ВОРОНЕЖСКИЙ ИНСТИТУТ МВД РОССИИ

А. С. Лукьянов
А. А. Терентьев
А. В. Попов

СЕТЕВЫЕ ТЕХНОЛОГИИ ПЕРЕДАЧИ ДАННЫХ

Учебное пособие

Воронеж
2024

ББК 32.973
Л84

Рецензенты:

Е. В. Шаталов – начальник УГИБДД ГУ МВД России по Воронежской области, кандидат технических наук, полковник полиции;

Е. Н. Селявкин – заместитель начальника отдела информационных технологий, обеспечения эксплуатации автоматизированных информационных систем и межведомственного информационного взаимодействия ЦИТСиЗИ ГУ МВД России по Воронежской области, подполковник внутренней службы.

Лукьянов А. С.

Л84 Сетевые технологии передачи данных : учебное пособие / А. С. Лукьянов, А. А. Терентьев, А. В. Попов. – Воронеж : Воронежский институт МВД России, 2024. – 83 с.

ISBN 978-5-00229-153-3

Учебное пособие предназначено для формирования у обучающихся целостного представления об инфокоммуникационных системах, необходимого для эффективного изучения радиотехнических дисциплин.

В пособии изложены вопросы построения инфокоммуникационных сетей, обеспечивающих высокоскоростную передачу данных. Приведено описание протоколов различных уровней эталонной модели взаимодействия открытых систем и даны современные подходы, обеспечивающие передачу массивов данных за приемлемые отрезки времени.

Предназначено для курсантов и слушателей образовательных организаций МВД России.

Л-60-23(I)-2024 ББК 32.973

ISBN 978-5-00229-153-3

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

В настоящее время важнейшей задачей совершенствования существующей системы связи МВД России является интеграция различных видов связи, т.е. построение инфокоммуникационной сети на основе цифровых технологий, стандартов, протоколов, технических средств.

Компьютерные сети – важная часть сегодняшнего мира, а область их применения охватывает буквально все сферы человеческой деятельности. Последние два десятилетия характеризуются динамичным развитием сетевых технологий, что связано с широкой популярностью, пришедшей к интернету, развитием веб-технологий, потокового аудио и видео, систем обмена сообщениями в реальном времени. Повсеместное использование компьютерных сетей требует от современного пользователя наличия соответствующих знаний и навыков. Сети включают в себя множество концепций и технологий.

В данном пособии предпринята попытка компактного изложения основ технологий компьютерных сетей. Дается общее описание сетевых компьютерных технологий, основы построения и функционирования локальных и глобальных компьютерных сетей, принципы взаимодействия устройств сети, приводятся наиболее важные термины и определения, рассматриваются популярные сетевые службы и сервисы.

Вычислительные сети создаются для эффективного предоставления различных информационно-вычислительных услуг пользователям сети в результате обеспечения быстрого и надежного доступа к аппаратным, программным и информационным ресурсам, распределенным в этой сети.

Так как связь между компонентами вычислительной сети может, как правило, осуществляться на больших расстояниях, в названии технических средств связи это подчеркивается наличием приставки «теле» (на расстоянии), то есть телекоммуникационные средства, или просто телекоммуникации. Всемирная тенденция к объединению компьютеров в сети обусловлена рядом важных причин, таких как ускорение передачи информационных сообщений, возможность быстрого обмена информацией между пользователями, получение и передача сообщений, не отходя от рабочего места, возможность мгновенного получения любой информации из любой точки земного шара, а также обмен информацией между компьютерами разных фирм и производителей, работающих под разным программным обеспечением.

Правовыми основаниями организации систем связи ОВД являются содержащиеся в законах и подзаконных актах правила и предписания, регламентирующие назначение, построение и эксплуатацию систем. Основными документами, определяющими правовую основу, являются:

- Федеральный закон «О связи» от 7 июля 2003г. № 126-ФЗ;
- Приказ МВД России от 23 сентября 2015 г. № 926.

1. СИГНАЛЫ И ЛИНИИ СВЯЗИ

1.1. Понятия и основные характеристики сигналов

Телекоммуникационные системы и сети, взаимодействуя друг с другом, образуют *систему электросвязи* – комплекс технических средств, обеспечивающих электросвязь определенного вида.

Классификация систем электросвязи весьма разнообразна, но в основном определяется видами передаваемых сообщений, средой распространения электрических сигналов (рис. 1.1.) и способами распределения информации: коммутируемые или некоммутируемые сети передачи сообщений.

Рис. 1.1. Классификация систем электросвязи
по видам передаваемых сообщений и среды распространения

Сообщение – форма представления информации для передачи ее от источника информации к потребителю. Применительно к сфере телекоммуникаций *сообщение* – информация, передаваемая с помощью электромагнитных сигналов средствами электросвязи.

Сигнал – материальный носитель или физический процесс, отражающий (несущий) передаваемое сообщение.

Классификация сигналов может быть самой разнообразной, но особый интерес вызывают электрические сигналы, называемые *сигналами электросвязи* и представляющие *электрические напряжения или токи, изменение параметров которых во времени отражает передаваемое сообщение.* К электрическим сигналам относятся: телефонные, телеграфные, факсимильные сигналы, сигналы передачи данных, сигналы телевизионного и звукового вещания, сигналы телеконтроля и телеуправления.

Комплекс технических средств и среды распространения, обеспечивающий передачу первичного сигнала в определенной полосе частот или с определенной скоростью передачи между сетевыми станциями или сетевыми узлами, называется *каналом передачи.* Линейные сигналы при прохождении по среде распространения испытывают ослабление (затухание), подвергаются различным *искажениям* и *помехам*. Для устранения влияния этих факторов на качество передачи сигналов через определенные расстояния в зависимости от вида системы передачи устанавливаются *усилители*, *регенераторы* или *ретрансляторы*, которые вместе со средой распространения образуют *линейный тракт* системы передачи. Первичный сигнал и его параметры представлены на рисунке 1.2.

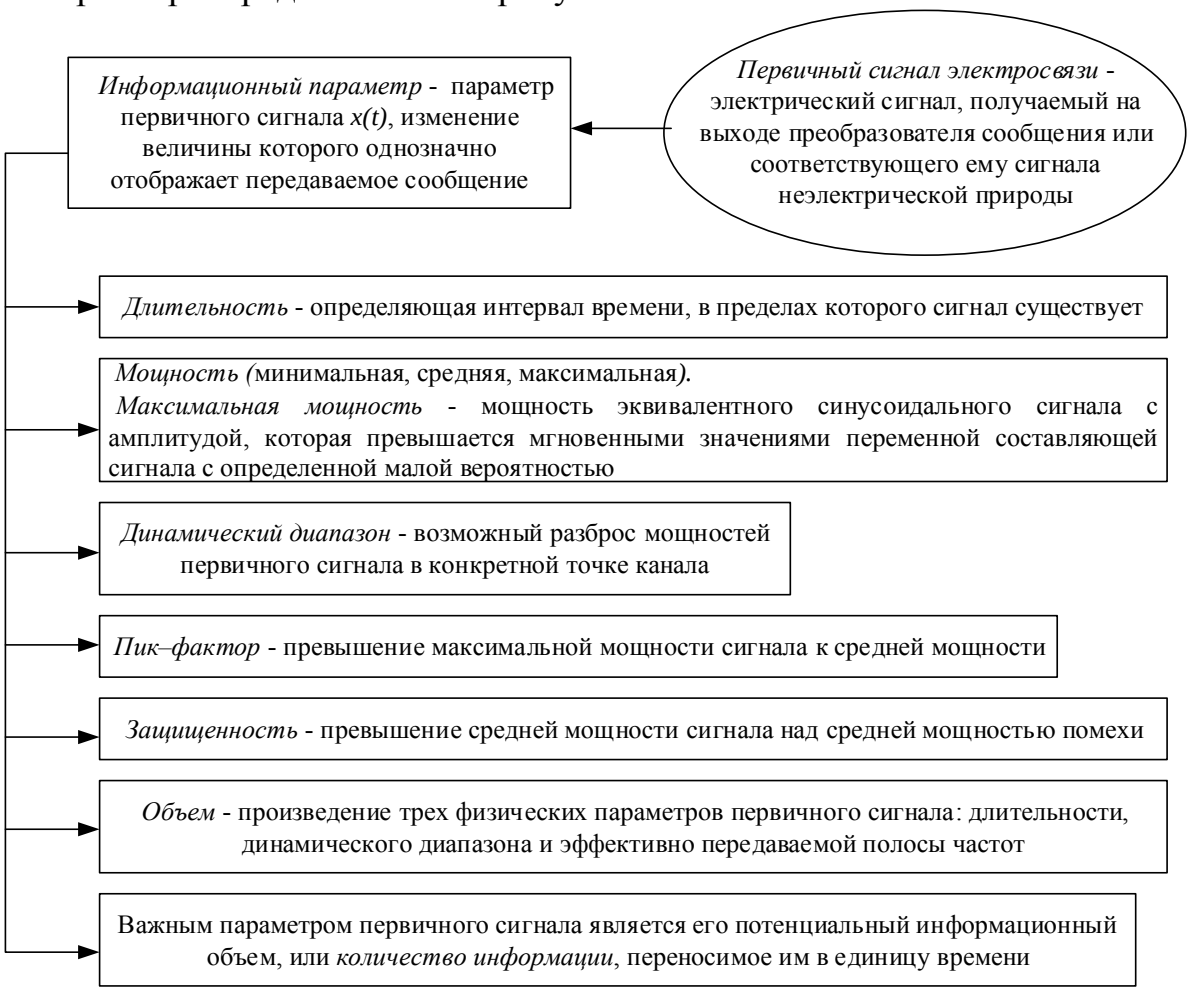


Рис. 1.2. Параметры первичного сигнала

Информационным параметром, например, может быть амплитуда, частота или фаза гармонического электрического сигнала; амплитуда, длительность или фаза импульсов периодической последовательности; структура и разрядность кодовых комбинаций и др.

Первичный сигнал в структуре телекоммуникационных систем и сетей (ТКСС) есть объект *транспортировки*, так как он должен быть передан по каналу от передатчика к приемнику. ТКСС представляет технику *транспортирования* сигнала, а телекоммуникационные сети – специфическую *транспортную сеть*. Поэтому для установления соотношений между параметрами и характеристиками первичных сигналов и свойствами каналов передачи вводят такие параметры и характеристики первичных сигналов, которые просто измерить и по которым можно определить условия их передачи с минимальными искажениями и максимальной защищенностью.

Первичные сигналы электросвязи (непрерывные и дискретные) являются непериодическими функциями времени. Таким сигналам соответствует сплошной спектр, содержащий бесконечное число частотных составляющих. Однако всегда можно указать диапазон частот, в пределах которого сосредоточена основная энергия сигнала (не менее 90%).

Этот диапазон еще называют *эффективно передаваемой полосой частот* сигнала, устанавливаемой экспериментально, исходя из требований качества передачи для конкретного вида первичных сигналов.

Классификация первичных сигналов разнообразна, но наибольшее применение нашла классификация по виду передаваемых сигналов и по виду передаваемых сообщений. Классификация по виду сигналов охватывает аналоговые и цифровые сигналы, узкополосные и широкополосные.

Если отношение граничных частот эффективно передаваемой полосы частот первичного сигнала $F_{макс} / F_{мин} \leq 2$, то такие сигналы называются *узкополосными*, а если $F_{макс} / F_{мин} >> 2$, то такие сигналы называются *широкополосными*.

Аналоговым (непрерывным) сигналом называется сигнал электросвязи, у которого величина представляющих (информационных) параметров может принимать непрерывное множество состояний. Аналоговым сигналом может быть и импульсный сигнал, если один из его параметров (амплитуда, длительность, частота следования, фаза) принимает бесчисленное множество состояний. Пример представлен на рисунке 1.3.

*Цифровым (дискретным) сигнал*ом называется сигнал электросвязи, у которого счетное множество величин одного из представляющих параметров описывается ограниченным набором *кодовых комбинаций.* Примерами таких сигналов являются сигналы передачи данных и телеграфии, телеконтроля и телеуправления, телемеханики и др. (рис. 1.4).

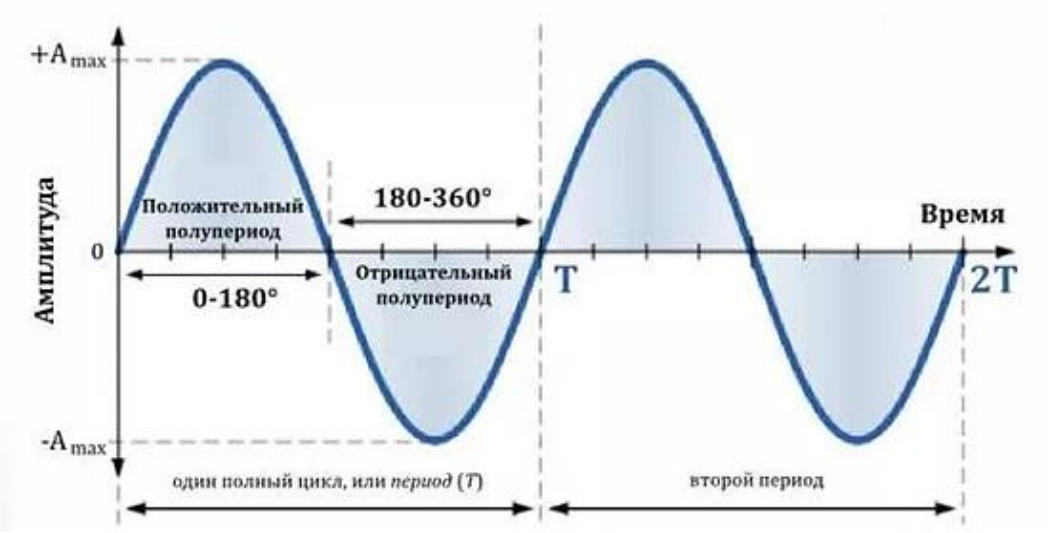


Рис. 1.3. Пример аналогового сигнала

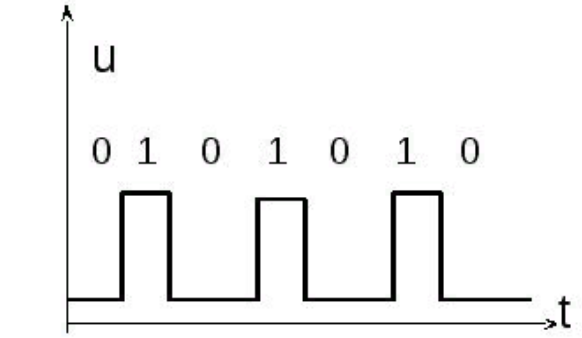


Рис. 1.4. Пример цифрового сигнала

Оцифровка аналогового сигнала складывается из трех операций:

- *дискретизация* сигналов по времени (получение сигнала АИМ) (рис. 1.5);

- *квантование* – процесс сопоставления значений амплитуды взятого дискрета (сигнала АИМ) ближайшему выделенному уровню, т. е. одному из 256 так называемых *уровней квантования* (рис. 1.6);

- *кодирование* основано на замене значения квантованного дискрета восьмиразрядным словом (представление его в виде «00101111»). Квантование и кодирование осуществляются с помощью кодера.

Процесс *дискретизации по времени* – процесс получения мгновенных значений преобразуемого аналогового сигнала с определенным временным шагом, называемым *шагом дискретизации*.

Количество осуществляемых в одну секунду замеров величины сигнала называют *частотой дискретизации* (для достоверной передачи речи частота дискретизации f = 8000 имп/с).

Рис. 1.5. Дискретизация сигнала

Требуемая скорость (ширина) канала для передачи голоса в цифровом виде: 8*8000=64 Кбит/с. (Число разрядов (бит) в канальном интервале – 8, частота дискретизации, имп/с – 8000).

Классификация первичных сигналов по виду передаваемых сообщений охватывает *телефонные (речевые)* сигналы и сигналы *звукового вещания*, сигналы *передачи данных* и *телеграфии*, *телевизионные сигналы* и *факсимильные сигналы*, сигналы телемеханики, телеуправления и телеконтроля, являющиеся частным случаем сигналов передачи данных.

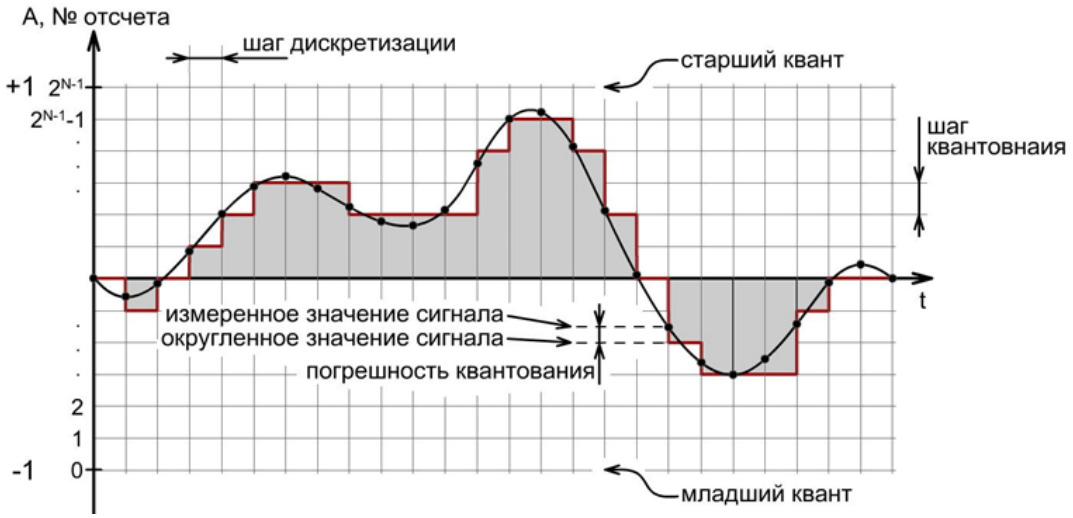


Рис. 1.6. Линейное квантование

Усиленные области частот (форманта) характерны для спектра конкретного звука. Звуки речи различаются друг от друга числом формант и их расположением в частотной области. Поскольку форманты значительно мощнее других составляющих, то они главным образом и воздействуют на ухо слушающего, формируя звучание того или иного звука.

1.2. Кабельные среды передачи данных

Для построения сетей применяются линии связи, использующие различную физическую среду. В качестве физической среды в коммуникациях используются: металлы (в основном медь), сверхпрозрачное стекло (кварц) или пластик и эфир. Физическая среда передачи данных может представлять собой кабель «витая пара», коаксиальный кабель, волоконно-оптический кабель и окружающее пространство. В одной линии связи можно образовать несколько каналов связи (виртуальных или логических каналов), например путём частотного или временного разделения каналов (ЧРК, ВРК).

Под *каналом передачи данных* понимают средства двухстороннего обмена данными, которые включают в себя линии связи и аппаратуру передачи (приёма) данных. Каналы передачи данных связывают между собой источники информации и приёмники информации.

К линиям связи (ЛС) всех видов предъявляются следующие основные требования:

• осуществление связи на практически требуемые расстояния;

• широкополосность и пригодность для передачи различных видов сообщений;

• защищенность цепей от взаимных влияний и внешних помех, а также от физических воздействий (атмосферных явлений, коррозии и пр.);

• стабильность параметров линии, устойчивость и надежность связи;

• экономичность системы связи в целом.

Проводные линии связи используются для передачи телефонных и телеграфных сигналов, компьютерных данных, а также в качестве магистральных. По проводным линиям связи могут быть организованы аналоговые и цифровые каналы передачи данных. Скорость передачи по проводным линиям является относительно низкой.

Кроме того, к недостаткам этих линий относятся слабая помехозащищённость и возможность простого несанкционированного подключения к сети. *Воздушные ЛС* (ВЛС) не имеют изолирующего покрытия между проводниками, роль изолятора играет слой воздуха. Проводники выполняются в основном из биметаллической сталемедной (сталеалюминевой) проволоки, которая подвешивается на деревянных или железобетонных опорах с помощью фарфоровых изоляторов. Используемый частотный диапазон ВЛС не превышает 150 кГц.

Кабельные линии связи имеют довольно сложную структуру. Кабель состоит из проводников, заключённых в несколько слоев изоляции. В сетях используются три типа кабелей:

1. Симметричный провод (twisted pair) состоит из двух совершенно одинаковых в электрическом и конструктивном отношениях изолированных проводников (или несколько пар проводников). Пары проводов скручива-

ются между собой с целью уменьшения наводок. Витая пара является достаточно помехоустойчивой и является дешевым и распространенным видом связи. По конструкции и взаимному расположению проводников различают симметричные и коаксиальные провода и кабели связи (рис. 1.7).

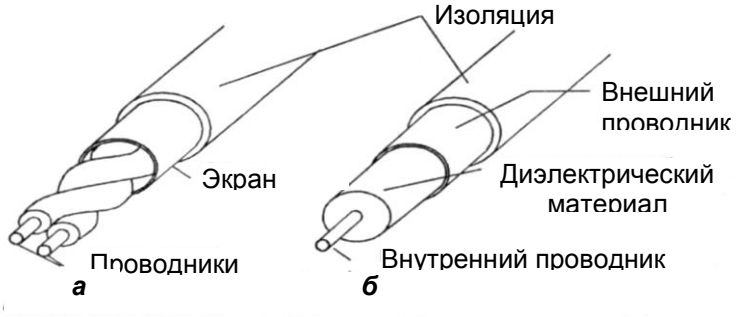


Рис. 1.7. Типичный вид симметричного провода (а) и коаксиального провода (б)

Согласно международному стандарту ISO/IEC 11801 приложение E, для обозначения конструкции экранированного кабеля используется комбинация из трех букв:

- U – неэкранированный,
- S – металлическая оплётка (только общий экран),
- F – металлизированная лента (алюминиевая фольга).

Из этих букв формируется аббревиатура вида xx/xTP, обозначающая тип общего экрана и тип экрана для отдельных пар.

Различают экранированные (STP) и неэкранированные (UTP) симметричные провода. Необходимо различать электрическую изоляцию проводящих жил и электромагнитную. Первая состоит из непроводящего диэлектрического материала (бумаги или полимера). Во втором случае помимо электрической изоляции жилы помещаются внутрь электромагнитного экрана.

Распространены следующие типы конструкции экрана:

- *Неэкранированный кабель* (U/UTP): экранирование отсутствует. Категория 6 и ниже.
- *Индивидуальный экран* (U/FTP): экранирование фольгой каждых отдельных пар. Защищает от внешних помех и от перекрёстных помех между витыми парами.
- *Общий экран* (F/UTP, S/UTP, SF/UTP): общий экран из фольги, оплётки, или фольги с оплёткой. Защищает от внешних электромагнитных помех.
- *Индивидуальный и общий экран* (F/FTP, S/FTP, SF/FTP): индивидуальные экраны из фольги для каждой витой пары, плюс общий экран из фольги, оплётки, или фольги с оплёткой. Защищает от внешних помех и от перекрёстных помех между витыми парами.

Согласно стандартам, кабели делятся на несколько категорий по своей «пропускной способности» и описываются стандартами ANSI/EIA/TIA-568, ISO/IEC 11801, в таблице 1 представлены категории кабелей связи.

Таблица 1

Категории кабелей

Категория	Полоса частот, МГц	Применение
5	100	Fast Ethernet, Gigabit Ethernet (4-парный кабель, используется при построении локальных и для прокладки телефонных линий, поддерживает скорость передачи данных до 100 Мбит/с при использовании 2 пар и до 1000 Мбит/с при 4 пар)
5e	100	Fast Ethernet, Gigabit Ethernet (аналогичен предыдущей категории, но усовершенствованная категория 5 (уточненные/ /улучшенные спецификации), 5e является самым распространённым и используется для построения компьютерных сетей. Преимущества данного кабеля в более низкой себестоимости и меньшей толщине)
6	250	10 Gigabit Ethernet (неэкранированный кабель (UTP) состоит из 4 пар проводников и способен передавать данные на скорости до 10 Гбит/с на расстояние до 55 м.)
6a	500	10 Gigabit Ethernet (аналогичен предыдущей категории только передает данные на расстояние до 100 метров. Добавлен в стандарт в 2008 г. Кабель этой категории имеет либо общий экран (F/UTP), либо экраны вокруг каждой пары (U/FTP))
7	600	10 Gigabit Ethernet (спецификация на данный тип кабеля утверждена только международным стандартом ISO 11801, но не ANSI/TIA-568-C. Скорость передачи данных до 10 Гбит/с. Кабель этой категории имеет общий экран и экраны вокруг каждой пары (F/FTP или S/FTP))
7a	1000	10 Gigabit Ethernet (аналогичен предыдущей категории)
8/8.1	1600-2000	100 Gigabit Ethernet (В разработке, техническая рекомендация ISO/IEC TR 11801-99-1 и международный стандарт ISO 11801 редакция 3. Полностью совместим с кабелем категории 6A. Скорость передачи данных до 40 Гбит/с при использовании стандартных коннекторов 8P8C. Кабель этой категории имеет либо общий экран, либо экраны вокруг каждой пары (F/UTP или U/FTP))
8.2	1600-2000	100 Gigabit Ethernet (почти аналогичен предыдущей категории. Полностью совместим с кабелем категории 7A. Скорость передачи данных до 40 Гбит/с при использовании стандартных коннекторов 8P8C либо GG45/ARJ45 и TERA)

Экранирование применяют в первую очередь для повышения переходного затухания на ближнем и дальнем концах, в целях повышения помехозащищенности. Некоторые типы экранов придают кабелю дополнительную механическую прочность.

