OSPF – 110
Алгоритм Dijkstra выбора первого кратчайшего пути (shortest path first algorithm) – позволяет формировать пути свободные от маршрутных петель.
База данных состояний соединений (link-state database) – хранит полную информацию о состоянии каналов связи.
Метрика протокола OSPF (**cost)** базируются на полосе пропускания bandwidth. **Метрика (Cost) = 10^8 / Bandwidth.**
Нулевая область (area 0) – является главной или единственной.
Пакет обновлений несет маршрутную информацию при возникновении изменений в сети. В ответ на принятый пакет обновлений посылается **пакет подтверждения**.
Пакеты Hello используются, чтобы устанавливать и поддерживать **отношения смежности** (adjacency) между соседними устройствами.
Период рассылки Hello-пакетов составляет 10 секунд с использованием адресов 224.0.0.5 или 224.0.0.6 многоадресного режима.
Протокол состояния канала – Open Shortest Path First (**OSPF)** характеризуется административным расстоянием 110
Состояние связи (соединения) – описание интерфейса, которое должно включать IP адрес интерфейса, маску подсети, тип сети и так далее.

Суммарное значение метрики всех соединений через сеть рассчитывает алгоритм **Dijkstra** протокола **OSPF**.
Таблицы данных соседних устройств (neighbor table) – содержат идентификаторы устройств.

Ключевые термины лекции 13

Анализируемые параметры (адреса источника**,** адреса назначения**,** протокола и номера порта верхнего уровня) – указываются в списке доступа.
Идентификационный номер списка доступа – определяет тип списка.
Команда `deny any` (запретить все остальное) – присутствует неявно в конце списка и не позволит передавать по сети несоответствующие пакеты.
Сетевые фильтры или **списки доступа** (Access Lists – ACL) – средства защиты сетей. Используются, чтобы разрешать (permit) или запрещать (deny) продвижение пакетов через маршрутизатор.
Стандартные, расширенные, именованные – различные типы списков доступа.
Утверждения (условия) – определяют, следует ли пакеты принимать или отклонять во входных и выходных интерфейсах маршрутизатора.

Ключевые термины лекции 14

Безопасность портов (port security) коммутаторов обеспечивается различными методами.
`Виртуальный интерфейс` vlan 1 `введен` для управления `коммутатором.`
Максимальное число MAC-адресов узлов, которым разрешено присоединяться к данному интерфейсу коммутатора, повышает безопасность.
Параметры, конфигурируемые на коммутаторе (IP-адрес, шлюз по умолчанию, маска), необходимы для целей управления.
Пароли на коммутаторе конфигурируются так же, как на маршрутизаторе
Режимы реагирования системы на нарушения безопасности – различны, по умолчанию режим реагирования установлен в состояние «**Выключение**» (Shutdown).
Таблица коммутации (таблица MAC-адресов) может формироваться, изменяться и дополняться в статическом или динамическом режиме.

Ключевые термины лекции 15

Виртуальные локальные сети (VLAN) – повышают безопасность и гибкость топологических решений.

Маркировка пакета (tagging) – обеспечивает механизм управления потоком данных.
Режим доступа (mode access) – служит для подключения пользователей к портам коммутатора.
Режим транк (mode trunk) – служит для создания агрегированного логического канала.
Сети VLAN – реализуют сегментацию сети на широковещательные домены на базе коммутаторов.
Сеть по умолчанию – сеть VLAN1 служит для целей управления.
Стандарт IEEE 802.1Q – предусматривает введение поля меток (тег).
Транк (trunk**)** – агрегированный логический канал, заменяющий совокупность физических каналов между устройствами.
Уникальный идентификатор кадра **тег** виртуальной сети определяет членство VLAN каждого пакета.

Ключевые термины лекции 16

Глобальные сети (**WAN**) обеспечивают связь между далеко расположенными локальными сетями, удаленными пользователями.
Канальное оборудование (**DCE**) соединяет центральный офис провайдера (CO) с локальной петлей. Оборудование DCE обеспечивает провайдер, который предоставляет услуги для DTE.
Коммутаторы-маршрутизаторы имеют много портов, характеризуются высокой производительностью и функцией маршрутизации.
Короткие идентификаторы в сетях с предварительным соединением помечают каждое соединение маршрута, идентификаторы хранятся в таблице коммутации.
Последняя миля (last-mile) или местная петля (local loop) – это система кабелей и оборудования, которая соединяет оборудование помещения клиента (**CPE**) с центральным офисом (**CO**) поставщика услуг.
Протокол высокоуровневого управления соединением (**HDLC**) установлен по умолчанию на всех устройствах Cisco. Поле адреса длиной 1 – 2 байта может содержать уникальный, групповой или широковещательный адрес.
Протокол точка-точка (**PPP**) адреса задает формально. Поле адреса всегда содержит широковещательный адрес 11111111.
Терминальное оборудование (**DTE**), например, маршрутизатор, готовит данные и передает их по локальной петле в сеть провайдера.
Устройство согласования с каналом (**CSU/DSU**) для цифровых линий может быть встроено в интерфейс маршрутизатора.