Кабели S/STP в сравнении с STP обладают лучшими характеристиками по защите от внешних помех и по уровню ЭМИ.

STP и S/STP кабели следует применять во всех случаях, перечисленных для S/UTP кабелей, когда:

- требуется получение длин кабельных сегментов более 90 м;

- необходимо построение систем передачи данных, для которых электрические характеристики кабелей категории 5 являются недостаточными;
- должны выполняться повышенные требования по защите от несанкционированного доступа к передаваемой информации.

UTP кабели в сравнении с экранированными обладают следующими преимуществами:

- меньшая стоимость;
- меньшая трудоемкость монтажа и эксплуатации;
- отсутствие повышенных требований к внутреннему заземляющему контуру здания;
- лучшие массогабаритные показатели;
- меньший радиус изгиба.

Основными преимуществами экранированных конструкций являются потенциально лучшая защита от внешних электромагнитных наводок, повышенная механическая прочность в случаях применения оплеточных экранов и лучшая защита от несанкционированного доступа к передаваемой информации. Высокая теплопроводность металлических элементов в некоторых типах экранов обеспечивает эффективный отвод тепла, возникающего в проводниках в процессе передачи информации.

2. Коаксиальный кабель (coaxial cable) – кабель с центральным медным проводом, окружённым слоем изолирующего материала для того, чтобы отделить центральный проводник от внешнего проводящего экрана (медной оплетки или слой алюминиевой фольги). Внешний проводящий экран кабеля покрывается изоляцией (рис. 1.8).

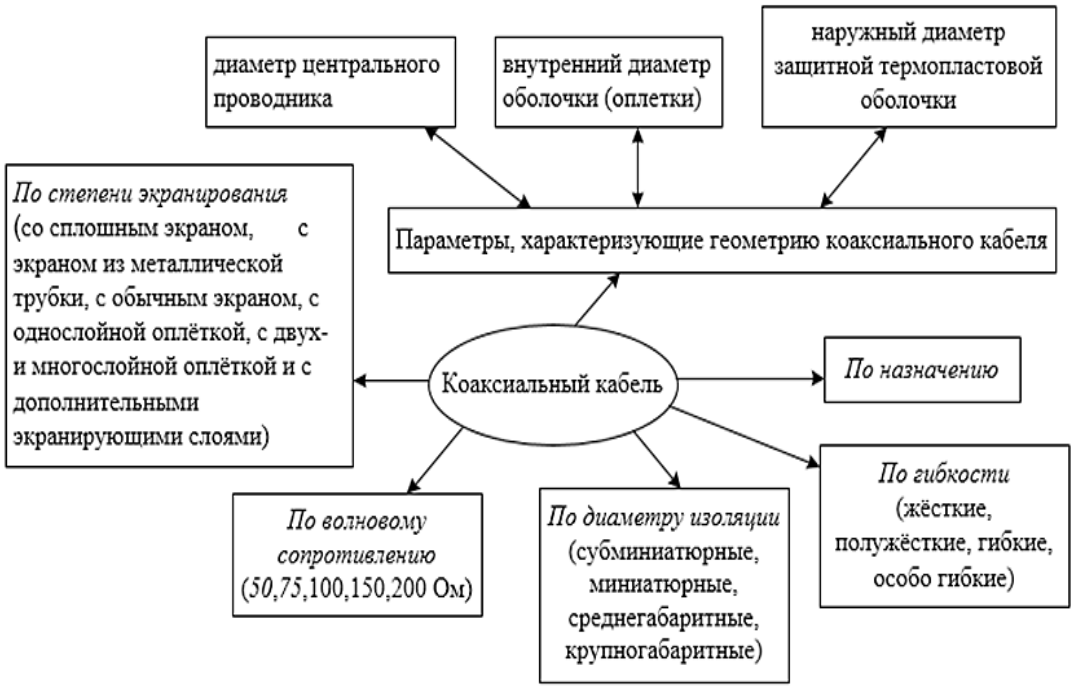


Рис. 1.8. Классификация коаксиального кабеля

Существует два типа коаксиального кабеля: тонкий коаксиальный кабель диаметром 5 мм и толстый коаксиальный кабель диаметром 10 мм. У толстого коаксиального кабеля по сравнению с тонким отмечается меньшее затухание. Стоимость коаксиального кабеля выше стоимости витой пары и выполнение монтажа сети сложнее, чем для витой пары. Коаксиальный кабель более помехозащищенный, чем витая пара и снижает собственное излучение. Пропускная способность от 50 до 100 Мбит/с.

Допустимая длина линии связи – несколько километров. Несанкционированное подключение к коаксиальному кабелю сложнее, чем к витой паре. Структура коаксиального кабеля представлена на рисунке 1.9.

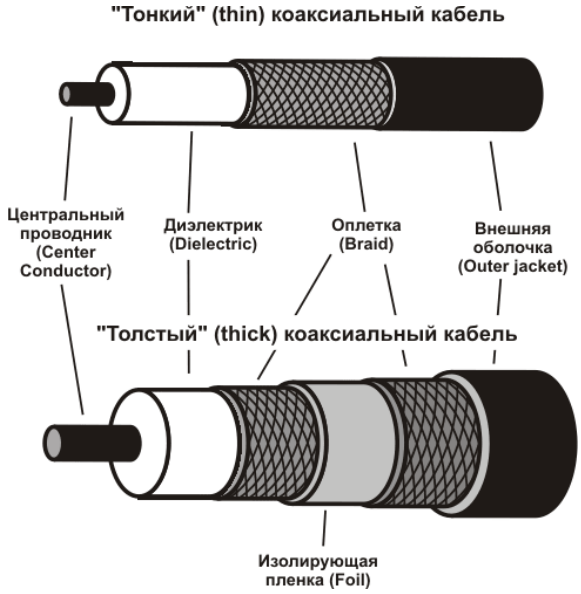


Рис. 1.9. Структура коаксиального кабеля

Цепи линии связи (ЛС) постоянно находятся под воздействием сторонних электромагнитных полей различного происхождения.

Выделяют две основные группы источников сторонних полей:

- *внутренние* – соседние физические и искусственные цепи данной линии связи;

- *внешние* – энергетически и конструктивно не связанные с линией связи.

Внешние источники помех, в свою очередь, по-своему происхождению делятся на:

- *естественные* – грозовые разряды, солнечная радиация и пр.;

- *созданные человеком* – высоковольтные линии передачи, радиостанции, линии электрифицированных железных дорог, электрические сети промышленных предприятий и отдельные энергоемкие устройства.

3. Волоконно-оптический кабель (ВОК) – оптическое волокно на кремниевой или пластмассовой основе, заключённое в материал с низким коэффициентом преломления света, который закрыт внешней оболочкой. Оптическое волокно передаёт световые сигналы (мода) только в одном направлении, поэтому кабель состоит из двух волокон, которые позволяют

передавать огромное количество информации. На передающем конце ВОК необходимо преобразовать электрический сигнал в световой, а на приёмном конце необходимо произвести обратное преобразование (рис. 1.10).

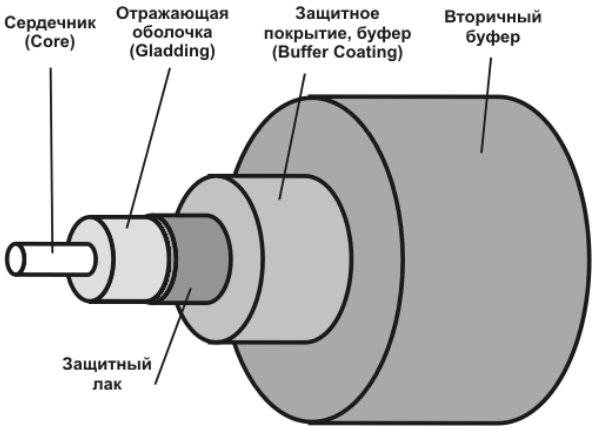


Рис.1.10. Структура волоконно-оптического кабеля

Среди основных преимуществ этого типа кабеля можно выделить следующие:

- чрезвычайно высокий уровень помехозащищённости и отсутствие излучения;
- большая пропускная способность;
- малые масса и габариты;
- надежная техника безопасности;
- долговечность.

Произвести несанкционированное подключение очень сложно. Скорость передачи данных составляет примерно 3 Гбит/с.

Среди основных недостатков оптоволоконного кабеля можно выделить сложность его монтажа, небольшую механическую прочность и чувствительность к ионизирующим излучениям.

Основными способами увеличения пропускной способности в волоконно-оптических системах передачи информации (ВОСПИ) являются методы уплотнения:

- пространственное уплотнение;
- модовое (угловое) уплотнение (МУ);
- временное уплотнение (ТДМ);
- спектральное уплотнение.

Пространственное уплотнение

Состоит в увеличении числа оптических волокон в многожильном волоконно-оптическом кабеле (ВОК), которые разработаны с числом волокон 2, 4…12, 24…144 и т. д. как ленточного, так и радиально-симметричного типов. Увеличение числа волокон в кабелях связи способствует многократному увеличению пропускной способности ВОСПИ, но осложняет проблему соединения таких кабелей.

Модовое (угловое) уплотнение (МУ)

Состоит в передаче оптических сигналов по многомодовому оптическому волокну на разных оптических модах волновода, а также используется свойство сохранять угловую ориентацию раздельно возбужденной группы мод. В видимой области спектра число рабочих каналов при МУ может составлять несколько десятков – сотен. Данный способ уплотнения пригоден к использованию лишь для линий передачи малой, менее 200 м протяженности и при сравнительно низких скоростях передачи сигналов.

Временное уплотнение (TDM)

Состоит в увеличении частоты передачи сигналов, т. е. в использовании при передаче (в цифровом режиме кодирования) импульсных сигналов минимальной деятельности и скважности. При использовании внешних волноводных модуляторов максимальная частота модуляции оптических сигналов достигает нескольких сотен Гбит/с.

Спектральное уплотнение (WDM) (уплотнение по длинам волн)

Состоит в одновременной передаче по одножильному оптическому кабелю нескольких оптических сигналов с различными длинами волн несущих. Является альтернативой метода пространственного уплотнения. При этом достигается значительный экономический эффект за счет сокращения стоимости используемого волокна в линейном кабеле. Данный метод позволяет обеспечивать развитие сети без проведения дополнительных строительных работ. В пределах спектральной полосы прозрачности кварцевого волокна можно разместить несколько информационных сигналов и тем самым многократно увеличить пропускную способность одножильного ВОК.

Одним из важных преимуществ спектрального уплотнения является наиболее полное использование сверхширокой спектральной полосы пропускания оптического волокна (ОВ).

В обычных WDM-системах (Wavelength Division Multiplexing) расстояние между спектральными несущими в ИК-диапазоне длин волн может составлять единицы-десятки нм при ширине спектра излучателей около 0.1 нм. Основные компоненты ВОСПИ представлены на рисунке 1.11.

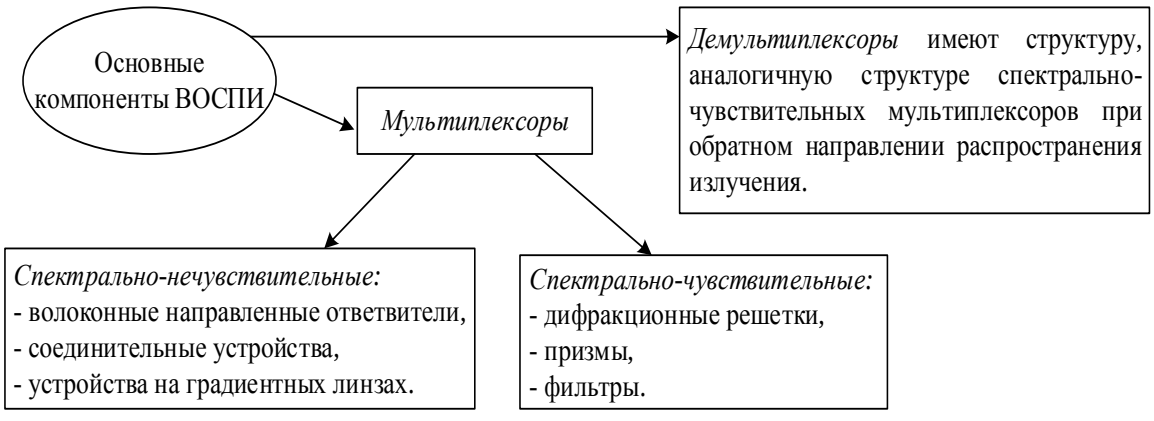


Рис. 1.11. Основные компоненты ВОСПИ со спектральным разделением

Мультиплексоры-демультиплексоры для ВОСПИ со спектральным уплотнением должны обладать минимальными оптическими потерями в рабочих каналах и минимальным уровнем переходных помех. Величина переходного затухания определяется не только разностью длин волн несущих, но и ширинами спектра источника и полосы пропускания фильтра, применяемого в спектральном мульти-демультиплексоре.

Спектральное уплотнение допускает передачу по одномодовому ВОК в каждом из спектральных рабочих каналов информационных сигналов с очень большой частотой и считается одним из перспективных направлений развития магистральных ВОСПИ.

Преимущества ВОЛС настолько значительны, что, несмотря на перечисленные недостатки, эти линии связи очень широко используются на практике. В ВОЛС применяют электромагнитные волны оптического диапазона. Напомним, что видимое оптическое излучение лежит в диапазоне длин волн 380...760 нм. Оптическое волокно (ОВ) изготавливается в виде цилиндров с совмещенными осями и различными коэффициентами преломления. Внутренний цилиндр называется *сердцевиной*, а внешний слой – *оболочкой*. Принцип распространения оптического излучения вдоль оптического волокна основан на отражении от границы сред с разными показателями преломления. Жила ОВ может быть названа оптическим световодом.

Затухание ОВ определяется потерями на поглощение и рассеяние излучения в оптическом волокне. Потери на поглощение зависят от чистоты материала, потери на рассеяние – от неоднородностей показателя преломления материала. Сегодня в мире существует несколько десятков фирм, производящих волоконно-оптические кабели различного назначения. Определяющими параметрами при производстве ВОК являются условия эксплуатации и пропускная способность линии связи.

По условиям эксплуатации кабели подразделяют на монтажные, станционные, зоновые и магистральные. Первые два типа кабелей предназначены для прокладки внутри зданий и сооружений. Они компактны, легки и, как правило, имеют небольшую строительную длину. Кабели последних двух типов предназначены для прокладки в колодцах кабельных коммуникаций, в грунте, на опорах вдоль ЛЭП, под водой. Эти кабели имеют защиту от внешних воздействий и строительную длину более двух километров.

При изготовлении ВОК в основном используются два подхода: конструкции со свободным перемещением элементов и конструкции с жесткой связью между элементами.

1.3. Методика и оборудование для тестирования сетей связи

Развитие инфокоммуникационных возможностей происходит в направлении улучшения параметров передачи данных по уже имеющимся

каналам. Универсальные удобные приборы отличаются надежной и современной конструкцией и предназначены для использования в полевых условиях, а также для решения лабораторных задач.

Под *контрольно-измерительными приборами* (КИП) понимаются устройства для получения информации о состоянии технологических процессов путем измерения их параметров.

Контрольно-измерительные приборы можно классифицировать по следующим основным признакам, представленным на рисунке 1.12.

Рис. 1.12. Классификация основных признаков
контрольно-измерительных приборов

Используется спектр контрольно-измерительных приборов, предназначенных для выполнения определенных измерительных задач. Данные приборы можно разделить на две большие категории по уровням модели OSI, на которых они работают. Это приборы для проведения измерений на физическом уровне или на протокольных уровнях, более подробно виды контрольно-измерительных приборов представлены на рисунке 1.13.

Измерения (односторонние и двухсторонние) проводятся для проверки характеристик коммутаторов, при создании оборудования связи, а также можно быстро выявить причину и место неисправности. Многообразие протоколов и технологий проводных сетей обуславливает широкую номенклатуру средств их тестирования.

На данный момент есть две актуальные методики тестирования сетей на канальном уровне: методика RFC 2544 и методика Y.1564 тестирования сетей.

Рекомендация RFC2544 была разработана в 1999 году и принята IETF. Методика RFC 2544 является стандартом для разнопланового тестирования сетей Ethernet. Она описывает сценарий автоматизированной процедуры тестирования Ethernet канала при отсутствии рабочего трафика. Тест позволяет проверить определенные параметры, описанные в уровне обслуживания (SLA). Методология тестов определяет размеры кадров, продолжительность испытания и число повторений испытаний.

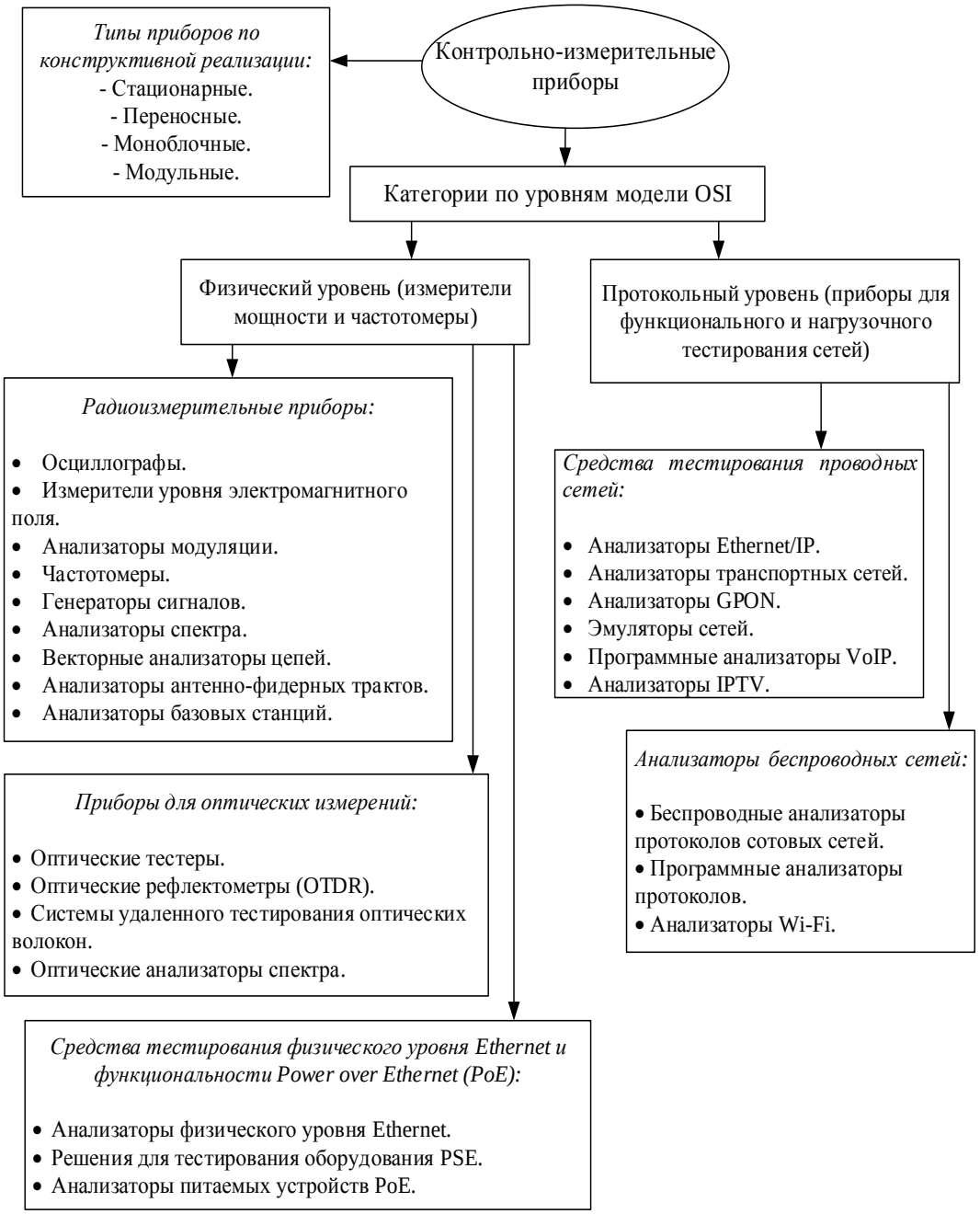


Рис. 1.13. Виды контрольно-измерительных приборов

Есть 4 основных теста:

- Определение пропускной способности (throughput).

Данный тест предназначен для фиксации максимальной скорости коммутации для сетевых элементов, расположенных в транспортных сетях Ethernet.

- Определение задержки распространения (latency).

Анализ временного интервала прохождения кадра от источника к получателю и обратно. При этом величина называется круговой задержкой. При передаче данных с одного порта на второй, измеряется просто задержка передачи. По умолчанию рекомендовано проводить 30 испытаний, по итогам высчитывается средняя задержка.

- Определение зависимости уровня потерь кадров (frame loss rate). С помощью данного теста рассчитывается процент кадров, не переданных сетевым элементом при неизменной нагрузке вследствие недостатка аппаратных ресурсов. Важно учитывать, что большой процент потерь кадров вызывает снижение качества сервиса.
- Определение предельной нагрузки (back-to-back).

Применяется большей частью для тестирования таких сетевых устройств, как концентраторы, коммутаторы и маршрутизаторы.

ITU-T Y.1564 – это методика тестирования активации услуги Ethernet, которая представляет собой новый стандарт ITU-T для включения, установки и устранения неисправностей услуг на базе Ethernet. Это единственная стандартная методология тестирования, которая позволяет полностью проверить соглашения об уровне обслуживания (SLA) Ethernet в одном тесте. Методика Y.1564 предназначена для использования в качестве инструмента проверки соглашения об уровне обслуживания сети (SLA), а также для выполнения среднесрочного и долгосрочного тестирования услуг, подтверждающего, что сетевые элементы могут должным образом предоставлять все услуги, находясь под нагрузкой.

Существует 6 основных тестов:

- Определение пропускной способности или информационной скорости (IR) – это показатель скорости передачи доступных или потребляемых ресурсов передачи данных, выраженный в битах в секунду.
- Определение задержки передачи кадра (FTD) – это измерение временной задержки между передачей и приемом кадра. Обычно это измерение в оба конца, то есть при вычислении одновременно измеряются направления от ближнего конца к дальнему и от дальнего к ближнему.
- Определение вариации задержки кадра (FDV), также известное как джиттер пакетов – это измерение изменений временной задержки между доставками пакетов. В случайные моменты может иметь место приоритезация, что также приводит к отправке пакетов со случайной скоростью. Таким образом, пакеты принимаются нерегулярно. Прямым следствием этого джиттера является нагрузка на принимающие буферы конечных узлов, где буферы могут использоваться чрезмерно или недостаточно при больших колебаниях джиттера.
- Определение коэффициента потери кадров (FLR): обычно выражается в виде отношения, это измерение количества потерянных пакетов по отношению к общему количеству отправленных пакетов. Потеря кадров может быть вызвана рядом проблем, таких как перегрузка сети или ошибки во время передачи.
- Определение коэффициента потери кадров по отношению к SAC: обычно выражается как индикация «прошел / не прошел». SAC (Критерии приемлемости услуг) – это часть SLA операторов сетей, которая ссылается на требования FLR для тестируемого сетевого пути.
- Определение доступности (AVAIL): обычно выражается как % времени работы для тестируемого канала, например, имеет ли сеть 99,999% времени безотказной работы.

2. ОСНОВЫ ОРГАНИЗАЦИИ СЕТЕЙ

2.1. Эталонная модель взаимодействия OSI

Организацией сети называется обеспечение взаимосвязи между рабочими станциями, периферийным оборудованием (принтерами, накопителями на жестких дисках, сканерами, приводами) и другими устройствами. При организации сети одной из задач является согласование различных типов компьютеров за счёт использования общих протоколов.

Протокол является описанием набора правил и соглашений, регламентирующих обмен информацией между устройствами в сети.

Локальные сети служат для объединения рабочих станций, периферии, терминалов и других устройств. Локальная сеть позволяет повысить эффективность работы компьютеров за счет совместного использования ими ресурсов, например, файлов и принтеров.

Характерными особенностями локальной сети являются:

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

Глобальные сети служат для объединения локальных сетей и обеспечивают связь между компьютерами, находящимися в локальных сетях. Глобальные сети охватывают значительные географические пространства и дают возможность связать устройства, расположенные на большом удалении друг от друга.

Когда-то наблюдался значительный рост глобальных сетей. Новые технологии и продукты внедрялись сразу после их появления, и поэтому многие сети были сформированы с использованием различных аппаратных и программных средств. Вследствие этого многие сети оказались несовместимыми между собой и стало сложным организовывать обмен информацией между компьютерами, использующими различные сетевые спецификации.

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

Эталонная модель OSI стала основной архитектурной моделью взаимодействия между компьютерами. Несмотря на то, что были разработаны и другие архитектурные модели, большинство поставщиков сетей ссылаются на их соответствие эталонной модели OSI.

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

Эталонная модель OSI делит задачу перемещения информации между компьютерами через сетевую среду на семь менее крупных и, следовательно, более легко разрешимых подзадач.

Каждая из этих семи подзадач выбрана потому, что она относительно автономна и, следовательно, ее легче решить без чрезмерной опоры на внешнюю информацию. Такое разделение на уровни называется *иерархическим представлением.* Каждый уровень соответствует одной из семи подзадач (рис. 2.1).

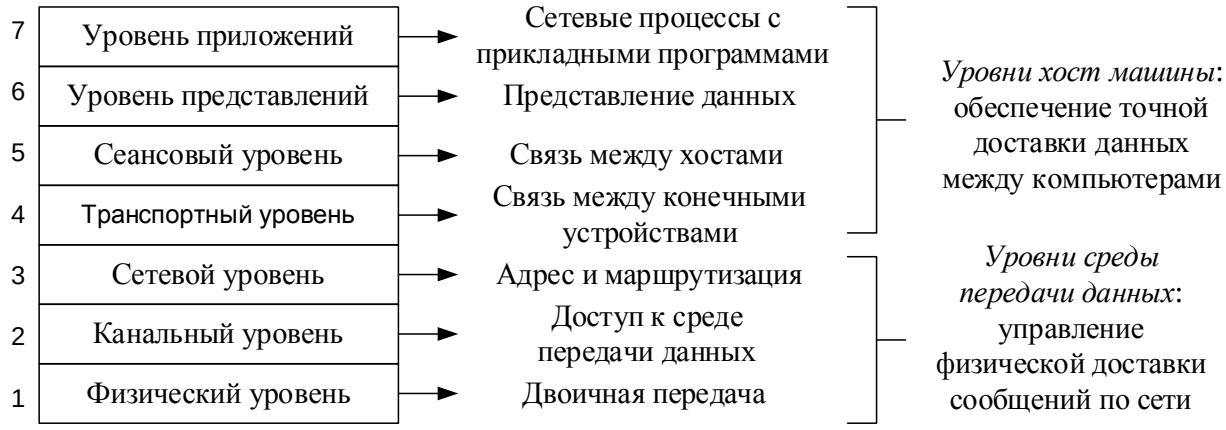


Рис. 2.1. Уровни эталонной модели OSI

Поскольку нижние уровни (с 1 по 3) модели OSI управляют физической доставкой сообщений по сети, их часто называют *уровнями среды передачи данных (media layers).* Верхние уровни (с 4 по 7) модели OSI обеспечивают точную доставку данных между компьютерами в сети, поэтому их часто называют *уровнями хост-машины (host layers)* (рис. 2.2).

В большинстве сетевых устройств реализованы все семь уровней. Однако для ускорения выполнения операций в некоторых сетях сама сеть реализует функции сразу нескольких уровней.

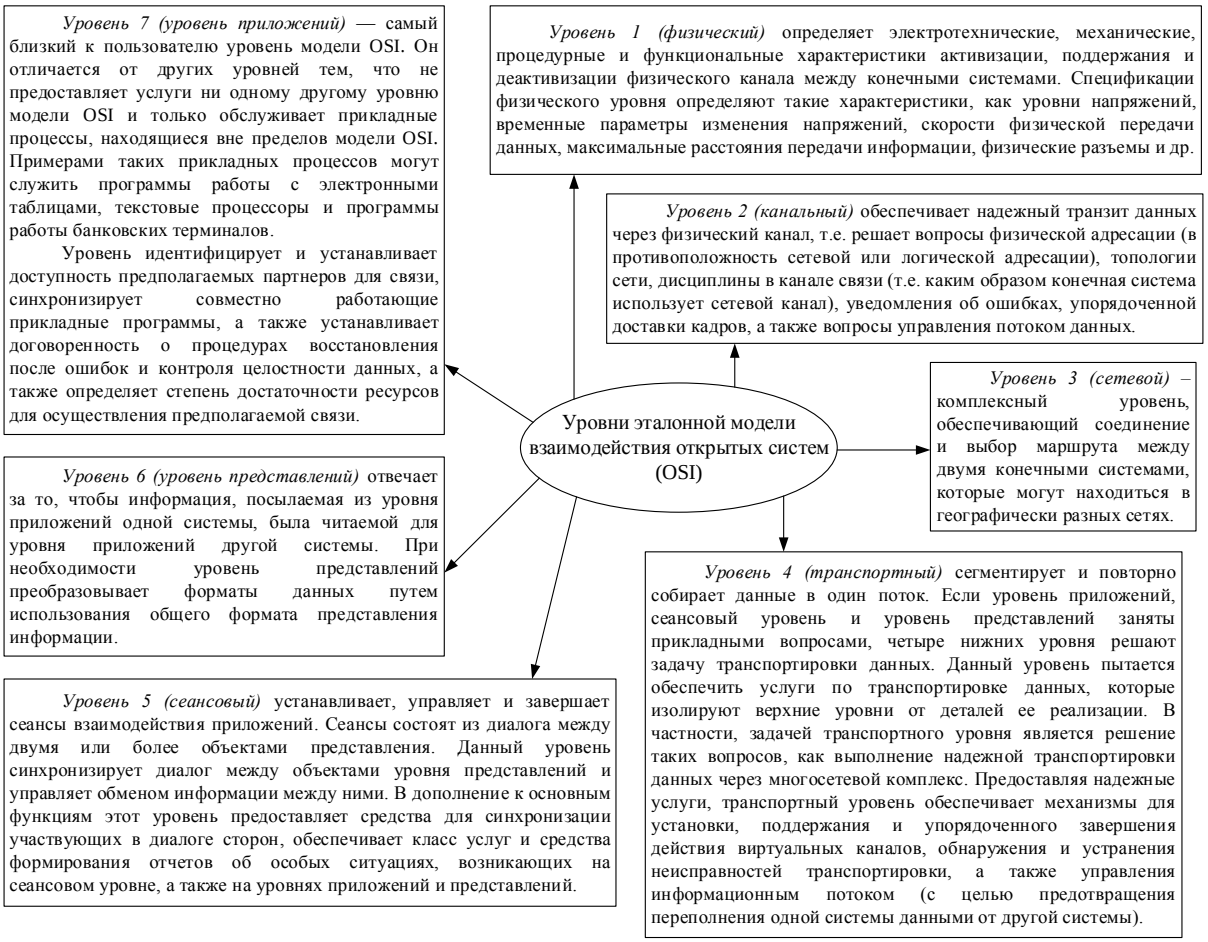


Рис. 2.2. Описание уровней эталонной модели взаимодействия открытых систем (OSI)

Модель OSI не является схемой реализации сети, т.к. она только определяет функции каждого уровня. Поэтому каждый уровень эталонной модели выполняет соответствующие ему функции, определенные стандартом OSI, к которому может обратиться любой производитель сетевых продуктов.

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

– делит взаимосвязанные аспекты работы сети на менее сложные элементы;

– определяет стандартные интерфейсы для автоматического интегрирования в систему новых устройств *(plug-and-play)* и обеспечения совместимости сетевых продуктов разных поставщиков;

– дает возможность инженерам закладывать в различные модульные функции межсетевого взаимодействия симметрию, что позволяет легко наладить их взаимодействие;

– изменения в одной области не требуют изменений в других областях, что позволяет отдельным областям развиваться быстрее;

– делит сложную межсетевую структуру на дискретные, более простые для изучения подмножества операций.

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

Модель OSI исключает прямую связь между равными по положению уровнями, находящимися в разных системах, как показано на рисунке 2.3.

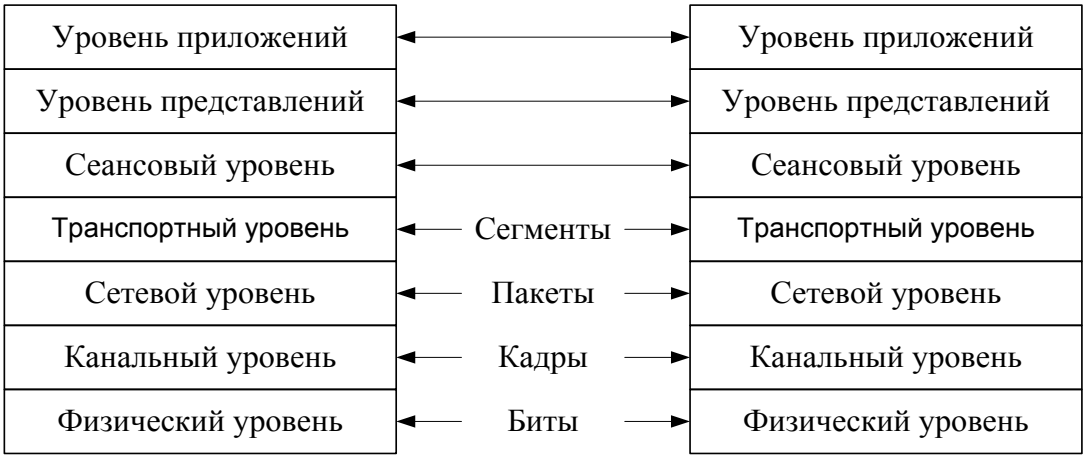


Рис. 2.3. Равные по положению уровни разных систем для связи между собой используют собственные протоколы

Каждый уровень системы имеет свои определенные задачи, которые он должен выполнять. Для этого он должен общаться с соответствующим уровнем в другой системе.

Обмен сообщениями между одноранговыми уровнями (*блоками данных протокола, protocol data units, PDU)* осуществляется с помощью протокола соответствующего уровня. Каждый уровень может использовать свое специфическое название для PDU.

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

Например, в семействе протоколов TCP/IP транспортные уровни для обмена пользуются сегментами (рис. 2.3). Таким образом, TCP-сегменты становятся частью пакетов сетевого уровня (также называемых *дейтаграммами)* и будут участвовать в обмене между соответствующими IP-уровнями. В свою очередь, на канальном уровне IP-пакеты должны стать частью кадров, которыми обмениваются непосредственно соединенные устройствами. В конечном итоге при передаче данных по протоколу физического уровня с использованием аппаратных средств кадры преобразовываются в биты. Информацию, посланную в сеть, называют *данными,* или *пакетами*

данных, или *кадрами.* Если один компьютер (источник) хочет послать данные другому компьютеру (получателю), то данные сначала должны быть собраны в пакеты. Под инкапсуляцией понимается процесс погружения данных в заголовок (или *трейлер*) конкретного протокола перед отправкой их в сеть.

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

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

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

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

При выполнении сетями услуг пользователям поток и вид упаковки информации изменяются.

Инкапсуляция имеет определенные этапы преобразования:

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

2. *Упаковка данных для сквозной транспортировки.* Для передачи через сетевой комплекс данные соответствующим образом упаковываются. Благодаря использованию сегментов транспортная функция гарантирует надежное соединение участвующих в обмене сообщениями хост-машин на обоих концах почтовой системы.

3. *Добавление сетевого адреса в заголовок.* Данные помещаются в пакет или дейтаграмму, которая содержит сетевой заголовок с логическими адресами отправителя и получателя. Эти адреса помогают сетевым устройствам посылать пакеты через сеть по выбранному пути.

4. *Добавление локального адреса в канальный заголовок.* Каждое сетевое устройство должно поместить пакеты в кадр. Кадры позволяют взаимодействовать с ближайшим непосредственно подключенным сетевым устройством в канале. Каждое устройство, находящееся на пути движения

данных по сети, требует формирования кадров для соединения со следующим устройством.

5. *Преобразование в последовательность битов для передачи.* Для передачи по физическим каналам (обычно по кабелям) кадр должен быть преобразован в последовательность единиц и нулей. Функция тактирования дает возможность устройствам различать эти биты в процессе их перемещения в среде передачи данных. Среда на разных участках пути следования может меняться. Например, сообщение электронной почты может выходить из локальной сети, затем пересекать магистральную сеть комплекса зданий и дальше выходить в глобальную сеть, пока не достигнет получателя, находящегося в удаленной локальной сети.

2.2. Сетевые устройства и узлы

Сетевыми устройствами называются аппаратные средства, используемые для объединения сетей. По мере увеличения размеров и сложности компьютерных сетей усложняются и сетевые устройства, которые их соединяют. Однако все сетевые устройства служат для решения одной или нескольких общих задач. На рисунке 2.4 представлены символы следующих сетевых устройств: повторителя, концентратора, моста и маршрутизатора.

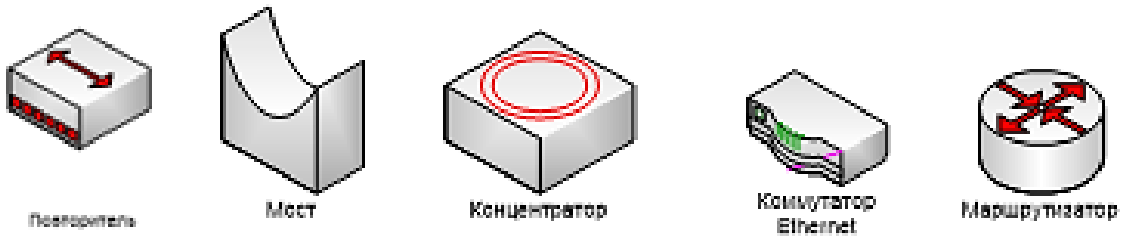


Рис. 2.4. К сетевым устройствам относятся повторители, концентраторы, мосты и маршрутизаторы

В настоящее время повторители и концентраторы практически не используются, т.к. технологии их применения являются устаревшими. Однако в некоторых сегментах сети ОВД ещё возможно их применение. На рис. 2.5 представлены задачи и особенности сетевых устройств.

Повторители относятся к уровню 1 (физическому) эталонной модели OSI. Когда сигналы покидают передающую станцию, они четкие и легко распознаются. Однако, чем длиннее кабель, тем сильнее затухает и ухудшается сигнал. В конечном итоге это приводит к тому, что сигнал уже не может быть правильно распознан. Например, спецификации для витой пары категории 5 кабеля Ethernet устанавливают расстояние 100 метров как максимально допустимое для прохождения сигнала. Если сигнал проходит по сети больше указанного расстояния, то нет гарантии, что сетевой адаптер правильно распознает сигнал.

Повторители позволяют увеличить протяженность сети, гарантируя при этом, что сигнал будет распознан принимающими устройствами. Использование повторителей для увеличения числа узлов сети. При организации сетей общей проблемой является слишком большое количество устройств, подключаемых к сети. Сигналы ухудшаются и становятся более слабыми, поскольку каждое устройство, подключенное к сети, становится причиной небольшого ослабления сигнала. Более того, т.к. сигнал проходит через слишком большое количество рабочих станций или узлов, он может оказаться настолько ослабленным, что принимающее устройство не сможет его распознать. Решить эту проблему можно с помощью повторителей, которые принимают ослабленный сигнал, фильтруют его от помех, усиливают и отправляют дальше в сеть, тем самым увеличивая расстояния, на которых сеть может функционировать. Благодаря этому появляется возможность увеличить число узлов в сети.

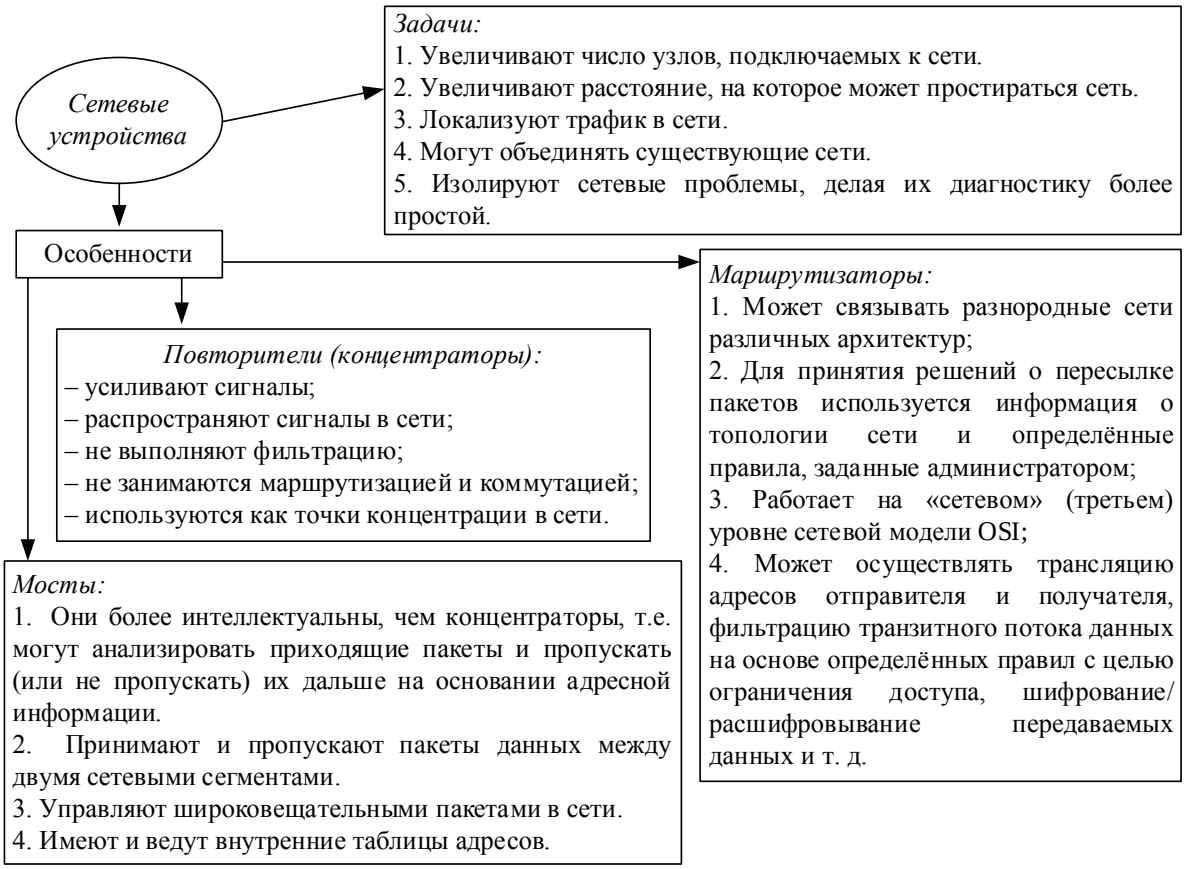


Рис. 2.5. Задачи и особенности сетевых устройств

Концентратор можно представить себе в виде устройства, которое содержит множество независимых, но связанных между собой модулей сетевого оборудования. В локальных сетях концентраторы ведут себя как мультипортовые повторители. В таких случаях концентраторы используются, чтобы разделить сетевые носители и обеспечить множественное подключение. Недостатком использования концентратора является то, что он не может фильтровать сетевой трафик.

Под *фильтрацией* понимается процесс, в ходе которого в сетевом трафике контролируются определенные характеристики, например адрес источника, адрес получателя или протокол, и на основании установленных критериев принимается решение – пропускать трафик дальше или игнорировать его. В концентраторе данные, поступившие на один порт, передаются дальше на все порты. Следовательно, концентратор передает данные во все участки или сегменты сети, независимо от того, должны они туда направляться или нет.

Если имеется только один кабель, связывающий все устройства в сети, или если сегменты сети связаны только нефильтрующими устройствами (например, концентраторами), несколько пользователей могут попытаться послать данные в один и тот же момент времени. Если одновременно пытаются передавать несколько узлов, то возникает *конфликт*. В этом случае данные от разных устройств сталкиваются друг с другом и повреждаются. Одним из методов решения проблемы слишком большого трафика и большого числа конфликтов в сети является использование мостов.

Мосты работают на уровне 2 (канальном) эталонной модели OSI и не занимаются исследованием информации от верхних уровней. Назначение мостов состоит в том, чтобы устранить ненужный трафик и уменьшить вероятность возникновения конфликтов. Это достигается путем разделения сети на сегменты и за счет фильтрации трафика по пункту назначения или MAC-адресу. Мосты фильтруют трафик только по MAC-адресу, поэтому они могут быстро пропускать трафик, представляющий любой протокол сетевого уровня. Так как мосты проверяют только MAC-адрес, то протоколы не имеют для них значения. Как следствие, мосты отвечают только за то, чтобы пропускать или не пропускать пакеты дальше, основываясь при этом на содержащихся в них MAC-адресах. Чтобы фильтровать и, соответственно, выборочно пропускать сетевой трафик, мосты строят таблицы соответствия всех MAC-адресов, находящихся в сети и других сетях.

При поступлении данных на вход моста он сравнивает адрес получателя, содержащийся в пакете данных, с MAC-адресами в своей таблице. Если мост обнаружит, что MAC-адрес пункта назначения данных расположен в том же сегменте сети, что и отправитель, то он не пропустит данные в другой сегмент. Другим типом устройств межсетевого взаимодействия являются *маршрутизаторы.* Как было сказано выше, мосты, прежде всего, используются для соединения сегментов сети. Маршрутизаторы же используются для объединения отдельных сетей и для доступа к ресурсам ИМТС ОВД.

Они обеспечивают сквозную маршрутизацию при прохождении пакетов данных и маршрутизацию трафика между различными сетями на основании информации сетевого протокола или уровня 3 и способны принимать решение о выборе оптимального маршрута движения данных в сети (рис. 2.6).

С помощью маршрутизаторов также может быть решена проблема чрезмерного широковещательного трафика, т.к. они не переадресовывают дальше широковещательные кадры, если им это не предписано.

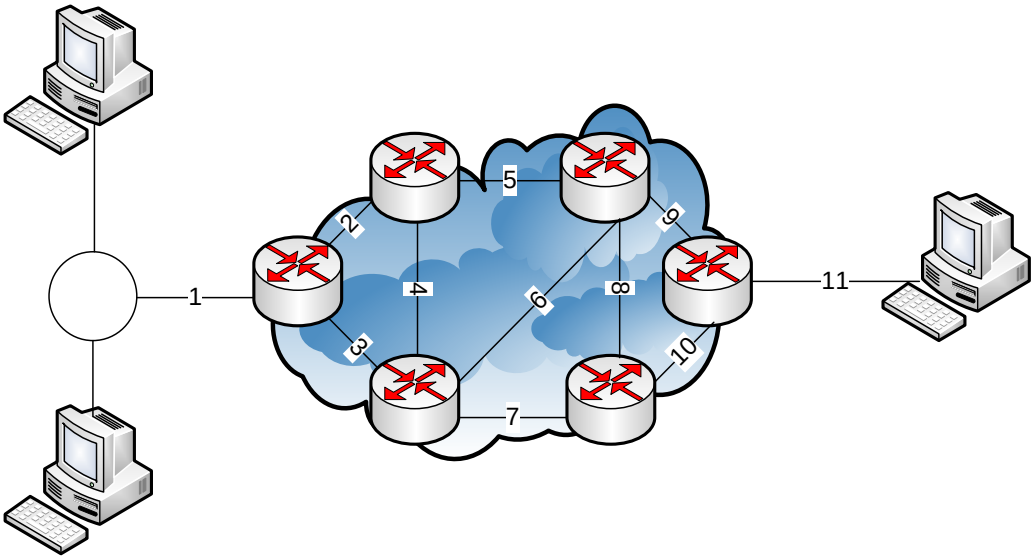


Рис. 2.6. Маршрутизаторы используют уровень 3
для определения оптимального маршрута доставки данных в сети
и помогают сдерживать объём широковещательных пакетов

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

Физические или MAC-адреса обычно устанавливаются производителем сетевого адаптера и фиксируются в адаптере на аппаратном уровне, а IP-адреса обычно назначаются сетевым администратором. Чтобы маршрутизация была успешной, необходимо, чтобы каждая сеть имела уникальный номер. Этот уникальный номер сети включен в IP-адрес каждого устройства, подключенного к сети.

2.3. Функционирование локальных и глобальных сетей

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

Стандарты локальных сетей определяют вид кабельных систем и сигналы на физическом и канальном уровнях эталонной модели OSI.

Рассмотрим стандарты Ethernet и IEEE 802.3 с краткой историей их развития. Ethernet был разработан Исследовательским центром корпорации Xerox в Пало Альто (PARC) в 1970 году и является на сегодняшний день наиболее популярным стандартом. Ethernet стал основой для спецификации IEEE 802.3, которая была выпущена в 1980 году Институтом инженеров по электротехнике и электронике. Вскоре после этого компании Digital Equipment Corporation, Intel Corporation и Xerox Corporation совместно разработали и выпустили спецификацию Ethernet версии 2.0, которая была в значительной степени совместима со стандартом IEEE 802.3. На сегодняшний день Ethernet и IEEE 802.3 являются наиболее распространенными стандартами локальных вычислительных сетей. Сети на основе Ethernet используются для транспортировки данных между различными устройствами – компьютерами, принтерами и файл-серверами. Технология Ethernet дает возможность устройствам коллективно пользоваться одними и теми же ресурсами, т.е. все устройства могут пользоваться одной средой доставки.

Средой доставки называется метод передачи и приема данных.