Список терминов и сокращений

A

ACL – Access Control List – список контроля доступа, список доступа.
Acknowledgment – подтверждения принятых данных, подтверждение доставки.
ATM – Asynchronous Transfer Mode – асинхронный способ передачи данных.
ARP – Address Resolution Protocol **–** протокол разрешения адресов.

B

Bandwidth – полоса пропускания.
BDR – Backup Designated Router – запасной назначенный маршрутизатор.
BGP – Border Gateway Protocol **–** протокол граничного шлюза.
Best-effort delivery – доставка по возможности, доставка с наибольшими возможными усилиями.
Bridge – мост.
Broadcast – широковещательная передача, широковещание.
Bus – шина.
Bootstrap – загрузчик, программа начальной загрузки.

C

CDMA – Code Division Multiple Access – множественный доступ с кодовым разделением.
Checksum – контрольная сумма
CIDR – classless interdomain routing – бесклассовая междоменная маршрутизация.
Classless routing – бесклассовая маршрутизация
CLI – command-line interface – интерфейс командной строки.
Connectionless protocol – протокол, не ориентированный на соединение, протокол дейтаграммного типа (без предварительного соединения отправителя и получателя)
Connection-oriented protocol – протокол ориентированный на предварительное соединение отправителя и получателя
CSMA/CD – Carrier Sence Multiply Access with Collision Detection – метод множественного доступа к среде с контролем несущей и обнаружением коллизий.
CSU/DSU – Channel Service Unit /Data Service Unit – каналообразующее оборудование, согласующее с каналом устройство.
Cut-through switching – сквозная коммутация или коммутация “на лету”.

D

Data – данные
DA – Destination Address – адрес получателя, адрес назначения.
DCE – Data Circuit-terminating Equipment или Data Communications Equipment – канальное телекоммуникационное оборудование.

Delay – задержка.
DHCP – Dynamic Host Configuration Protocol – протокол динамического конфигурирования узлов.
Distance-vector Protocol – протокол вектора расстояния.
DNS – Domain Name System – система доменных имен.
DR – Designated Router – назначенный маршрутизатор.
DSAP – Destination Service Access Point – адрес точки входа службы назначения.
DSL - Digital Subscriber Line (цифровая абонентская линия)
DSSS – Direct Sequence Spread Spectrum – прямое последовательное расширение спектра.
DTE – Data Terminal Equipment – оконечное или терминальное оборудование.
DWDM – Dense Wave-length Division Multiplexing – плотное спектральное уплотнение по длине волны.

E

EGP – Exterior Gateway Protocol – протокол внешней маршрутизации.
EIGRP – Enhanced Interior Gateway Routing Protocol – расширенный протокол внутренней маршрутизации.
Ethernet – сетевая технология канального уровня.

F

Fiber optic – оптическое волокно.
Flash –флэш-память (энергонезависимая).
Forwarding – перенаправление, продвижение (кадра, пакета).
FTP – File Transfer Protocol – протокол передачи файлов.
FR – Frame Relay – сети трансляции кадров.
Frame – кадр.

G

Gateway Default – шлюз по умолчанию.

H

HDLC – High-level Data Link Control – протокол высокоуровневого управления соединением.
Header – заголовок.
Hop count – количестве переходов (между маршрутизаторами).
Host – конечный узел, абонент, компьютер, хост.
HTTP – Hypertext Transfer Protocol – протокол передачи гипертекстовой информации.
HTTPS – HTTP Secure, защищенный протокол передачи гипертекстовой информации.
Hub – концентратор.

I

IANA – Internet Assigned Numbers Authority – организация, распределяющая адреса в Интернете.
IEEE – Institute of Electrical and Electronics Engineers – Институт инженеров по электротехнике и радиоэлектронике.
IGP – Interior Gateway Protocol – протокол внутренней маршрутизации.
IMAP – Internet Messaging Access Protocol – протокол электронной почты.
IMS – Internet Multi Service – мультисервисная сеть.
IOS – Internetwork Operation System – сетевая операционная система.
IP – Internet Protocol (сетевой протокол)
IPv4, **IPv6** – сетевые интернет протоколы 4-ой и 6-ой версий.
ISDN – Integrated Services Digital Network – цифровая сеть с интегрированными услугами.
ISO – International Standards Organization – международная организация по стандартизации.
ITU – International Telecommunications Union– международный союз телекоммуникаций.

L

LAN – Local Area Network – локальная сеть.
LER – Label switch Edge Router – пограничный маршрутизатор, коммутирующий пакеты по меткам.
Link-state Protocol – протокол состояния канала.
LLC – Logical Link Control – управление логической передачей данных.
LSA – Link-State Advertisement – извещение о состоянии соединения.
LSR – Label Switching Router –маршрутизатор, коммутирующий пакеты по меткам.
Last-mile (**local loop**) – «последняя миля», соединение оборудования помещения клиента (customer premises equipment - **CPE**) с центральным офисом (central office - **CO**) поставщика услуг.