Ethernet должен был заполнить нишу между глобальными, низкоскоростными сетями и специализированными сетями машинных залов, передающими данные с высокой скоростью, но на очень ограниченные расстояния. Ethernet хорошо подходит для приложений, когда локальные коммуникации должны выдерживать перидически возникающие высокие нагрузки на пиковых скоростях передачи данных.

Стандарты Ethernet и IEEE 802.3 определяют локальные сети с шинной топологией, работающие в монополосном режиме со скоростью передачи 10 Мбит/с. Такие ЛВС называют 10Base. На рисунке 2.7 показан вариант комбинирования трех существующих стандартов выполнения разводки в сетях.

– *10Base2* – известен как тонкий Ethernet, допускает протяженность сетевых сегментов на коаксиальном кабеле до 185 метров;

– *10BaseS* – известен как толстый Ethernet, допускает протяженность сетевых сегментов на коаксиальном кабеле до 500 метров;

– *10BaseT* – использует для передачи кадров недорогой кабель на основе витой пары.

Стандарты 10BaseS и 10Base2 обеспечивают доступ нескольким станциям в одном сегменте ЛВС. Станции подключаются к сегменту с помощью кабеля, который одним концом соединяется с интерфейсом блока подключения *(attachment unit interface, AUI)* на станции, а другим – с трансивером, подключаемым к коаксиальному кабелю Ethernet. Трансивер еще называют *устройством подключения к среде передачи данных (media attachment unit, MAU)*. Поскольку стандарт 10BaseT обеспечивает доступ только для одной станции, то в локальных сетях на базе 10BaseT станции почти всегда подключаются к концентратору или сетевому коммутатору. При подобной конфигурации принято считать, что концентратор или сетевой коммутатор относится к тому же сегменту, что и подключенные к нему станции.

Все работы по монтажу и прокладке сетей на основе витой пары необходимо начинать с составления подробной схемы прокладки кабелей и размещения устройств. При прокладке кабеля UTP соблюдаются следующие условия.

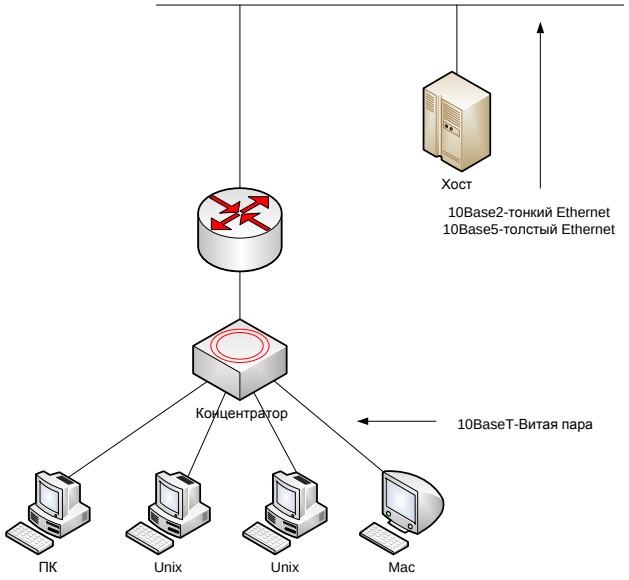


Рис. 2.7. Сеть может объединять в себе различные типы доступа, задаваемые стандартом Ethernet/802.3

Максимальная длина кабеля между розетками или между розеткой и *patch* панелью – 90 метров. Это правило разработано исходя из ограничения максимального расстояния в 100 метров между компьютером и коммутатором. Причем оставшиеся 10 метров отводятся на провод патчкорд (*patch cord*) между розеткой и компьютером, а также розеткой (*patch панелью*) и коммутатором. Для сетей категории 5 может быть не более 3 отрезков кабеля между двумя устройствами (как на рис. 2.8).

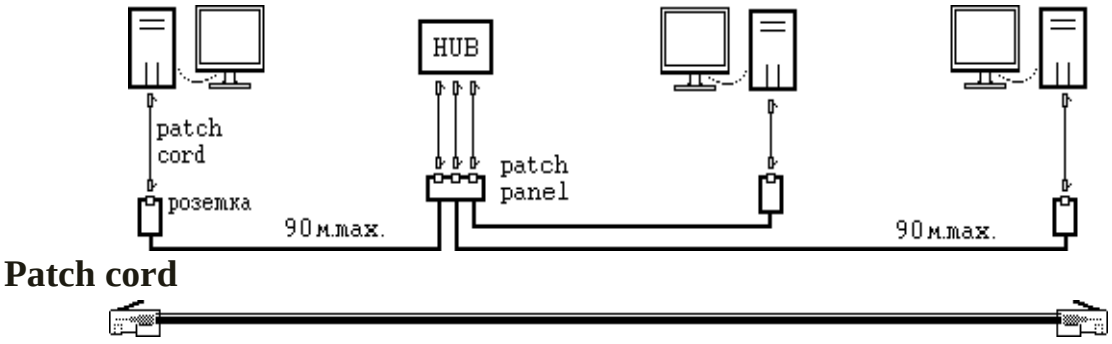


Рис. 2.8. Ограничения на длину кабелей

Patch cord – отрезок витой пары (не более 5 метров) с обжатыми на его концах коннекторами RJ-45, предназначенный для подключения компьютера к сетевой розетке. Обычно изготавливается из кабеля более гибкого и прочного, чем основной кабель (многожильный кабель), чтобы случайно не передавить и не переломить его. Коннектор RJ-45 монтируется на кабель в соответствии со схемами 568A или 568B, при этом в ведомственных подразделениях традиционно применяется схема 568B.

Канальные уровни протоколов Ethernet и IEEE 802.3 обеспечивают транспортировку данных по физическому каналу, непосредственно соединяющему два соединенных устройства. Например, как показано на рисунке 1.25, три устройства могут напрямую быть связаны друг с другом с помощью сети Ethernet. Рядом с компьютером с ОС Linux (слева) и компьютером с ОС Windows (в центре на рисунке) указаны их *адреса управления доступом к среде передачи данных* (MAC-адреса), используемые канальным уровнем. Маршрутизатор, расположенный справа, также использует MAC-адреса каждого из своих сетевых интерфейсов. Для обозначения интерфейса маршрутизатора, работающего по протоколу IEEE 802.3, используется аббревиатура, принятая в *Межсетевой операционной системе корпорации Cisco (Cisco Interwork Operating System, IOS),* – символ *E*, за которым указывается номер интерфейса. Например, E0 – это имя интерфейса IEEE 802.3 под номером 0 (рис. 2.9).

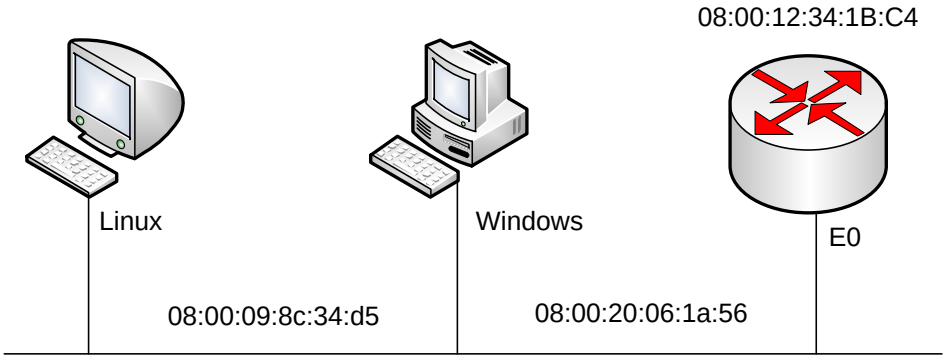


Рис. 2.9. В маршрутизаторах Cisco Ethernet/IEEE 802.3 – канал передачи использует интерфейс, название которого состоит из символа *E* и порядкового номера *0*

В сети Ethernet данные, посылаемые одним узлом, проходят через весь сегмент. По мере движения данные принимаются и анализируются каждым узлом. Когда сигнал достигает конца сегмента, он поглощается специальным оконечным элементом. Это необходимо для того, чтобы предотвратить движение сигнала в обратном направлении. В каждый отдельный момент времени в локальной сети возможна только одна передача. Например, в сети с линейной шинной топологией пакет данных передается от станции A к станции D (рис. 2.10). Этот пакет принимается всеми станциями. Станция D распознает свой адрес и обрабатывает кадр.

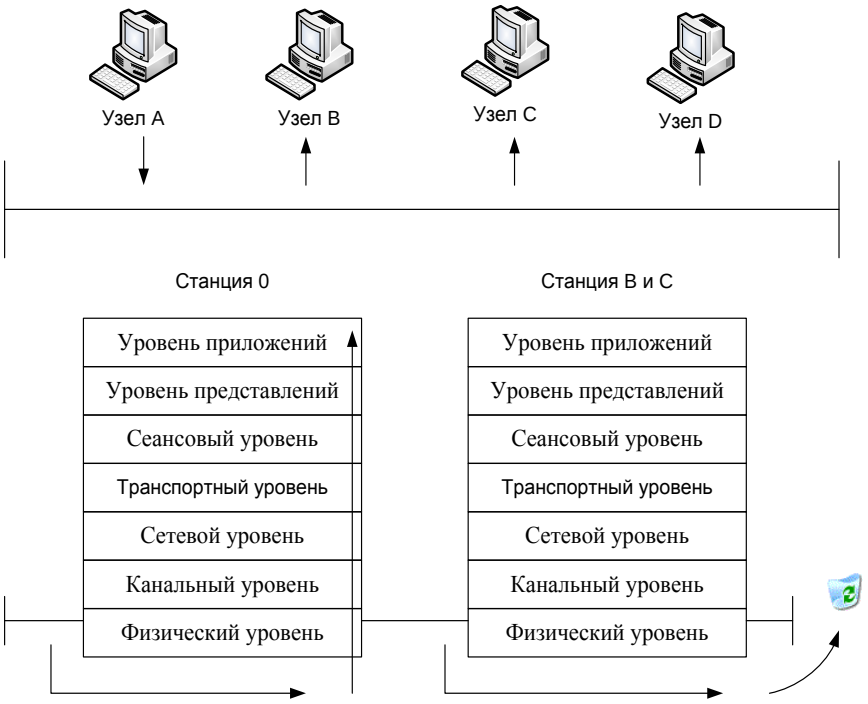


Рис. 2.10. Станция D распознаёт свой адрес и принимает кадр;
станции B и C не распознают свои MAC-адреса и игнорируют его

Станции B и C не распознают свои MAC-адреса и игнорируют кадр.

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

Технология Ethernet является *технологией коллективного использования среды передачи данных.* Это означает, что все устройства в сети должны следить за передачами в сети и конкурировать или договариваться о возможности, или праве, на передачу.

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

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

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

Перед отправкой данных узел «прослушивает» сеть, чтобы определить, можно ли осуществлять передачу, или сеть сейчас занята. Если в данный момент сеть никем не используется, узел осуществляет передачу. Если сеть занята, узел переходит в режим ожидания. Возникновение конфликтов возможно в том случае, если два узла, «прослушивая» сеть, обнаруживают, что она свободна, и одновременно начинают передачу. В этом случае возникает конфликт, данные повреждаются и узлам необходимо повторно передать данные позже. Алгоритмы задержки определяют, когда конфликтующие узлы могут осуществлять повторную передачу. В соответствии с тре-

бованиями CSMA/CD каждый узел, начав передачу, продолжает «прослушивать» сеть на предмет обнаружения конфликтов, узнавая таким образом о необходимости повторной передачи. Если последующие попытки также заканчиваются неудачно, узел повторяет их до 16 раз, после чего отказывается от передачи.

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

В современных ЛВС, составляющих сегменты в ОВД спецификации Ethernet и IEEE 802.3 не применяются. На смену им пришли новые технологии Fast Ethernet, Gigabit Ethernet, 10-Gigabit Ethernet и 100-Gigabit Ethernet.

По мере развития компьютерных технологий и появления новых более мощных компьютеров, скорость технологии Ethernet перестала быть достаточной для нормальной работы сетей, которые уже просто не справлялись с возросшими нагрузками на каналы связи. Поэтому в 1995 г. были утверждены новые стандарты – IEEE 802.3u и 802.12, позволяющие реализовывать взаимодействие компьютеров через сеть на скорости 100 Мбит/с.

Стандарт IEEE 802.3u основан на технологии Fast Ethernet, которую разработала группа производителей сетевого оборудования, состоящая из таких компаний, как 3Com и SynOptics. Этот стандарт стал дополнением к уже существовавшему стандарту IEEE 802.3.

Разработчики отказались от использования в качестве физической среды передачи данных коаксиального кабеля, полностью перейдя на витую пару и оптоволокно, которые позволяют поддерживать требуемые скорости соединений, и при этом являются более удобным и экономичным решением.

Как и стандарт IEEE 802.3, описывающий технологию Интернет, новый стандарт установил спецификации для различных сред передачи данных.

100Base-TX использует для передачи данных кабель на основе неэкранированной витой пары пятой категории или экранированной витой пары первой категории. Максимальная длина сегмента при этом составляет 100 м. Стандарт 100Base-T4, как и в технологии Ethernet, предполагает использование кабеля на основе неэкранированных витых пар третьей категории. Но для возможности увеличить скорость до 100 Мбит/с здесь используются все четыре пары вместо двух, как это было раньше. При этом одна витая пара используется для прослушивания несущей частоты и обнаружения коллизий, а оставшиеся три пары – для передачи данных. Скорость передачи данных каждой из пар составляет 33 Мбит/с, что суммарно и дает скорость в 100 Мбит/с.

100Base-FX имеет много общего со спецификацией 100Base-TX, по сути, это его реализация для многомодового оптоволоконного кабеля, который и используется в качестве физической среды передачи данных. Максимальная длина сегмента для Fast Ethernet, построенного на этой технологии, зависит от режима передачи. Одновременная передача данных в обоих направлениях называется полнодуплексной передачей, а соответственный режим передачи – полнодуплексным. В этом случае длина сегмента не должна превышать 2 км.

Режим, при котором обмен данными осуществляется путем чередования приема и передачи, называется полудуплексным. Длина отрезка кабеля, соединяющего узлы сети, при этом не должна быть больше 412 м.

После разработки стандартов, позволяющих передавать данные на скорости 100 Мбит/с, достаточно скоро снова назрела необходимость в переходе на новый уровень скоростей. Сложность возникла при строительстве крупных корпоративных сетей, где серверы, работающие при 100 Мбит/с, перегружали магистральные каналы связи. Поэтому следующим шагом в развитии высокоскоростных сетей стала технология Gigabit Ethernet, обеспечивающая возможность передачи данных на скорости 1000 Мбит/с.

Технологии Gigabit Ethernet соответствует стандарт 802.3z, который определяет для нее в качестве физической среды передачи данных одномодовый и многомодовый оптоволоконный кабель, а также экранированную витую пару с волновым сопротивлением 75 Ом. Чуть позже была разработана реализация Gigabit Ethernet для кабеля на основе витой пары категории 5 (стандарт IEEE 802.3ab). Также определены и соответствующие физическим средам спецификации.

1000Base-LX (L – от long wavelength – длинная волна) предусматривает использование как многомодового, так и одномодового оптоволокна и излучения с длиной волны в диапазоне 1270–1355 нм. Длинноволновой лазер дороже, чем коротковолновой, но допускает передачу на более длинные дистанции. Для полудуплексного режима передачи длина сегмента составляет 316 м, тогда как для полнодуплексного – 550 м для многомодового оптоволокна и 5 км для одномодового.

1000Base-SX (S – от short wavelength – короткая волна) предполагает передачу только по многомодовому оптоволокну и длину волны в диапазоне 770–860 нм. Длина сегмента в полудуплексном режиме передачи составляет 275 м для волокна диаметром 62,5 нм и 316 м для волокна 50 нм, в дуплексном режиме соответственно 275 и 550 м.

1000Base-T использует для передачи все четыре витые пары кабеля категории 5. Передача происходит параллельно по каждой паре со скоростью 250 Мбит/с. Показатели максимального числа подключаемых узлов, длины сегмента, диаметра сети остаются стандартными для кабеля на основе витой пары пятой категории.

1000Base-CX в качестве физической среды использует специальную экранированную витую пару с волновым сопротивлением 75 Ом для каждого проводника (Twinax). Передача осуществляется в полудуплексном режиме, причем данные посылаются по двум проводникам одновременно. Максимальная длина сегмента при этом может составлять всего 25 м.

Следующим этапом развития технологий высокоскоростной передачи данных стал стандарт IEEE 802.3ae – 10 Gigabit Ethernet (10 GbE), одобренный в июне 2002 г. С его появлением область использования Ethernet расширилась до масштабов городских (MAN) и глобальных (WAN) сетей.

В стандарте описано несколько спецификаций, определяющих использование в качестве среды передачи данных одно– и многомодовые оптоволокна, методы кодирования, применяемые длины волн и т.д.

2.4. Стандарты глобальных сетей

Глобальные сети работают за пределами географических возможностей ЛВС, используя последовательные соединения различных типов для обеспечения связи в пределах значительных географических областей.

По определению, глобальные сети объединяют устройства, расположенные на большом удалении друг от друга. К устройствам глобальных сетей относятся следующие (рис. 2.11).

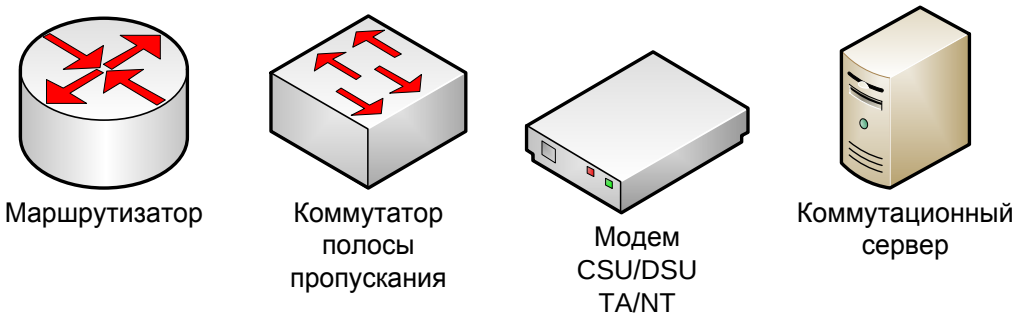


Рис. 2.11. Основными устройствами WAN являются маршрутизаторы, широкополосные коммутаторы, модемы и коммуникационные серверы

1. *Маршрутизаторы,* обеспечивающие большое количество сервисов, включая организацию межсетевого взаимодействия и интерфейсные порты WAN.

2. *Коммутаторы,* которые подключают полосу для передачи голосовых сообщений, данных и видео.

3. *Модемы,* которые служат интерфейсом для голосовых сервисов.

4. *Устройства управления каналом/цифровые сервисные устройства (channel service units/digital service units, CSU/DSUs),* которые являются интерфейсом для сервисов *T1/E1*.

5. *Терминальные адаптеры и оконечные сетевые устройства (terminal adapter / network termination, TA/NT),* которые служат интерфейсом

для служб *цифровой сети с интеграцией услуг (Integrated Services Digital Network, ISDN).*

6. *Коммуникационные серверы (communication servers),* которые концентрируют входящие и исходящие пользовательские соединения по коммутируемым каналам связи.

7. *Медиаконвертеры* – устройства, сопрягающие разнородные физические среды передачи данных двух и более сетей.

Определением, разработкой и внедрением стандартов в области глобальных сетей занимаются следующие организации: международный телекоммуникационный союз (International Telecommunication Union, ITU), ранее – Международный консультативный комитет по телеграфии и телефонии (Consultative Committee for International Telegraphy and Telephony, CCITT); международная организация по стандартизации (International Organization for Standardization, ISO); рабочая группа по инженерным проблемам Internet (Internet Engineering Task Force, IETF); ассоциация электронной промышленности (Electronic Industries Association, EIA). Стандарты глобальных сетей обычно описывают требования канального и физического уровней.

Протоколы физического уровня WAN описывают, как обеспечить электрическое, механическое, операционное и функциональное подключение к WAN-сервисам. Как правило, эти сервисы предоставляются *провайдерами услуг глобальной сети (WAN service providers)*, например региональными и национальными операторами связи, почтовыми, телефонными и телеграфными агентствами. Протоколы канального уровня WAN описывают, каким образом кадры переносятся между системами по одному каналу передачи данных. Они включают протоколы, обеспечивающие работу через службы двухточечной и многоточечной связи, а также службу множественного доступа по коммутируемым каналам типа Frame Relay.

Физический уровень WAN описывает интерфейс между терминальным оборудованием (Data Terminal Equipment, DTE) и оборудованием передачи данных (Data Communications Equipment, DCE). К терминальному оборудованию относятся устройства, которые входят в интерфейс «пользователь-сеть» со стороны пользователя и играют роль отправителя данных, получателя данных или вместе. Устройства DCE обеспечивают физическое подключение к сети, пропуск трафика и задание тактовых сигналов для синхронизации обмена данными между устройствами DCE и DTE (рис. 2.12). Обычно устройство DCE расположено у сервис-провайдера, а DTE – подключаемое устройство. В этой модели сервисы предоставляются DTE-устройствам с помощью модемов или устройств CSU/DSU.

Интерфейс «пользователь-сеть» определяется несколькими стандартами физического уровня.

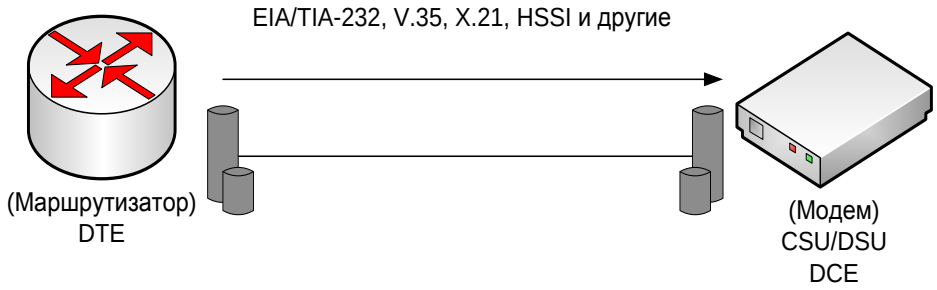


Рис. 2.12. Сервисы доступны DTE-устройствам через модемы или устройства CSU/DSU

• *EIA/TIA-232* – общий стандарт интерфейса физического уровня, разработанный EIA и TIA, который поддерживает скорость передачи данных в несбалансированном канале до 64 Кбит/с. Этот стандарт очень похож на спецификацию V.24 и ранее был известен как RS-232.

• *EIA/TIA-449* – популярный интерфейс физического уровня, разработанный EIA и TIA. По существу, это более быстрая (до 2 Мбит/с) версия стандарта EIA/TIA-232, позволяющая работать с кабелями большей длины.

• *V.24* – стандарт для интерфейса физического уровня между терминальным оборудование (DTE) и оборудованием передачи данных (OCE). Он был разработан ITU-T. По сути, V.24 – то же самое, что и стандарт EIA/TIA-232.

• *V.35* – разработанный ITU-T стандарт, который описывает синхронный протокол физического уровня, используемый для связи между устройствами доступа к сети и пакетной сетью. Рекомендован для скоростей передачи данных вплоть до 48 Кбит/с.

• *X.21* – разработанный ITU-T стандарт, который используется для последовательной связи по синхронным цифровым линиям.

• *G.703* – разработанные ITU-T электрические и механические спецификации для связи между оборудованием телефонных компаний и терминальным оборудованием (DTE) с использованием байонетных BNC-разъемов и на скоростях, соответствующих каналу типа E1.

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

Существует несколько методов канальной инкапсуляции, связанных с линиями синхронной последовательной передачи данных (рис. 2.13).

• HDLC (High-level Data Link Control – высокоуровневый протокол управления каналом).

• Frame Relay.

• PPP (Point-to-Point Protocol – протокол связи «точка-точка»).

• ISDN

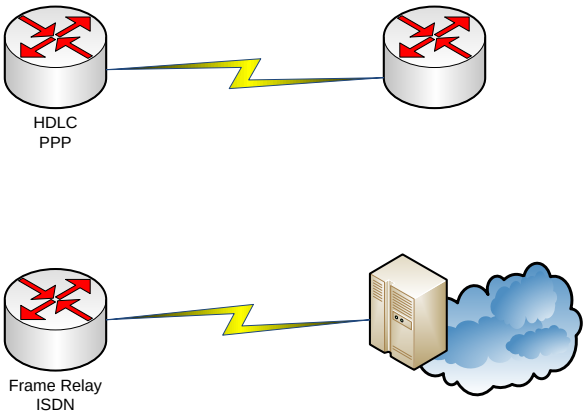


Рис. 2.13. Канальная инкапсуляция для линий синхронной последовательной передачи данных, включая протоколы HDLC, Frame Relay, PPP и ISDN

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

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

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

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

3. СЕТЕВАЯ АДРЕСАЦИЯ

3.1. Адресное пространство с плоской и иерархической структурой

При объединении в сеть нескольких узлов возникает проблема идентификации конкретного узла, которому предназначены пересылаемые данные. Другими словами, возникает проблема адресации узлов компьютерной сети. На практике адресация производится не для самих узлов сети, а для их сетевых интерфейсов, т.е. наборов средств и правил, позволяющих осуществлять обмен информацией. Это объясняется тем, что один узел сети может иметь несколько сетевых интерфейсов, например, в маршрутизаторах.

Существует множество систем адресации и, соответственно, множество форматов представления адресов. Например, адрес может иметь вид числовой или символьной последовательности. Множество всех допустимых адресов в какой-либо системе адресации называется *адресным пространством*. Структура адресного пространства может быть линейной (плоской) или иерархической.

Примером плоского адреса является MAC-адрес. MAC-адрес или физический адрес, – уникальный идентификатор, однозначно определяющий каждый сетевой интерфейс.

Каждый компьютер, независимо от того, подключен он к сети или нет, имеет уникальный физический адрес. Не существует двух одинаковых физических адресов. Физический адрес (или MAC-адрес от англ. Media Access Control – управление доступом к среде, также Hardware Address) запрограммирован в микросхеме *сетевого адаптера*.

Таким образом, именно плата сетевого адаптера подключает устройство к среде передачи данных. Каждый интерфейс плат сетевых устройств, которые работают на физическом канальном уровнях эталонной модели OSI, имеют свой уникальный MAC-адрес.

В сети, когда одно устройство готовит пересылку данных другому устройству, оно может установить канал связи с этим другим устройством, воспользовавшись его MAC-адресом. Отправляемые источником данные содержат MAC-адрес пункта назначения. По мере продвижения пакета в среде передачи данных сетевые адаптеры каждого из устройств в сети сравнивают MAC-адреса пункта назначения, имеющиеся в пакете данных, со своим собственным физическим адресом. Если адреса не совпадают, сетевой адаптер игнорирует этот пакет и данные продолжают движение к следующему устройству. Если же адреса совпадают, то сетевой адаптер делает копию пакета данных и размещает ее на канальном уровне компьютера. После этого исходный пакет данных продолжает движение по сети, и каждый следующий сетевой адаптер проводит аналогичную процедуру сравнения.

Примером иерархических адресов служат сетевые IP-адреса, которые используют при своей работе протокол IP стека TCP/IP. Поскольку протокол IP относится к сетевому уровню, то и IP-адреса часто называют сетевыми адресами.

В IP-сетях каждый узел имеет IP-адрес, который представляет собой уникальное 32-битовое двоичное число. IP-адресация существует на уровне 3 (сетевом) эталонной модели OSI и в отличие от MAC-адресов, которые существуют в плоском адресном пространстве, IP-адреса имеют иерархическую структуру.

На рисунке 3.1 каждая сеть имеет свой адрес, который относится ко всем хост-машинам, принадлежащим данной сети, а внутри сети каждая хост-машина имеет свой уникальный адрес.

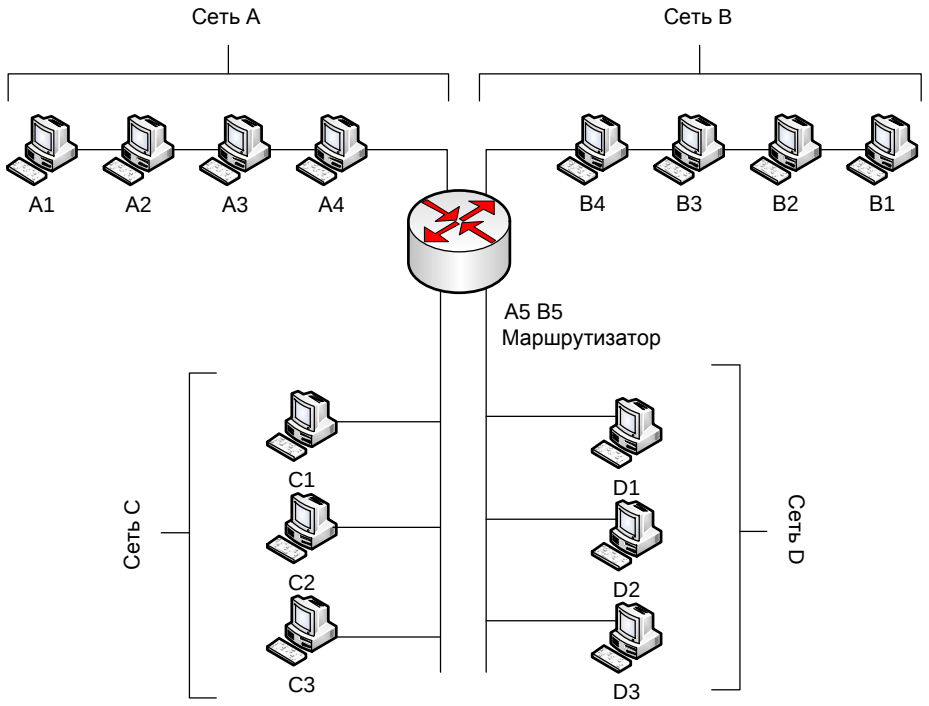


Рис. 3.1. Уникальная адресация позволяет конечным станциям связываться между собой

При адресации, имеющей иерархическую структуру, адресное пространство состоит из вложенных друг в друга подгрупп адресов, последовательно уточняющих конечного адресата. IP-адрес устройства состоит из адреса сети, к которой принадлежит устройство, и адреса устройства внутри этой сети. Следовательно, если устройство переносится из одной сети в другую, его IP-адрес должен быть изменен так, чтобы отразить это перемещение (рис. 3.2 – рис. 3.5). Кроме числовых схем адресации, также применяются схемы адресации, использующие символьное представление адресов. Символьные адреса гораздо проще запоминать, этому способствует еще и тот факт, что обычно они несут некую смысловую нагрузку. Поэтому такие адреса удобны там, где необходимо обеспечить интерфейс пользователя с сетевой программой.

Однако символьные адреса имеют переменный формат достаточно большой максимально возможной длины, поэтому хранение и передача по сети таких адресов вызывают ряд сложностей и являются не очень экономичными.

В сети ОВД используется IP-адресация, но поскольку пользователям приложений удобней работать с символьными адресами, то на прикладных уровнях *должна существовать символьная система адресации*, каждый адрес которой является мнемоническим обозначением соответствующего IP-адреса.

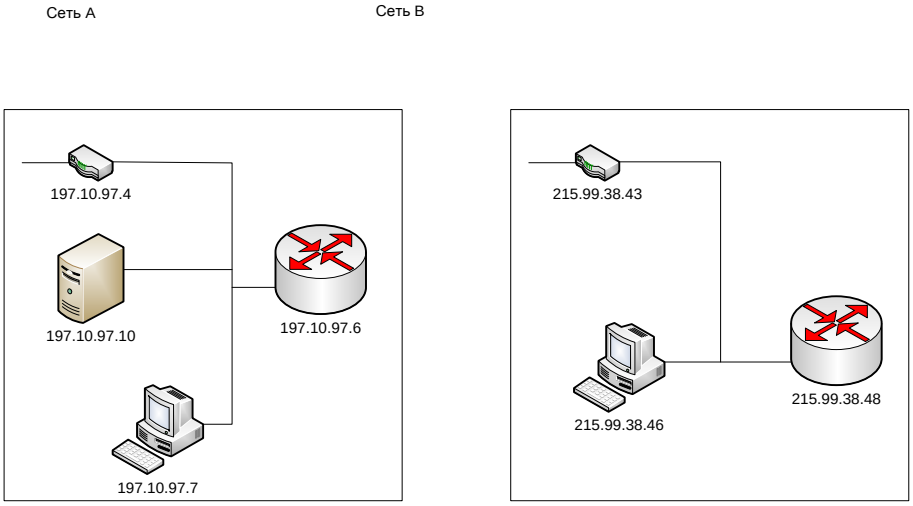


Рис. 3.2. В сети А находится сервер с адресом 197.10.97.10, который нужно перенести в сеть В

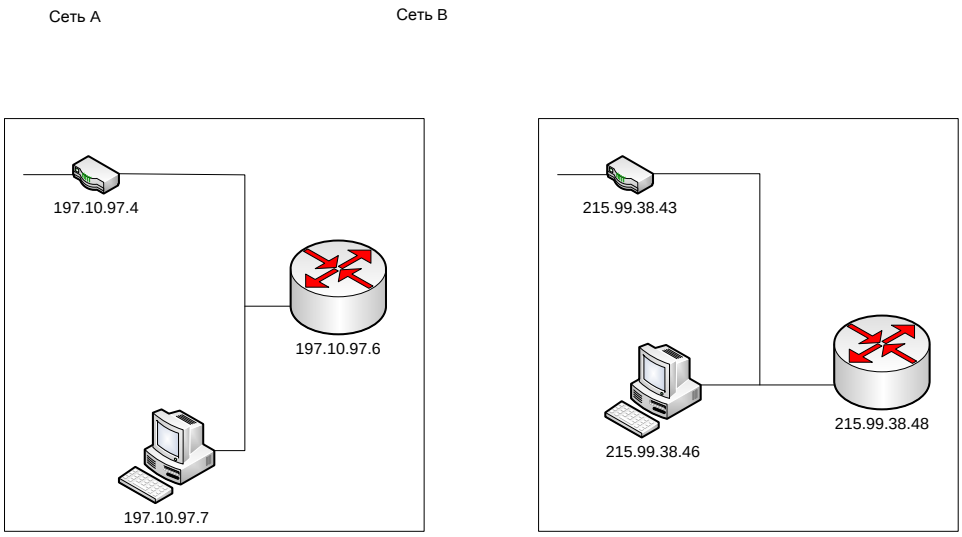


Рис. 3.3. Файл-сервер с адресом 197.10.97.10 удален из сети А

IP-адреса имеют сходство с почтовыми адресами, которые описывают местонахождение адресата, включая страну, город, улицу, номер дома и имя.

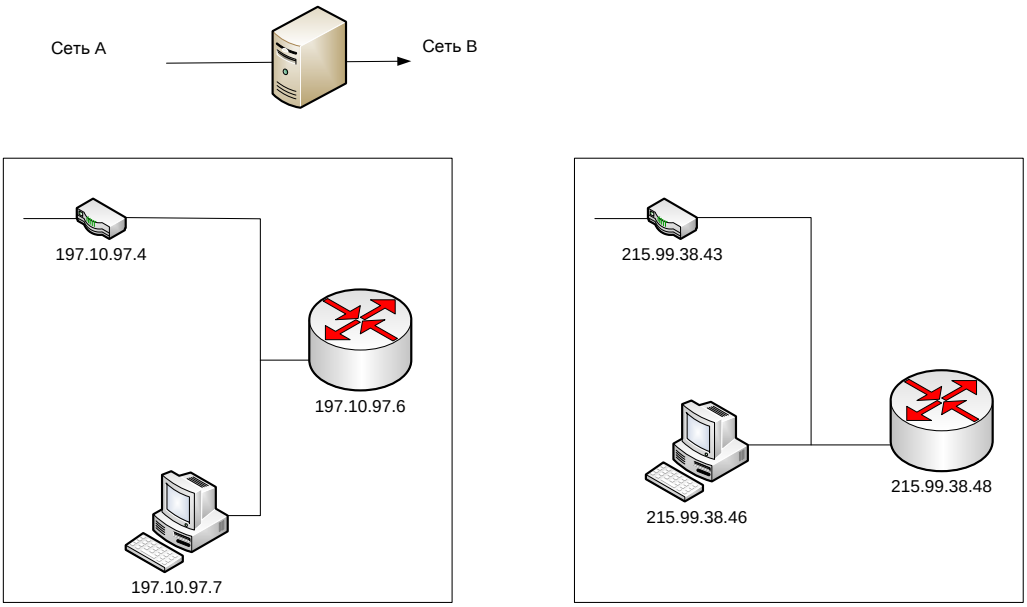


Рис. 3.4. Сервер доставлен на другую территорию

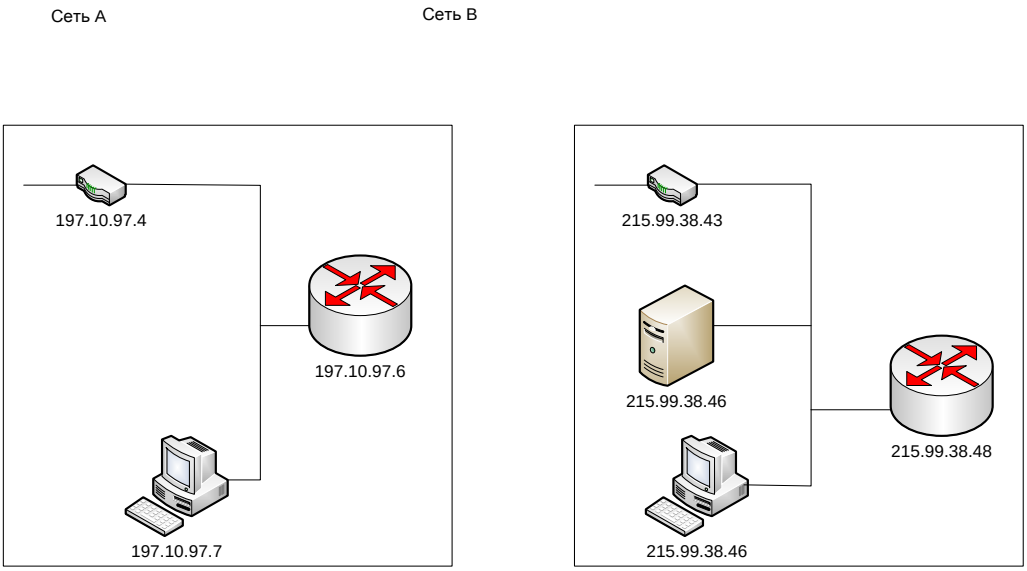


Рис. 3.5. Файл-сервер подключен к сети В, и ему присвоен новый адрес 215.99.38.49

Раньше символьная адресация обеспечивалась средствами операционных систем, хранившими таблицы соответствия физического адреса узла сети и его символьного адреса. Однако такие системы изначально разрабатывались для работы в небольших локальных сетях. При этом имена узлов имели линейную структуру, т.е. не разделялись на несколько частей. Чтобы определить физический адрес узла, соответствующий некоторому символьному имени, проводился опрос всех узлов локальной сети посредством механизма широковещательных запросов.

Но в больших сетях или в сетях, объединяющих несколько подсетей, более эффективно применение иерархической системы адресации, и, соответственно, адресов, состоящих из нескольких «вложенных» друг в друга частей.

Примером такой системы адресации может служить доменная система имен (Domain Name System), применяемая в Интернете, имеющая иерархическую древовидную структуру и допускающая большую степень вложенности, т.е. большое количество иерархических подуровней.

Доменное имя может состоять из нескольких частей, отделенных друг от друга точками, например mail.vimvd.ru. Каждая из таких частей называется *доменом*. Под доменом можно подразумевать некую совокупность компьютеров, имеющих какие-либо схожие свойства.

Доменное имя записывается так, что слева оказывается имя узла, входящего в домен, имеющий самый низкий уровень в иерархии, а справа — домен, имеющий самый высокий иерархический уровень. Поэтому крайний справа домен называется *доменом верхнего* или *первого уровня*. Следующий слева домен, отделенный точкой, является дочерним доменом по отношению к домену первого уровня, т.е. входит в него как его составная часть. Этот домен называется *доменом второго уровня*. Домены, которые являются дочерними для домена второго уровня, называются *доменами третьего уровня* и т.д.

В адресе mail.vimvd.ru доменом первого уровня является домен «ru», доменом второго уровня — «vimvd», слово «mail» является именем хоста.

Термин *«хост»* (от англ. host) употребляется в качестве синонима термина «узел сети», когда говорят о сетях, объединенных на основе использования стека TCP/IP. Названия доменов первого уровня назначаются централизованно, в соответствии с международным стандартом. *Имя домена первого уровня в ОВД* может обозначать псевдоним Министерства, например .mvd.

Доменом второго уровня в ОВД может являться псевдоним субъекта МВД РФ, которому принадлежит сеть или хост-компьютер, для адресации которых используется этот домен, например, guvo.mvd (Главное управление МВД РФ по Воронежской области).

Домены третьего и последующих уровней могут быть частью доменов второго уровня, на практике обычно представляют некие подсети либо дочерние хосты, например, gibdd.guvo.mvd (Управление государственной инспекции безопасности дорожного движения Главного управления МВД РФ по Воронежской области). Установление соответствия доменных имен сетевым адресам осуществляется централизованно с помощью сервиса DNS.

Сервис DNS – система обеспечения преобразования символических имен и псевдонимов локальных сетей и узлов в сети Интернет в IP-адреса и обратно.

Принцип работы сервиса DNS основан на использовании DNS-серверов. Каждый домен должен иметь свой DNS-сервер, который хранит таблицу соответствий доменных имен и IP-адресов данного домена, а также доменов, являющихся для него дочерними. В таблице также присутствует запись, относящаяся к родительскому домену. Таким образом, любой узел может получить сведения об искомом IP-адресе любого узла сети. Для этого узел последовательно обращается ко всем DNS-серверам, находящимся выше по иерархии, пока не дойдет до сервера, расположенного в домене, общем для данного узла, осуществляющего поиск, и искомого узла. Далее происходит последовательное обращение к серверам, находящимся ниже по доменной иерархии, пока домен, содержащий искомый узел, не будет найден.

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

Двоичная система исчисления базируется на возведении в степень числа 2: 2^1, 2^2, 2^3, 2^4 и т.д. *IP-адрес* представляет собой 32-разрядное двоичное число, записанное в виде четырех октетов, т.е. четырех групп, каждая из которых состоит из восьми двоичных знаков (нулей и единиц). Таким образом, в IP-адресе, записанном как

11000000.00000101.00100010.00001011,

первый октет представляет собой двоичное число 11000000,
второй октет – двоичное число 00000101,
третий октет – двоичное число 00100010,
четвертый октет – двоичное число 00001011 (рис. 3.6).

Октет (8 бит)	Октет (8 бит)	Октет (8 бит)	Октет (8 бит)
$2^7 2^6 2^5 2^4 2^3 2^2 2^1 2^0$	$2^7 2^6 2^5 2^4 2^3 2^2 2^1 2^0$	$2^7 2^6 2^5 2^4 2^3 2^2 2^1 2^0$	$2^7 2^6 2^5 2^4 2^3 2^2 2^1 2^0$
11000000	00000101	00100010	00001011
	Десятичный эквивалент		
192	5	34	11

Рис. 3.6. IP-адрес выражается в виде двоичных чисел, состоящих из нулей и единиц

Каждая позиция в октете представляет различные степени от 2. Величина показателя степени 2 назначается каждому разряду двоичного числа, начиная с крайнего правого. Чтобы определить, чему равно двоичное число, необходимо сложить значения всех разрядов в октете. Следовательно, для двоичного числа первого октета, показанного на рис. 3.6 (11000000), справедливо следующее:

0 умножается на 2^0 (1), что равно 0;
0 умножается на 2^1 (2), что равно 0;
0 умножается на 2^2 (4), что равно 0;
0 умножается на 2^3 (8), что равно 0;
0 умножается на 2^4 (16), что равно 0;
0 умножается на 2^5 (32), что равно 0;
1 умножается на 2^6 (64), что равно 64;
1 умножается на 2^7 (128), что равно 128.

Таким образом, двоичное число 11000000 равно десятичному числу 192.

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

В представлении в десятичной форме с разделением точками IP-адреса, или точечно-десятичные адреса, записываются следующим образом (рис. 3.7): каждое десятичное число представляет один байт из четырех, составляющих весь IP-адрес.

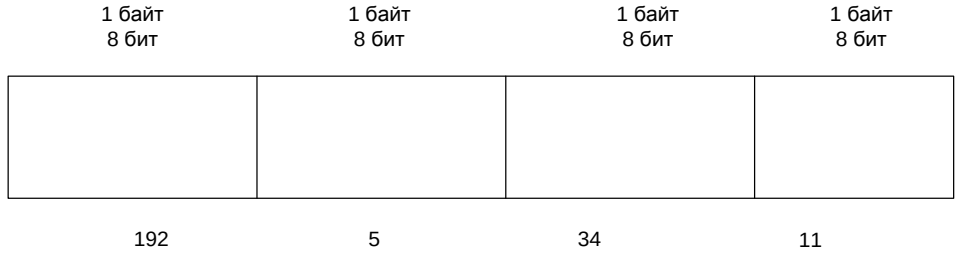


Рис. 3.7. 32-битовый IP-адрес состоит из 4 однобайтовых октетов

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

11000000
00000101
00100010
00001011

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

3.2. Структура IP-адресов и классы сетей

Каждая сеть, входящая в Интернет, имеет уникальный сетевой адрес, данные могут найти требуемый адресат. Для того чтобы каждый сетевой адрес был уникальным и отличался от любого другого номера, выделяются блоки IP-адресов в зависимости от размера их сетей. Каждый IP-адрес состоит из двух частей: номера сети и номера хоста (рис. 3.8). Сетевой номер идентифицирует сеть, к которой подключено устройство. Номер хоста идентифицирует устройство в этой сети.

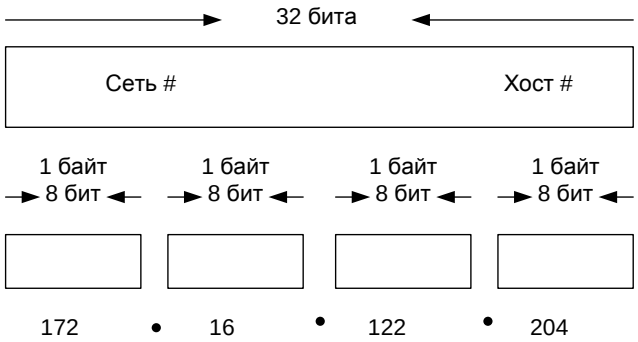


Рис. 3.8. IP-адрес состоит из номера сети и номера хоста

Используются три основных класса IP-адресов.

Класс A составляют IP-адреса, зарезервированные для правительственных учреждений, класс B – IP-адреса для компаний среднего уровня и класс C – для всех остальных организаций. Если записать IP-адреса класса A в двоичном формате, то первый бит всегда будет равен 0 (рис. 3.9). Если записать IP-адреса класса B в двоичном формате, то первые два бита всегда будут 0 и 1. Если записать IP-адреса класса C в двоичном формате, то первые три бита всегда будут 1, 1 и 0.

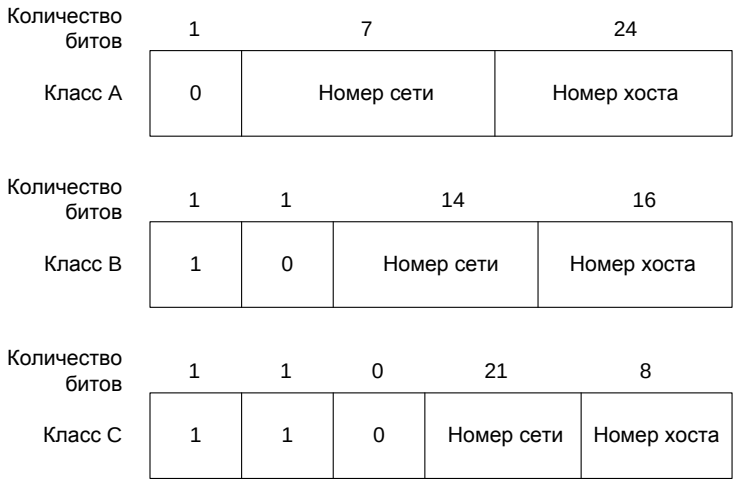


Рис. 3.9. Общий вид IP-адресов классов A, B и C

Всего существует пять классов сетевых адресов (рис. 3.10), но только три из них – классы A, B и C – используются в действующих сетях, а два других класса сетевых адресов зарезервированы.

Рис. 3.10. Типы классов сетевых адресов

Максимально возможное значение каждого октета IP-адреса равно 255 (рис. 3.11). Следовательно, это десятичное число могло бы быть присвоено первому октету сети любого класса. На практике применяются только числа до 223. Возникает вопрос: почему при максимально допустимом значении 255 для каждого октета используются только числа до 223? Это связано с тем, что часть номеров резервируется для экспериментальных целей и потребностей групповой адресации, и эти номера не могут быть присвоены сетям. Поэтому в первом октете IP-адресов значения с 224 по 255 для решения сетевых задач не используются.

128	64	32	16	8	4	2	1
2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
1	1	1	1	1	1	1	1

128 + 64 + 32 + 16 + 8 + 4 + 2 + 1 =255

Рис. 3.11. Максимально возможное значение в каждом октете IP-адреса – 255

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

В соответствии с соглашением в схемах IP-адресации любой IP-адрес, который заканчивается всеми двоичными нулями, резервируется для адреса этой сети. Примером адреса сети класса A может быть IP-адрес 95.0.0.0. Когда маршрутизаторы направляют данные через Интернет, они руководствуются при этом IP-адресами сетей.

Примером адреса сети класса B может быть IP-адрес 168.175.0.0. Следует заметить, что десятичные числа занимают первые два октета адреса сети класса B. Это объясняется тем, что оба октета обозначают номер сети. Только два последних октета содержат нули. Это связано с тем, что числа в этих октетах предназначены для обозначения номеров хостов, подключаемых к сети. Следовательно, для того чтобы обратиться ко всем устройствам в этой сети, т.е. к самой сети, сетевой адрес должен иметь нули в двух последних октетах. Поскольку адрес 168.175.0.0 зарезервирован для адреса сети (рис. 3.12), он никогда не будет использоваться в качестве IP-адреса какого-либо устройства, подключенного к этой сети.