M

MAC – Media Access Control – подуровень управления доступом к среде.
MDA – Mail Delivery Ag**ent –** агент доставки почты.
MPLS – Multi Protocol Label Switching – многопротокольная коммутация по меткам.
MTA – Mail Transfer Agent **–** агент передачи почты.
MUA – Mail User Agent **–** почтовый агент пользователя, почтовый клиент.
Multicast Mode – групповой режим передачи.
Multimode Fiber – многомодовое волокно.
MUX – мультиплексор.

N

NAT – Network Address Translation – трансляция сетевых адресов.
NIC – Network Interface Card – сетевой адаптер, сетевая карта.
NGN – Next Generation Network – сети следующего поколения.

Next hop address – адрес следующего перехода.
NVRAM – non-volatile RAM – энергонезависимая оперативная память, где хранится стартовый (*startup*) конфигурационный файл.

O

OFDM – Orthogonal Frequency Division Multiplexing **–** ортогональное частотное мультиплексирование.
OSI – Open System Interconnection reference model – базовая эталонная модель взаимодействия открытых систем.
OSPF – Open Shortest Path First – открытый протокол маршрутизации по состоянию канала.
OTN оптические транспортные сети.

P

PAT – Port Address Translation – трансляция сетевых адресов с использованием номеров портов.
PDH – Plesiochronous Digital Hierarchy **–** плезиохронная цифровая иерархия.
PDU – Protocol Data Unit – единица данных (протокола).
PDV – Path Delay Value – значение задержки в пути, удвоенная задержка распространения сигнала.
P2P – приложение peer-to-peer.
Peer-to-peer – модель соединения равноправных узлов сети.
POP – Post Office Protocol – протокол электронной почты.
PPP – Point-to-Point Protocol – протокол соединений точка-точка.
Private IP addresses – частные IP-адреса.
Public IP addresses – публичные IP-адреса.

Q

QoS – Quality of Service **–** качество обслуживания.

R

RIP – Routing Information Protocol – протокол маршрутизации на основе вектора расстояния.
Routed protocol – маршрутизируемый протокол (не путать с протоколом маршрутизации!).
Router – маршрутизатор
Routing protocol – протокол маршрутизации, маршрутизирующий протокол.
RTP – Reliable Transport Protocol – протокол надежной доставки.

S

SA – Source Address – адрес отправителя информации, адрес источника.
SDH – Synchronous Digital Hierarchy **–** синхронная цифровая иерархия.
Sequence Number – номер последовательности.
SFD – Start of Frame Delimiter – ограничитель начала кадра.
Singlemode Fiber – одномодовое волокно
SMTP – Simple Mail Transfer Protocol – протокол электронной почты.

SNMP – Simple Network Management Protocol, простой протокол управления сетью.
Socket – сокет, программный интерфейс.
Socket address – комбинация IP-адреса и порта (в сетевой терминологии).
Source Port – порт источник, который посылает данные.
SSAP – Source Service Access Point – адрес точки входа службы источника.
SSH – Secure Shell – протокол удаленного доступа, обеспечивающий шифрование передаваемых данных.
Store-and-forward switching – режим коммутации с промежуточным хранением или буферизацией
STP – shielded twisted pair – экранированная витая пара.
STP – Spanning-Tree Protocol – Протокол STP для предотвращения петель в коммутируемых сетях.
Switch – коммутатор.

T

TCP – Transmission Control Protocol – протокол управления передачей.
Telnet – протокол удаленного доступа, обеспечивающий подключение к командной строке удаленного узла.
TFTP – Trivial FTP – простой протокол передачи файлов.
Token Ring – сетевая технология канального уровня с передачей маркера.
Trunk – **транк** – канал, передающий кадры множества виртуальных локальных сетей, магистральный канал.

U

UDP – User Datagram Protocol – протокол дейтаграмм пользователя.
Updates routing – обновления маршрутизации.
UTP – unshielded twisted pair – неэкранированная витая пара.

V

VLAN – Virtual Local Area Networks – виртуальная локальная сеть.
VLSM – Variable-Length Subnet Mask – маска переменной длины.
Voice over IP – голос поверх IP.
VPN – Virtual private network – виртуальная частная сеть.

W

WAN – Wide Area Network – глобальная сеть.
WAP – Wireless Access Point – точка беспроводного доступа.
WDM – Wave-length Division Multiplexing – спектральное уплотнение по длине волны.
Wi-Fi – стандарт беспроводных локальных сетей.
Window Size – размер окна.
WLAN – Wireless LAN – беспроводные локальные сети.
WWW – World Wide Web – всемирная паутина; сервис предоставляющий доступ к гипертекстовой информации.