Процесс, в ходе которого источник отправляет данные всем устройствам в сети, называется *широковещанием*. Для того чтобы все устройства в сети обратили внимание на широковещание, должен использоваться такой IP-адрес, который смогли бы распознать и признать своим все устройства в сети. Следовательно, для сети 168.175.0.0, показанной на рис. 3.12, адресом широковещания может быть адрес 168.175.255.255.

Когда кадр (который является разновидностью данных) достигает маршрутизатора, последний выполняет несколько функций. Во-первых, маршрутизатор отделяет содержащийся в кадре канальный заголовок. В канальном заголовке находятся MAC-адреса источника данных и получателя. После этого маршрутизатор проверяет заголовок сетевого уровня, в котором содержится IP-адрес сети назначения. Далее маршрутизатор сверяется со своей таблицей, чтобы определить, через какой из своих портов нужно отправить данные, чтобы они достигли сети назначения. При транспортировке данных через Интернет одна сеть видит другую как отдельную сеть и не имеет при этом подробной информации о ее внутренней структуре. Это помогает поддерживать размеры таблиц маршрутизации небольшими.

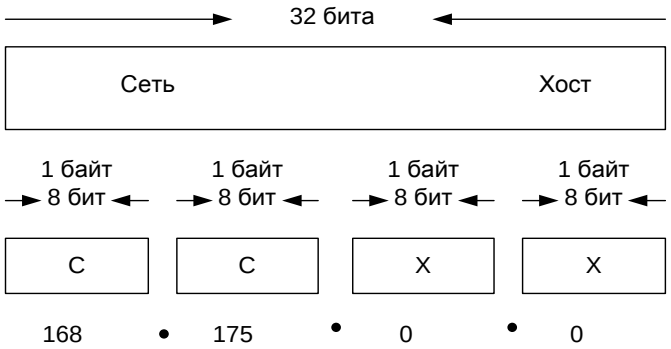


Рис. 3.12. Зарезервированный сетевой адрес 168.175.0.0 никогда не используется в качестве IP-адреса какого-либо устройства, подключенного к этой сети

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

3.3. Адресация, маскирование и планирование подсетей

Как и номера хост-машин в сетях класса A, класса B и класса C адреса подсетей задаются локально. Обычно это выполняет сетевой администратор. Так же, как и другие IP-адреса, каждый адрес подсети является уникальным. Использование подсетей никак не отражается на том, как внешний мир видит эту сеть, но в пределах организации подсети рассматриваются как дополнительные структуры. Для примера, сеть 172.16.0.0 разделена на 4 подсети: 172.16.1.0, 172.16.2.0, 172.16.3.0 и 172.16.4.0 (рис. 3.13).

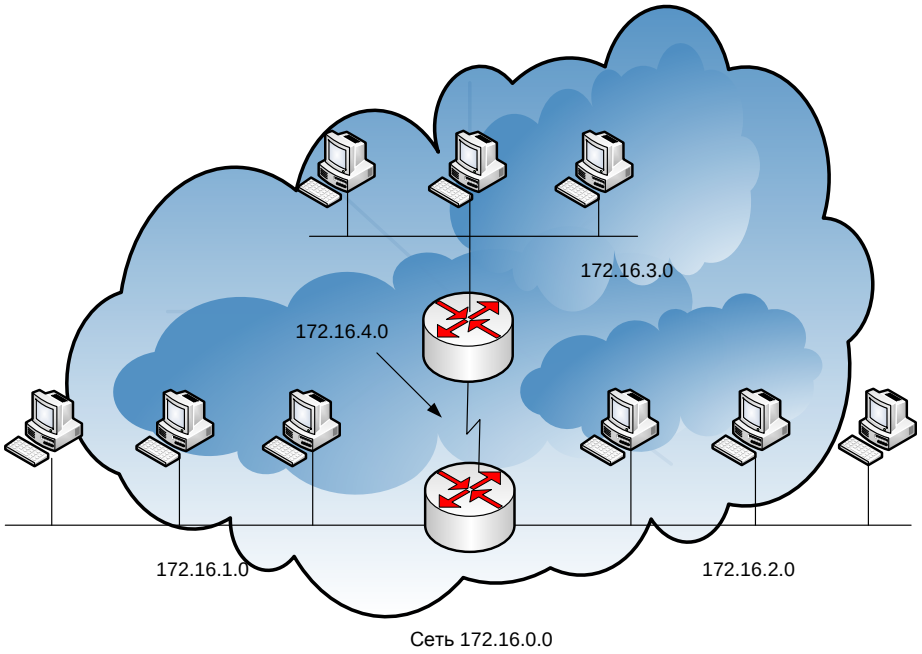


Рис. 3.13. Сеть 172.16.0.0 состоит из четырёх подсетей

Маршрутизатор определяет сеть назначения, используя адрес подсети, тем самым ограничивая объем трафика в других сегментах сети. С точки зрения адресации, подсети являются расширением сетевого номера (рис. 3.14). Сетевые администраторы задают размеры подсетей, исходя из потребностей организации и возможности роста. Адрес подсети включает номера сети, подсети и хост-машины внутри подсети. Благодаря этим трем уровням адресации подсети обеспечивают сетевым администраторам повышенную гибкость настройки.

Чтобы создать адрес подсети, сетевой администратор «заимствует» биты из поля хост-машин и переопределяет их в качестве поля подсетей (рис. 3.15). Количество «заимствованных» битов можно увеличивать до тех пор, пока не останется 2 бита. Поскольку в поле хостов сетей класса B имеются только 2 октета, для создания подсетей можно заимствовать до 14 бит. Сети класса C имеют только один октет в поле хостов. Следовательно, в сетях класса C для создания подсетей можно заимствовать до 6 бит.

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

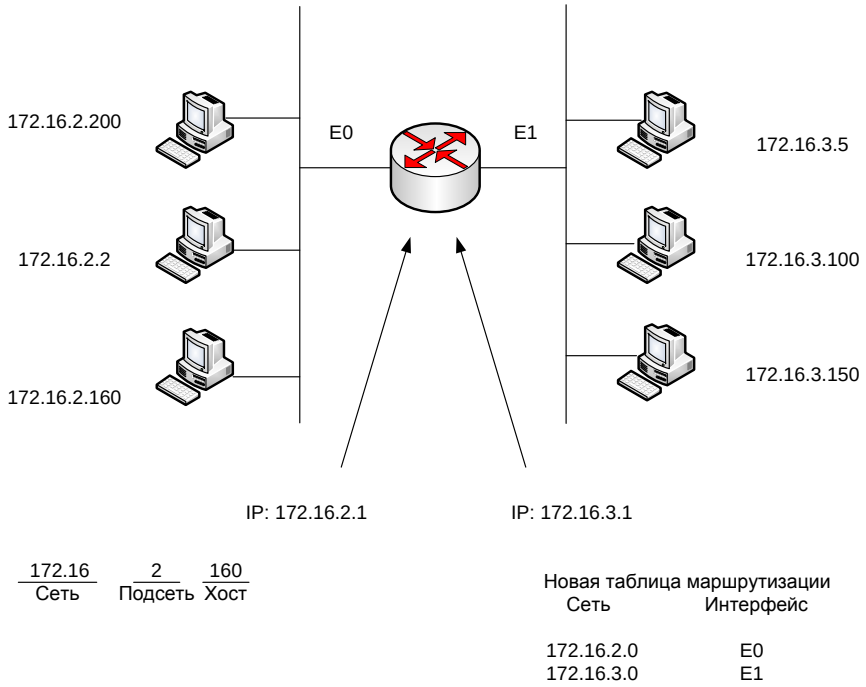


Рис. 3.14. Адресация подсетей расширяет номер путём создания подсетей

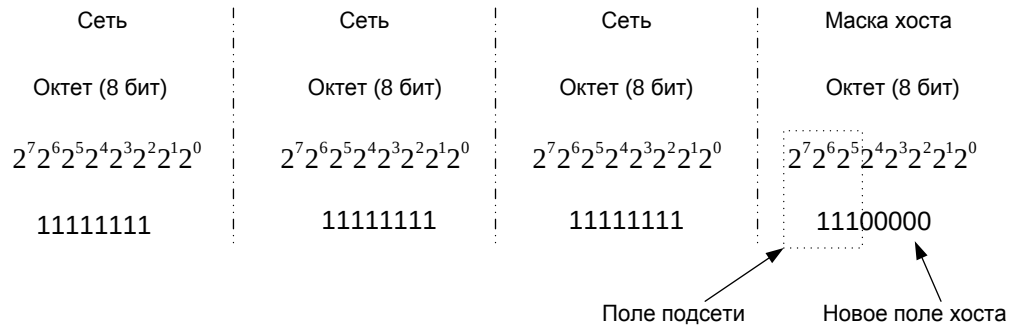


Рис. 3.15. Биты заимствуются из поля хост-машины
и переопределяются в качестве поля подсети

Чтобы понять смысл вышесказанного, рассмотрим сеть класса C. Все 8 бит в последнем октете используются для поля хостов. Следовательно, возможное количество адресов равно 2^8, или 256. Представим, что эту сеть разделили на подсети. Если из поля хостов заимствовать 1 бит, количество бит, которое можно использовать для адресации хостов, уменьшится до 7. Если записать все возможные комбинации нулей и единиц, можно убедиться, что число хостов, которые можно адресовать, стало равно 2^7, или 128. Если в сети класса C из поля хостов заимствовать 2 бита, то количество

бит, которое можно использовать для адресации хостов, уменьшится до 6. Общее число хостов, которое можно адресовать, станет равным 2^6, или 64.

IP-адреса, которые заканчиваются всеми двоичными единицами, зарезервированы для широковещания. Это утверждение справедливо и для подсетей. Рассмотрим сеть класса С с номером 197.15.22.0, которая разделена на восемь подсетей (табл. 3.1).

Таблица 3.1.

Последний октет сети класса С, разделенной на восемь подсетей

Подсеть	**Двоичные числа в поле подсети**	**Диапазон двоичных чисел в поле хостов**	**Диапазон десятичных чисел в поле хостов**
Первая	000	00000–11111	.0–.31
Вторая	001	00000–11111	.32–.63
Третья	010	00000–11111	.64–.95
Четвертая	011	00000–11111	.96–.127
Пятая	100	00000–11111	.128–.159
Шестая	100	00000–11111	.160–.191
Седьмая	101	00000–11111	.192–.223
Восьмая	110	00000–11111	.224–.255

Обратим внимание на IP-адрес 192.15.22.31. На первый взгляд, он ничем не похож ни на зарезервированный адрес сети, ни на адрес для широковещания. Однако, поскольку сеть разделена на восемь подсетей, первые 3 бита заимствуются для задания номера подсети. Это означает, что только последние 5 бит могут использоваться для поля хостов. Обратим внимание, что все 5 бит записаны в виде двоичных единиц. Следовательно, этот IP-адрес является зарезервированным адресом широковещания для первой подсети сети 197.15.22.0. IP-адреса, которые заканчиваются всеми двоичными нулями, зарезервированы для номера сети. Это утверждение справедливо и для подсетей. Чтобы убедиться в этом, можно еще раз обратиться к сети класса С с номером 197.15.22.0, разделенной на 8 подсетей (табл. 3.1).

Подсети скрыты от внешнего мира с помощью масок, называемых *масками подсети,* функцией которых является сообщить устройствам, в какой части адреса содержится номер сети, включая номер подсети, а в какой – номер хост-машины. Маски подсетей используют тот же формат, что и IP-адресация. Другими словами, маска имеет длину 32 бита и разделена на 4 октета. Маски подсетей имеют все единицы в части, соответствующей сети и подсети, и все нули в части, соответствующей хост-машине. По умолчанию, если нет заимствованных битов, маска подсети сети класса В будет иметь вид 255.255.0.0. Если же заимствовано 8 бит, маской подсети той же сети класса В будет 255.255.255.0 (рис. 3.16 и рис. 3.17). Маски подсети также используют 32-битовые IP-адреса, которые содержат все двоичные единицы в сетевой и подсетевой части адреса и все двоичные нули в хостовой части адреса.

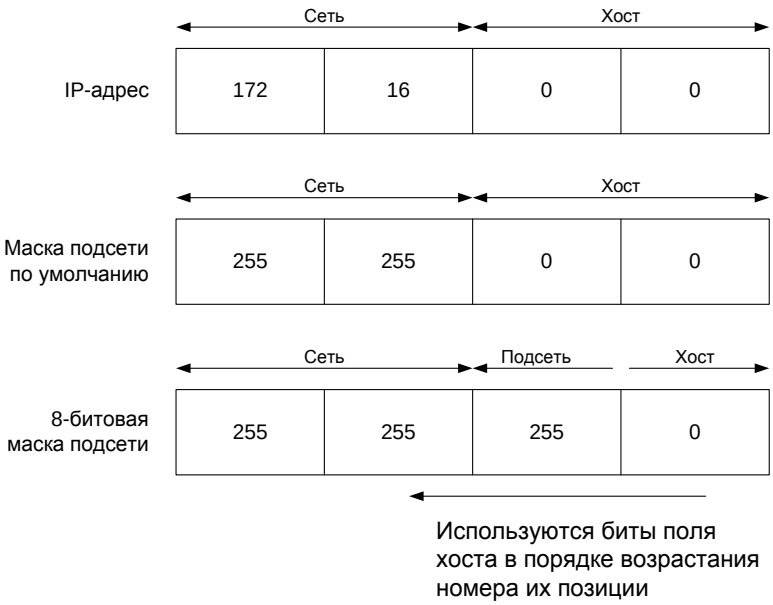


Рис. 3.16. Биты для создания подсети заимствуются из поля хост-машин, начиная со старших позиций

```
  128   64   32   16    8    4    2    1

128 64  32  16  8   4   2   1
-----------------------------

1   0   0   0   0   0   0   0   =128
1   1   0   0   0   0   0   0   =192
1   1   1   0   0   0   0   0   =224
1   1   1   1   0   0   0   0   =240
1   1   1   1   1   0   0   0   =248
1   1   1   1   1   1   0   0   =252
1   1   1   1   1   1   1   0   =254
1   1   1   1   1   1   1   1   =255
```

Рис. 3.17. Десятичные эквиваленты двоичных чисел, используемых в IP-адресах

Теперь рассмотрим сеть класса B, где для создания подсети вместо 8 бит в третьем октете заимствуются только 7. В двоичном представлении маска подсети в этом случае будет иметь вид 11111111.11111111.11111110.00000000. Следовательно, адрес 255.255.255.0 не может больше использоваться в качестве маски подсети.

В Интернете одна сеть «видит» другую как отдельную сеть и не имеет подробных сведений о ее внутренней структуре. Следовательно, также нет информации о том, какие подсети содержатся в этой сети.

Например, организация X имеет сеть класса B. Номер этой сети: 131.108.0.0. Внутри сеть компании X разделена на подсети. Однако внешние сети видят ее как одну единственную сеть. Предположим, что устройство из

другой сети, имеющее адрес 197.15.22.44, готовит передачу данных устройству, подключенному к сети организации X и имеющему IP-адрес 131.108.2.2. Эти данные движутся по Интернету, пока не достигают маршрутизатора, подключенного к сети организации. И здесь задача маршрутизатора состоит в том, чтобы определить, в какую из подсетей следует направить данные.

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

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

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

Чтобы лучше понять, как осуществляется операция логического умножения, рассмотрим работу маршрутизатора с различными видами масок подсети применительно к одной и той же сети. Возьмем сеть класса B с сетевым номером 172.16.0.0. После оценки потребностей сети сетевой администратор принимает решение заимствовать 8 бит для того, чтобы создать подсети. Как упоминалось выше, маска подсети в этом случае имеет вид 255.255. 255.0.

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

Теперь возьмем ту же сеть с адресом 172.16.0.0, но на этот раз сетевой администратор принимает решение заимствовать только 7 бит, чтобы создать подсети. В двоичной форме маска подсети для этого случая будет иметь вид 11111111.1111111.11111110.00000000.

Сети, изображенной на рисунке 3.18, присвоен адрес класса С 201.222.5.0. Предположим, необходимо организовать 20 подсетей, по 5 хостов в каждой. Можно разделить последний октет на части подсети и хостов и определить, какой вид будет иметь маска подсети. Размер поля подсети выбирается, исходя из требуемого количества подсетей. В этом примере выбор 29-битовой маски дает возможность иметь 221 подсеть. Адресами подсетей являются все адреса, кратные 8 (например, 201.222.5.16, 201.222.5.32 и 201.222.5.48).

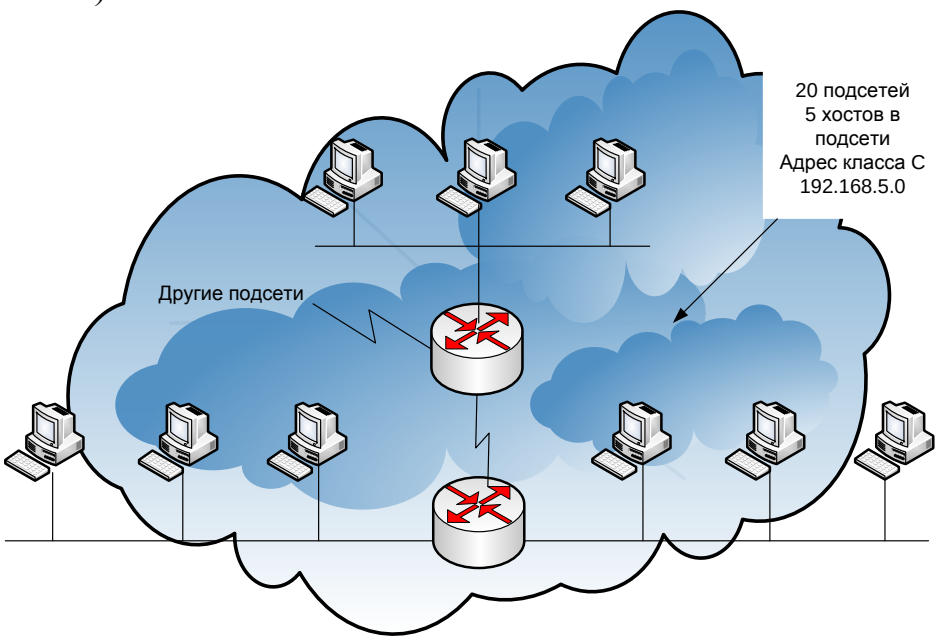


Рис. 3.18. Необходимо разделить сеть на 20 подсетей (по 5 хостов в каждой)

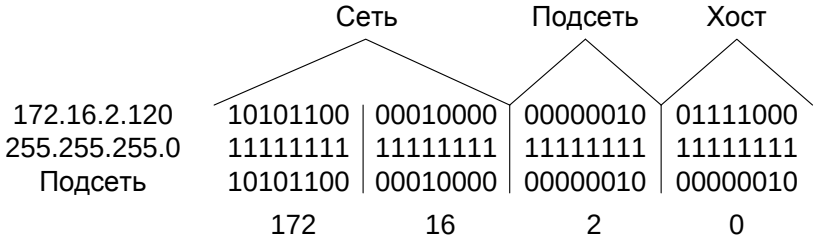
Оставшиеся биты в последнем октете используются для поля хост-машин. Для данного примера требуемое количество хост-машин равно 5, поэтому поле хост-машин должно содержать минимум 3 бита. Номера хост-машин могут быть 1, 2, 3 и т д. Окончательный вид адресов формируется путем сложения начального адреса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

Таблица 3.2 является примером таблицы, используемой для планирования подсетей. На рисунке 3.19 показано комбинирование входящих IP-адресов с маской подсети для получения номера подсети.

Таблица 3.2.

Планирование подсетей сети класса B

Количество бит для подсетей	**Номер маски подсети**	**Количество подсетей**	**Количество хост-машин**
2	255.255.192.0	2	16,385
3	255.255.224.0	6	8,190
4	255.255.240.0	14	4,094
5	255.255.252.0	30	2,046
6	255.255.248.0	62	1,022
7	255.255.254.0	126	510
8	255.255.255.0	254	254
9	255.255.255.128	510	126
10	255.255.255.192	1,022	62
11	255.255.255.224	2,046	30
12	255.255 255.240	4,094	14
13	255.255 255 248	8,190	6
14	255.255.255.252	16,382	2



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

Рис. 3.19. Пример планирования подсетей в сети класса B.
Выделение 8 бит для подсетей позволяет адресовать до 254 подсетей и 254 хостов

4. СЕТЕВОЙ УРОВЕНЬ И МАРШРУТИЗАЦИЯ

4.1. Идентификация составных частей сетевого адреса

Маршрутизаторы представляют собой устройства, которые реализуют сетевой сервис. Поскольку они являются активными и интеллектуальными узлами сети, то могут принимать участие в управлении сетью. Управление сетями достигается за счет обеспечения динамического контроля ресурсов и поддержки целей и задач сети, которые включают возможность установления связи, надежность в работе, управленческий контроль и гибкость. Маршрутизаторы в дополнение к базовым функциям коммутирования и маршрутизации также обеспечивают реализацию и других характеристик, которые помогают улучшить эффективность сети. К таким характеристикам относятся выстраивание последовательности прохождения трафика на основе приоритетов и его фильтрация. Часто маршрутизаторы требуются для поддержки множества протокольных групп, каждая из которых имеет свой собственный протокол маршрутизации, и для обеспечения параллельной работы различных сред. На практике маршрутизаторы имеют функции, которые позволяют создавать мостовые соединения, и, кроме того, могут играть роль усеченной формы концентратора.

Сетевой уровень для сетей играет роль интерфейсов и обеспечивает своему пользователю, транспортному уровню, сервис по наилучшей сквозной доставке пакетов. Сетевой уровень пересылает пакеты из сети источника в сеть пункта назначения. Выбор того, каким путем должен пойти трафик через сети, происходит на сетевом уровне. Функция выбора позволяет маршрутизатору оценивать имеющиеся пути до пункта назначения и устанавливать наилучший в этом плане метод обработки пакетов. Оценивая возможные пути, протоколы маршрутизации используют информацию о топологии сетей. Эта информация может конфигурироваться сетевым администратором или собираться посредством динамических процессов, выполняемых в сети.

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

На рисунке 4.1 показаны сети, в которых каждая связь между маршрутизаторами имеет номер, используемый маршрутизаторами в качестве адреса. Эти адреса должны нести в себе информацию, которая может быть использована в процессе маршрутизации. Это означает, что адрес должен содержать информацию о пути соединений сред передачи данных, которую процесс маршрутизации будет использовать для пересылки пакетов от отправителя в конечный пункт назначения. С помощью этих адресов сетевой

уровень может обеспечить организацию релейного соединения, которое будет связывать независимые сети. Непротиворечивость адресов уровня 3 во всем многосетевом комплексе также улучшает использование полосы пропускания, исключая необходимость в широковещательных рассылках. Широковещательные рассылки приводят к накладным расходам в виде ненужных процессов и напрасно расходуют мощности устройств или каналов связи, для которых эти широковещательные рассылки не предназначены. Благодаря использованию непротиворечивой сквозной адресации для представления пути соединений сред передачи данных сетевой уровень может находить путь до пункта назначения без ненужной загрузки устройств или каналов связи многосетевого комплекса широковещательными рассылками.

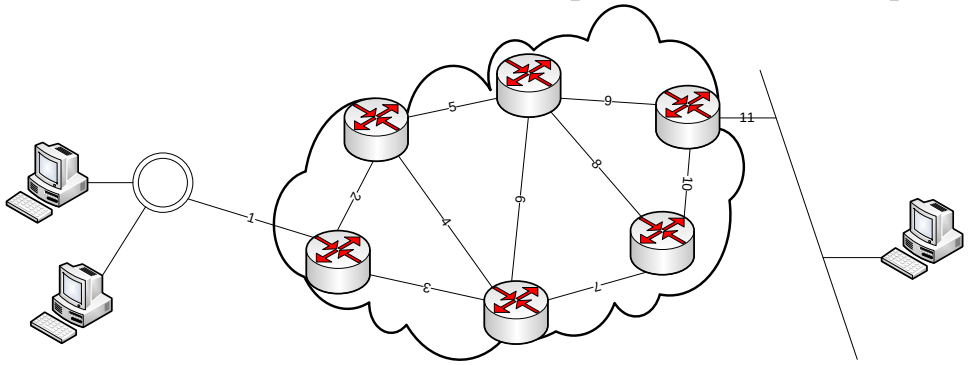


Рис. 4.1. Адреса отражают путь соединений сред передачи данных

На рис. 4.2 показаны три номера сетей: 1.1, 2.1 и 3.1, исходящих из маршрутизатора. Для некоторых протоколов сетевого уровня эти отношения задаются администратором сети, который назначает сетевые адреса в соответствии с планом адресации сетевого комплекса. Для других же протоколов сетевого уровня назначение адресов является частично или полностью динамическим. Большинство схем адресации в сетевых протоколах использует некоторую форму адреса хост-машины или узла. На рис. 3.3 показаны три хост-машины, использующие номер сети 1.

Сеть	Хост-машина
1	1 2 3
2	1
3	1

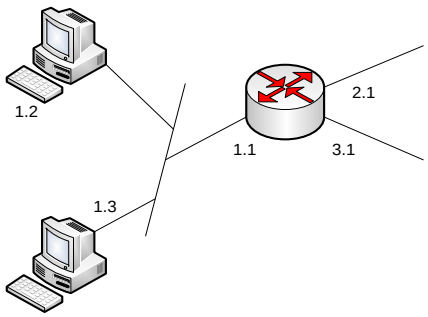


Рис. 4.2. Сетевой адрес состоит из сетевой части и части хост-машины

На рис. 4.3 показано, как маршрутизаторы используют адресацию для реализации своих основных функций маршрутизации и коммутации. Сетевая часть адреса используется для осуществления выбора пути, а узловая часть адреса говорит о порте маршрутизатора по пути следования. Функция коммутирования позволяет маршрутизатору принимать пакет на один интерфейс и переправлять его на другой, функция определения пути позволяет маршрутизатору выбрать наиболее подходящий интерфейс для переадресации пакета. Узловая часть адреса говорит о конкретном порте маршрутизатора, который имеет подключение к соседнему маршрутизатору в выбранном направлении.

Очень часто путают похожие термины *протокол маршрутизации (routing protocol)* и *маршрутизируемый протокол (routed protocol)* (рис. 4.4).

Маршрутизируемый протокол — любой сетевой протокол, который обеспечивает в адресе сетевого уровня достаточно информации, чтобы позволить передать пакет от одной хост-машины к другой на основе принятой схемы адресации. Маршрутизируемый протокол определяет формат и назначение полей внутри пакета. В общем случае пакеты переносятся от одной конечной системы к другой. Примером маршрутизируемого протокола является межсетевой протокол IP.

Протокол маршрутизации поддерживает маршрутизируемый протокол за счет предоставления механизмов коллективного использования маршрутной информации.

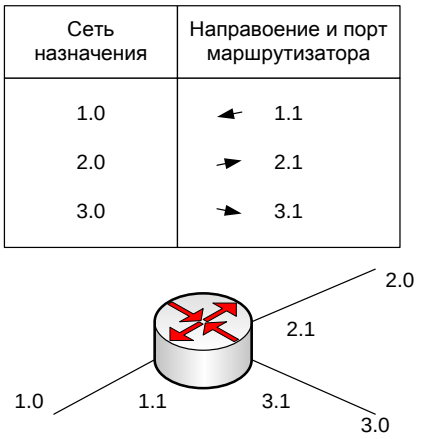
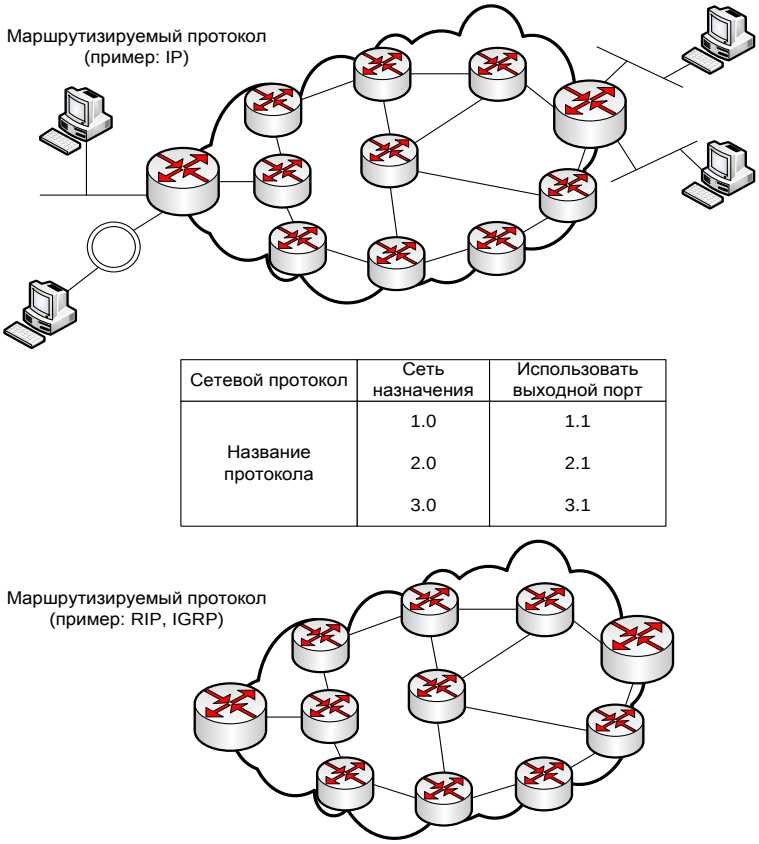


Рис. 4.3. Сетевая часть адреса используется для выбора пути

Сообщения протокола маршрутизации циркулируют между маршрутизаторами. Протокол маршрутизации позволяет маршрутизаторам обмениваться информацией с другими маршрутизаторами с целью актуализации и ведения таблиц. Примерами протоколов маршрутизации являются протокол маршрутной информации (RIP), протокол внутренней маршрутизации между шлюзами (IGRP), усовершенствованный протокол внутренней маршрутизации между шлюзами (EIGRP) и протокол маршрутизации с выбором кратчайшего пути (OSPF).



Сетевой протокол	Сеть назначения	Использовать выходной порт
Название протокола	1.0	1.1
	2.0	2.1
	3.0	3.1

Рис. 4.4. Маршрутизируемый протокол применяется для направления трафика, а протокол маршрутизации используется между маршрутизаторами для ведения таблиц

Маршрутизаторы способны поддерживать несколько независимых протоколов маршрутизации и вести таблицы маршрутизации для нескольких маршрутизируемых протоколов одновременно. Эта способность позволяет маршрутизатору доставлять пакеты нескольких маршрутизируемых протоколов по одним и тем же каналам передачи данных (рис. 4.5).

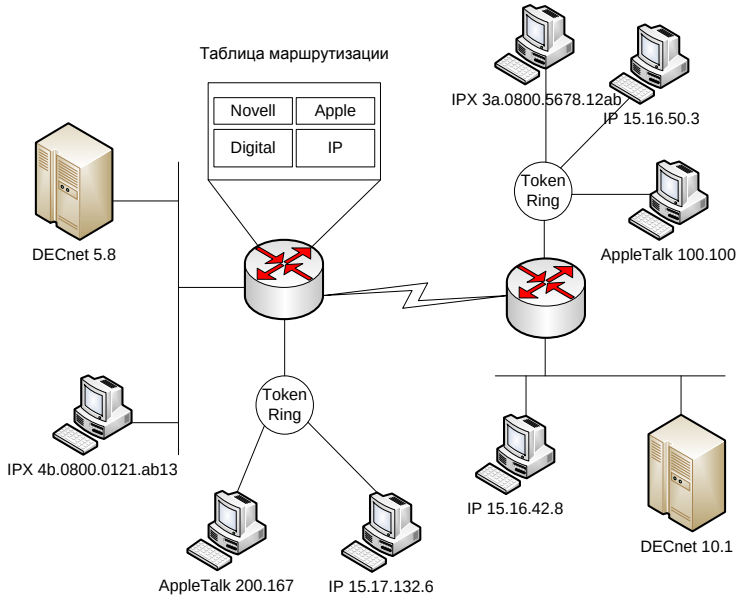


Рис. 4.5. Маршрутизаторы пропускают трафик всех маршрутизируемых протоколов, существующих в сети

Статическая информация администрируется вручную. Сетевой администратор вводит ее в конфигурацию маршрутизатора. Если изменение в топологии сети требует актуализации статической информации, то администратор сети должен вручную обновить соответствующую запись о статическом маршруте. Динамическая информация работает по-другому. После ввода администратором сети команд, запускающих функцию динамической маршрутизации, сведения о маршрутах обновляются процессом маршрутизации автоматически сразу после поступления из сети новой информации. Изменения в динамически получаемой информации распространяются между маршрутизаторами как часть процесса актуализации данных. Пример статического маршрута. Статическая маршрутизация имеет несколько полезных применений, которые связаны с привлечением специальных знаний администратора сети о сетевой топологии. Одним из таких применений является защита в сети. Динамическая маршрутизация раскрывает все, что известно о сети. Однако по причинам безопасности может понадобиться скрыть некоторые части сети. Статическая маршрутизация позволяет администратору сетевого комплекса задавать те сведения, которые могут сообщаться о закрытых частях сети.

Статический маршрут к сети также достаточен в том случае, если сеть доступна только по одному пути. Такой тип участка сетевого комплекса называется *тупиковой сетью.* Конфигурирование статического маршрута к тупиковой сети исключает накладные расходы, связанные с динамической маршрутизацией (рис. 4.6).

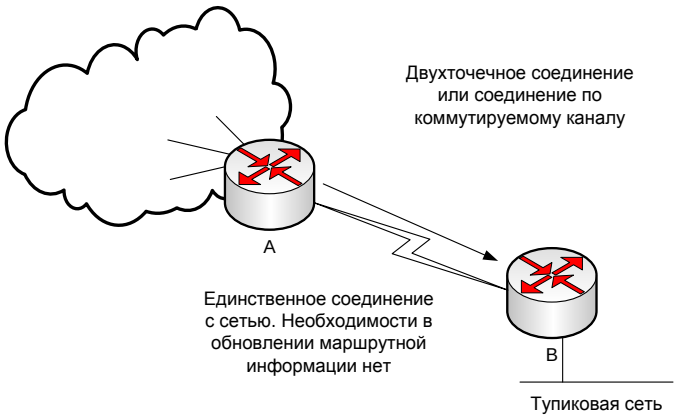


Рис. 4.6. Записи о статических маршрутах могут исключить необходимость в обновлении маршрутной информации по каналу глобальной сети

Пример маршрута по умолчанию. На рисунке 4.7 показано применение *маршрута по умолчанию* – записи в таблице маршрутизации, используемой для направления кадров, которые не имеют в таблице маршрутизации явно указанного следующего перехода. Маршруты по умолчанию могут устанавливаться как результат статического конфигурирования, выполняемого администратором.

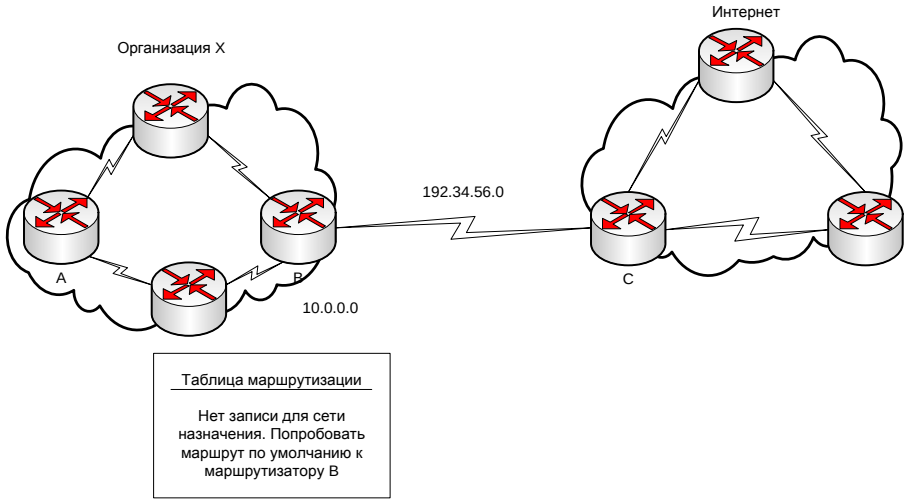


Рис.4.7. Маршрут по умолчанию используется только в тех случаях, когда следующий переход отсутствует в таблице маршрутизации в явном виде

В этом примере маршрутизаторы организации X «знают» только о топологии сети этой организации, но ничего «не знают» о других сетях.

Вместо сведений о каждой конкретной сети каждому маршрутизатору организации X сообщается маршрут по умолчанию, с помощью которого он может добраться до любого неизвестного пункта назначения, направляя пакет в сеть Интернет. Показанная на рисунке 4.8 сеть по-разному адаптируется к изменениям в топологии, в зависимости от того, используется статическая или динамическая информация.

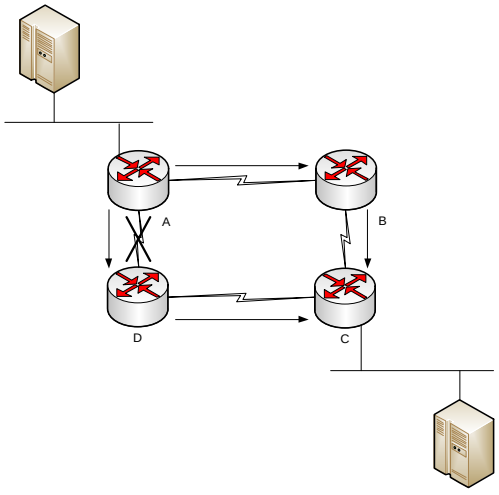


Рис. 4.8. Динамическая маршрутизация позволяет маршрутизаторам при необходимости автоматически использовать резервные маршруты

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

становится непроходимым, то маршрутизатор A не сможет ретранслировать пакет маршрутизатору D по статическому маршруту. Связь с сетью пункта назначения будет невозможна до тех пор, пока маршрутизатор A не будет реконфигурирован на ретрансляцию пакетов маршрутизатору B.

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

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

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

Эффективность динамической маршрутизации зависит от двух основных функций маршрутизатора:

– ведение таблицы маршрутизации;

– своевременное распространение информации – в виде пакетов актуализации среди других маршрутизаторов (рис. 4.9).

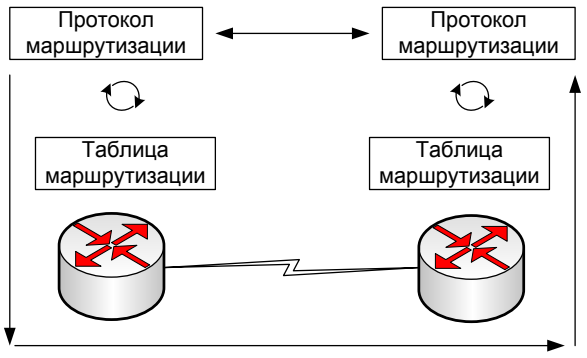


Рис. 4.9. Протоколы маршрутизации собирают и распространяют маршрутную информацию

Для обеспечения коллективного пользования информацией о маршрутах динамическая маршрутизация использует протокол маршрутизации. Протокол маршрутизации определяет набор правил, используемых маршрутизатором при его общении с соседними маршрутизаторами.

Например, протокол маршрутизации описывает:

– как отправляются пакеты актуализации;

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

Когда алгоритм маршрутизации обновляет таблицу маршрутизации, его главной целью является определение наилучшей информации для включения в таблицу. Каждый алгоритм маршрутизации интерпретирует понятие *наилучшая* по-своему. Для каждого пути в сети алгоритм генерирует число, называемое *метрикой.* Как правило, чем меньше величина этого числа, тем лучше путь (рис. 4.10).

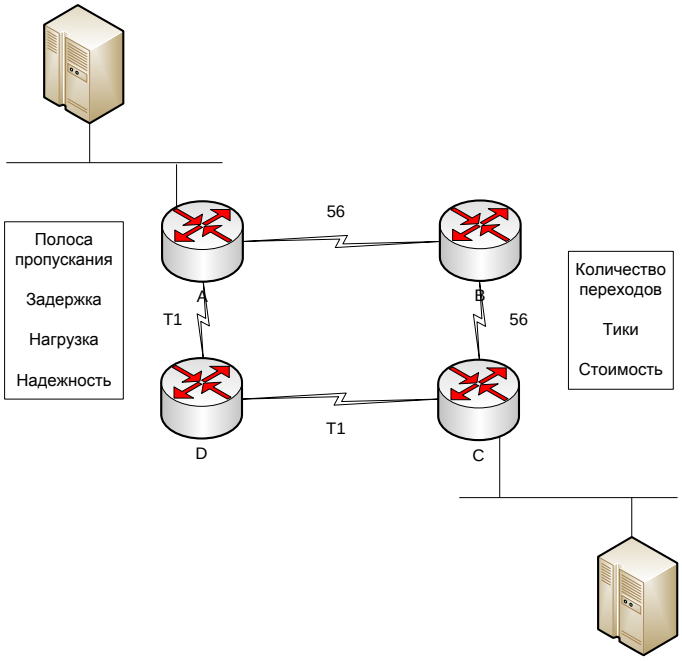


Рис. 4.10. Для нахождения наилучшего пути могут использоваться различные метрики

Метрики могут рассчитываться на основе одной характеристики пути. Объединяя несколько характеристик, можно рассчитывать и более сложные метрики. Как показано на рисунке 4.11, при вычислении значения метрики используется несколько характеристик пути.

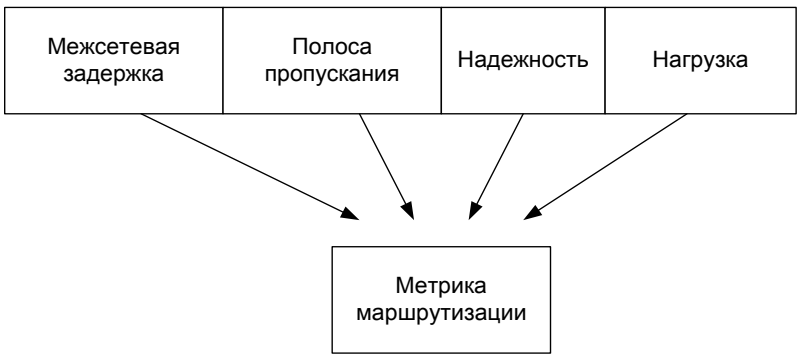


Рис. 4.11. Для вычисления метрик используется несколько характеристик пути

Наиболее общеупотребительными метриками, используемыми маршрутизаторами, являются следующие:

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

Полоса пропускания – пропускная способность канала передачи данных. Например, для арендуемой линии 64 Кбит/с обычно предпочтительным является канал типа T1 с полосой пропускания 1,544 Мбит/с.

Задержка – продолжительность времени, требующегося для перемещения пакета от отправителя получателю.

Нагрузка – объем действий, выполняемый сетевым ресурсом, например маршрутизатором или каналом.

Надежность – темп возникновения ошибок в каждом сетевом канале.

Тики – задержка в канале передачи данных, определяемая в машинных тактах.

Стоимость – произвольное значение, обычно основанное на величине полосы пропускания, денежной стоимости или результате других измерений, которое назначается сетевым администратором.

Большинство алгоритмов маршрутизации можно свести к трем основным алгоритмам (рис. 4.12).

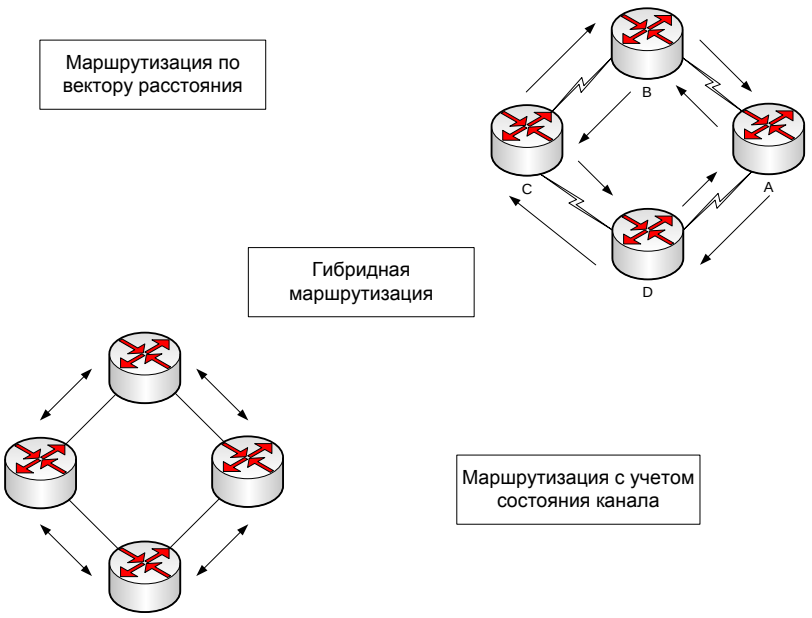


Рис. 4.12. Маршрутизация по вектору расстояния, с учётом состояния канала связи и гибридная – три основных типа алгоритмов маршрутизации

1. Подход на основе маршрутизации по вектору расстояния, в соответствии с которым определяются направление (вектор) и расстояние до каждого канала в сети.

2. Подход на основе оценки состояния канала (также называемый выбором наикратчайшего пути), при котором воссоздается точная топология всей сети (или, по крайней мере, той части, где размещается маршрутизатор).

3. Гибридный подход, объединяющий аспекты алгоритмов с определением вектора расстояния и оценки состояния канала.

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

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

4.2. Гибридная маршрутизация

Третий тип протоколов маршрутизации объединяет аспекты маршрутизации по вектору расстояния и маршрутизации с учетом состояния канала связи и называется *сбалансированной гибридной маршрутизацией.*

Для определения наилучших путей до сетей назначения протокол сбалансированной гибридной маршрутизации предусматривает использование векторов расстояния с более точной метрикой. Однако он отличается от большинства протоколов маршрутизации по вектору расстояния тем, что обновления базы данных маршрутной информации инициируются фактом изменения топологии.

Протоколы, относящиеся к типу сбалансированной гибридной маршрутизации, сходятся быстрее, приближаясь по этому показателю к протоколам маршрутизации с учетом состояния канала связи. Однако они отличаются от них меньшим потреблением таких ресурсов, как ширина полосы пропускания, объем памяти, и меньшими накладными расходами процессора. Примерами протоколов со сбалансированной гибридной маршрутизацией являются протокол взаимодействия открытых систем промежуточная система – промежуточная система (OSI Intermediate System – Intermediate System, IS-IS) и усовершенствованный протокол IGRP (EIGRP) компании Cisco. Вне зависимости от того, использует ли сеть механизмы маршрутизации по вектору расстояния или маршрутизации с учетом состояния канала

связи, ее маршрутизаторы должны выполнять одинаковые базовые функции маршрутизации. Сетевой уровень должен устанавливать связь и играть роль интерфейса с различными более низкими уровнями. Маршрутизаторы должны уметь без проблем работать с пакетами, инкапсулированными в различные кадры более низкого уровня, не меняя при этом адресацию пакета уровня 3. На рисунке 4.13 показан пример выполнения сетевым уровнем роли интерфейса в процессе маршрутизации из одной локальной сети в другую. В этом примере трафику пакетов из источника «хост 4», находящегося в сети 1 Ethernet, нужен путь к пункту назначения «хост 5» в сети 2.

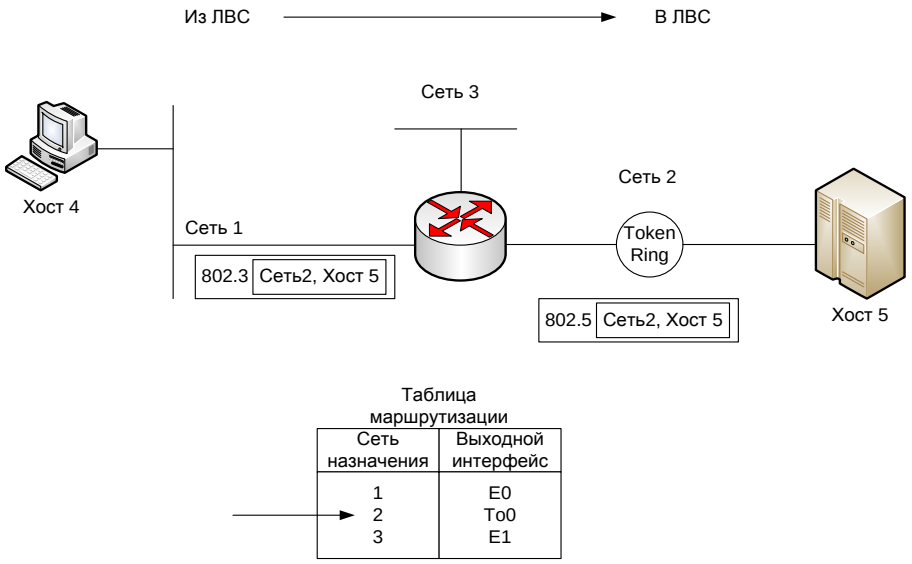


Рис. 4.13. При поиске маршрута маршрутизатор использует содержащийся в пакете сетевой адрес пункта назначения

Определение наилучшего пути для находящихся в локальных сетях хост-машин зависит от маршрутизатора и его непротиворечивой адресации сетей. Проверяя свои записи в таблице маршрутизации, маршрутизатор находит, что наилучший путь к сети 2 пункта назначения лежит через выходной порт To0 - интерфейс с ЛВС Token Ring.

Хотя формат кадра более низкого уровня должен измениться при коммутировании трафика маршрутизатором из сети 1 Ethernet в сеть 2 Token Ring, адресация источника и пункта назначения уровня 3 остается такой же. Как показано на рис. 4.13, адрес пункта назначения остается «Сеть 2, Хост 5», несмотря на другую инкапсуляцию более низкого уровня.

Для перенаправления трафика из локальной сети в глобальный сетевой уровень должен устанавливать связь и играть роль интерфейса с различными более низкими уровнями. По мере роста сетевого комплекса путь пакета может проходить через несколько точек ретрансляции и иметь дело с различными типами канального уровня, стоящими за различными локаль-

ными сетями. Например, на рисунке 4.14 пакет от показанной вверху рабочей станции с адресом 1.3 должен пройти три типа канальных уровней, чтобы попасть на файл-сервер с адресом 2.4, показанный внизу рисунка.

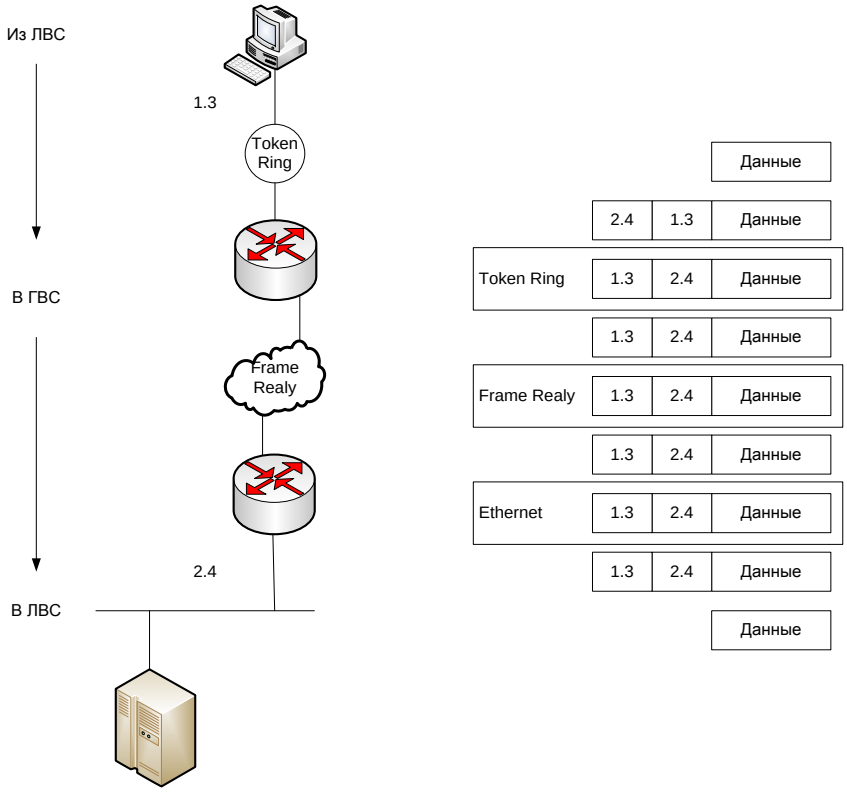


Рис. 4.14. При перенаправлении пакета маршрутизаторы сохраняют информацию о сквозном адресе

Маршрутизируемая связь осуществляется в следующей последовательности базовых шагов.

1. Рабочая станция посылает пакет файл-серверу, инкапсулируя его в кадр Token Ring, адресованный маршрутизатору A.

2. Когда маршрутизатор A получает кадр, он извлекает пакет из кадра Token Ring, инкапсулирует его в кадр Frame Relay и направляет этот кадр маршрутизатору B.

3. Маршрутизатор B извлекает пакет из кадра Frame Relay и переадресовывает его файл-серверу в составе вновь созданного кадра Ethernet.

4. Когда файл-сервер с адресом 2.4 принимает кадр Ethernet, он извлекает пакет и передает его соответствующему процессу более высокого уровня.

Маршрутизаторы обеспечивают возможность организации потока пакетов из локальной сети в глобальную за счет сохранения неизменными сквозных адресов источника и пункта назначения, инкапсулируя при этом пакет на порту в кадр канального уровня с форматом, соответствующим формату, используемому на следующем переходе пути.

5. КОНФИГУРИРОВАНИЕ МАРШРУТИЗАТОРОВ

5.1. Виртуальные локальные сети

Как показано на рисунке 5.1, виртуальная локальная сеть представляет собой логическое объединение устройств или пользователей. Объединение их в группу может производиться по выполняемым функциям, используемым приложениям, по отделам и т.д., независимо от их физического расположения в *сегментах (segment).* Конфигурирование виртуальной сети производится на коммутаторе программным путем. Виртуальные сети не стандартизированы и требуют использования программного обеспечения от производителя коммутатора.

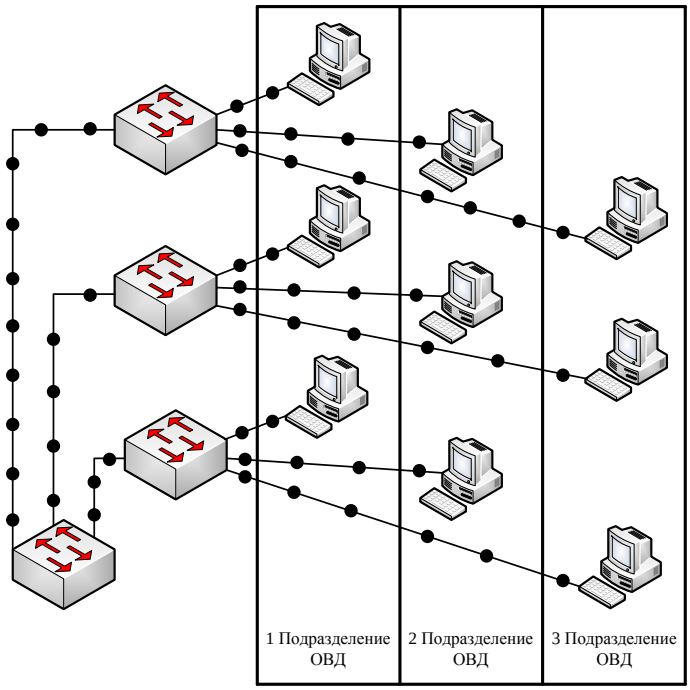


Рис. 5.1. Виртуальная сеть представляет собой группу устройств или пользователей, не ограниченную физическим сегментом сети

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

полосу пропускания, хотя требования к ней для различных групп и подразделений могут значительно различаться.

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

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

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

В локальных сетях, содержащих коммутирующие устройства, использование технологии виртуальных сетей представляет собой эффективный и экономически выгодный способ объединения пользователей сети в рабочие группы независимо от их физического расположения. На рисунке 5.2 проиллюстрированы различия между сегментацией в виртуальной сети и в обычной локальной сети.

Главными среди них являются следующие:

– виртуальные сети работают на 2-м и 3-м уровнях эталонной модели OSI;

– обмен информацией между виртуальными сетями обеспечивается маршрутизацией 3-го уровня;

– виртуальная сеть предоставляет средство управления широковещанием;

– включение пользователей в виртуальную сеть производится сетевым администратором;

– VLAN (Virtual Local Area Network) позволяет повысить степень защиты сети путем задания сетевых узлов, которым разрешено обмениваться информацией друг с другом.

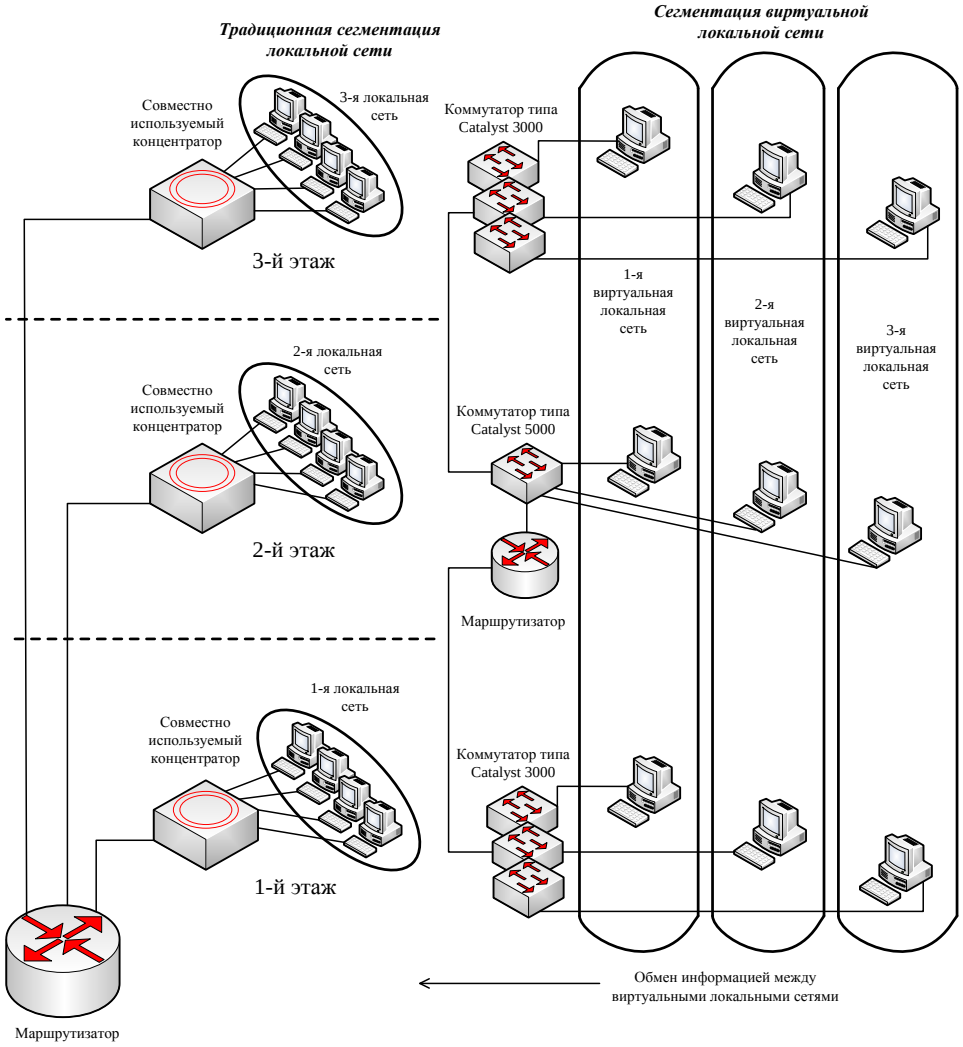


Рис. 5.2. В коммутируемой сети создание виртуальной сети обеспечивает сегментацию и организационную гибкость

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

– сотрудники одного отдела;

– группа сотрудников с пересекающимися функциями;

– различные группы пользователей, совместно использующих приложения или программное обеспечение.

Можно сгруппировать порты и пользователей в рабочую группу на одном коммутаторе или на нескольких соединенных между собой коммутаторах. Группируя порты и пользователей вокруг нескольких коммутаторов, можно создать инфраструктуру сети в одном здании, в нескольких соединенных между собой зданиях или даже сеть большой области, как показано на рис. 5.3.

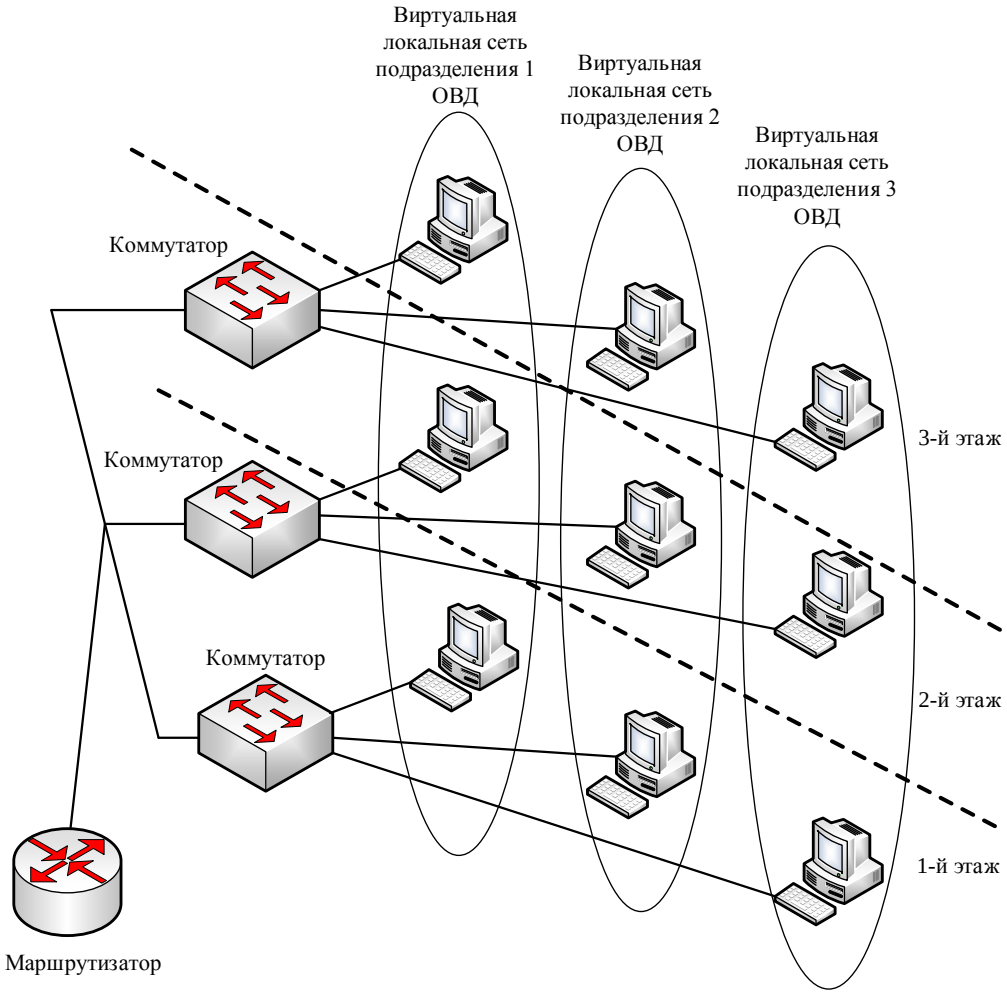


Рис. 5.3. Использование виртуальных сетей позволяет ликвидировать ограничения на обмен информацией между рабочими группами

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

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

5.2. Маршрутизаторы в виртуальных сетях

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

Маршрутизаторы остаются необходимыми и в коммутируемых архитектурах, в которых создана конфигурация виртуальной сети, поскольку они обеспечивают обмен информацией между логически определенными рабочими группами. Маршрутизаторы обеспечивают устройствам виртуальной сети доступ к совместно используемым ресурсам, таким как серверы и хосты. Они также обеспечивают связь с другими частями сети, которые логически сегментированы на основе традиционного подхода, основанного на выделении подсетей, или требуют доступа к удаленным серверам через каналы распределенных сетей. Обмен информацией на 3-м уровне, осуществляемый в коммутаторе или обеспечиваемый извне, является необходимым элементом любой высокопроизводительной коммутационной архитектуры. Внешние маршрутизаторы могут быть с высокой финансовой эффективностью интегрированы в коммутируемую архитектуру путем использования одного или нескольких высокоскоростных магистральных соединений.

Как правило, используются соединения *Gigabit Ethernet, 10-Gigabit Ethernet* или *ATM*, которые обладают следующими преимуществами:

– увеличенная пропускная способность соединений между коммутаторами и маршрутизаторами;

– использование всех физических портов маршрутизатора, требуемых для обмена информацией между *VLAN*;

– архитектура виртуальной локальной сети не только обеспечивает логическую сегментацию, но и значительно увеличивает эффективность работы сети.

Коммутаторы являются основными компонентами, обеспечивающими обмен данными в виртуальных сетях. Как показано на рисунке 5.4, в виртуальной сети они выполняют жизненно важные функции, являясь для устройств конечной станции точкой входа в среду коммутации, а также обеспечивают обмен данными в рамках всей организации.

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

Наиболее общими подходами к логической группировке пользователей в отдельные виртуальные сети являются фильтрация фреймов и их идентификация. Оба этих подхода характеризуются тем, что каждый фрейм исследуется при получении или отправке его коммутатором. Основываясь на

наборе правил, определяемом администратором, коммутаторы определяют, куда будет передан фрейм, будет ли он фильтроваться или передаваться широковещательно. Эти механизмы контроля могут применяться администратором централизованно (с использованием программного обеспечения для управления сетью) и легко реализуются во всей сети.

При фильтрации фреймов исследуется индивидуальная информация каждого фрейма. Для каждого коммутатора создается таблица фильтрации; это обеспечивает высокий уровень административного контроля, поскольку становится возможным исследование многих атрибутов каждого фрейма. В зависимости от типа коммутатора локальной сети (*LAN switch*) группировка может производиться на основе адресов управления доступом к передающей среде (*Media Access Control address*) или на основе протокола (*protocol*) сетевого уровня. Коммутатор сравнивает фильтруемые фреймы с элементами таблицы фильтрации и на этой основе предпринимает соответствующее действие.

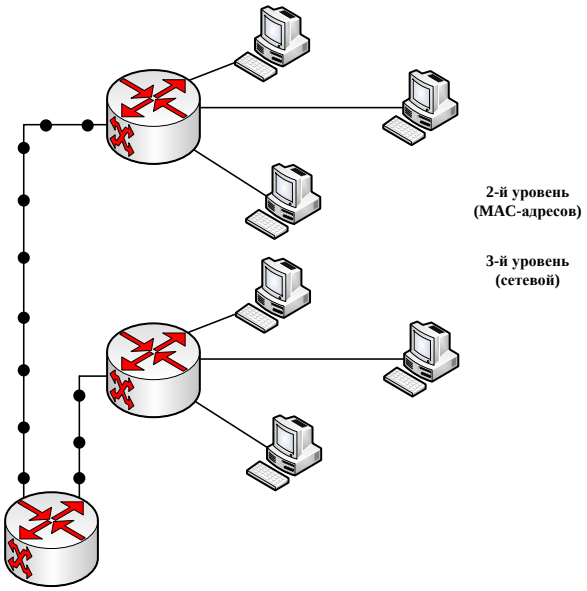


Рис. 5.4. Коммутаторы могут использоваться для группировки пользователей, портов или логических адресов в группы по интересам

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

При использовании тегов (*tag*) каждому фрейму назначается уникальный, определяемый пользователем идентификатор. Такой метод был избран отделом стандартов *Института инженеров по электротехнике и электронике (Institute of Electrical and Electronic Engineers, IEEE)* по той причине, что он допускает расширяемость сети. Использование фреймовых тегов получает все большее признание в качестве стандартного механизма распределения портов. По сравнению с фильтрацией фреймов он обеспечивает

большие возможности *расширения (scalability)* сети в пределах предприятия. Стандарт IEEE 802.lq регламентирует использование фреймовых тегов в качестве способа реализации виртуальной сети.

Использование фреймовых тегов при проектировании виртуальных сетей представляет собой подход, специально разработанный для коммутируемых коммуникаций. При использовании тегов в заголовок каждого фрейма при его отправке по сетевой магистрали помещается уникальный идентификатор. Этот идентификатор считывается и анализируется каждым коммутатором перед его широковещательной передачей или перед отправкой на другие коммутаторы, маршрутизаторы или устройства конечных станций. При выходе фрейма из сетевой магистрали и перед отправкой на конечную станцию коммутатор удаляет этот идентификатор из фрейма.

Процесс идентификации фреймов происходит на 2-м уровне эталонной модели OSI и не требует большой обработки или обмена служебными сообщениями.

Виртуальная сеть представляет собой коммутируемую сеть, в которой выполнено логическое сегментирование по исполняемым функциям, используемым приложениям или по принадлежности пользователей к определенному отделу, вне зависимости от физического расположения, их компьютеров. Каждый порт коммутатора может быть включен в виртуальную сеть. Все порты, включенные в одну виртуальную сеть, принимают широковещательные сообщения, в то время как порты, в нее не включенные, этих сообщений не принимают. Это повышает эффективность работы сети в целом.

В виртуальных сетях с центральным портом (port-centric VLAN) все узлы виртуальной сети подключены к одному и тому же интерфейсу маршрутизатора. На рис. 5.5 показано семейство пользователей виртуальной сети, подключенных к порту маршрутизатора.

Такое подключение облегчает работу администратора и повышает эффективность работы сети, поскольку:

– в виртуальной сети легко выполняются административные действия;

– повышается безопасность при обмене информацией между виртуальными сетями;

– пакеты не попадают в другие домены.

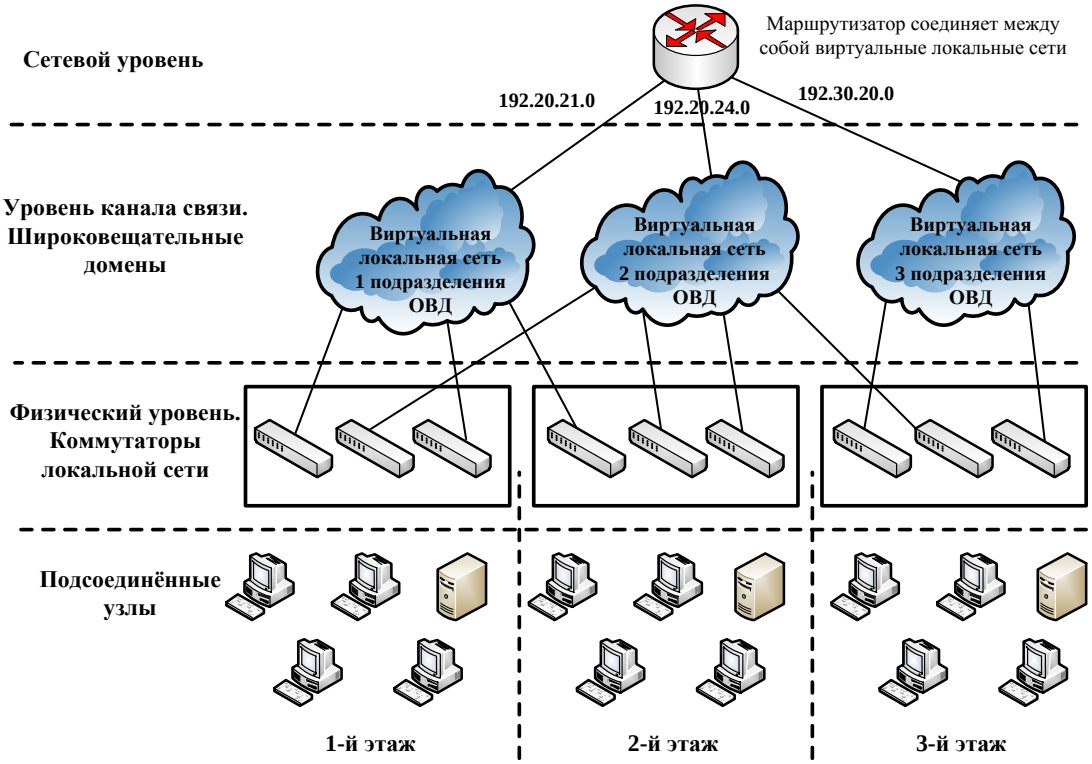


Рис. 5.5. В виртуальных сетях с центральным портом легко осуществляется контроль за всеми пользователями сети. Все узлы, подключенные к одному и тому же порту, должны находиться в одной виртуальной сети

5.3. Статические и динамические виртуальные сети

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

Динамические виртуальные сети (dynamic VLAN) представляют собой логическое объединение портов коммутатора, которые могут автоматически определять свое расположение в виртуальной сети. Функционирование динамической виртуальной сети основывается на MAC-адресах, на логической адресации или на типе протокола пакетов данных. При первоначальном подключении станции к неиспользуемому порту коммутатора соответствующий коммутатор проверяет MAC-адрес в базе данных управления

виртуальной сетью и динамически устанавливает соответствующую конфигурацию на данном порте. Основными достоинствами такого подхода является уменьшение объема работ в монтажном шкафу при добавлении нового пользователя или при переезде уже существующего и централизованное извещение всех пользователей при добавлении в сеть неопознанного пользователя. Основная работа в этом случае заключается в установке базы данных в программное обеспечение управления виртуальной сетью и в поддержании базы данных, содержащей точную информацию о всех пользователях сети.

В качестве достоинств виртуальных сетей можно выделить следующие их особенности:

– использование виртуальных сетей позволяет значительно экономить средства, затрачиваемые на решение вопросов, связанных с переездом в другое место, с появлением новых пользователей и с внесением изменений в структуру сети;

– виртуальные сети позволяют обеспечить контроль над широковещанием;

– они позволяют обеспечить защиту информации в рабочих группах и во всей сети;

– виртуальная сеть позволяет сэкономить средства за счет использования уже существующих коммутаторов.

Виртуальные сети представляют собой эффективный механизм управления изменениями физического расположения сетевых компонентов и узлов, а также уменьшения расходов, связанных с установкой новой конфигурации коммутаторов и маршрутизаторов. Пользователи виртуальной локальной сети могут совместно использовать одно и то же сетевое адресное пространство (IP-подсеть) независимо от их физического расположения. Если пользователь виртуальной сети переезжает из одного места в другое, оставаясь внутри той же самой виртуальной сети и оставаясь подключенным к тому же самому порту коммутатора, то его сетевой адрес не изменяется. Изменение положения пользователя требует всего лишь подключения его компьютера к одному из портов коммутатора и включения этого порта в прежнюю виртуальную сеть, как показано на рисунке 5.6.

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

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

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

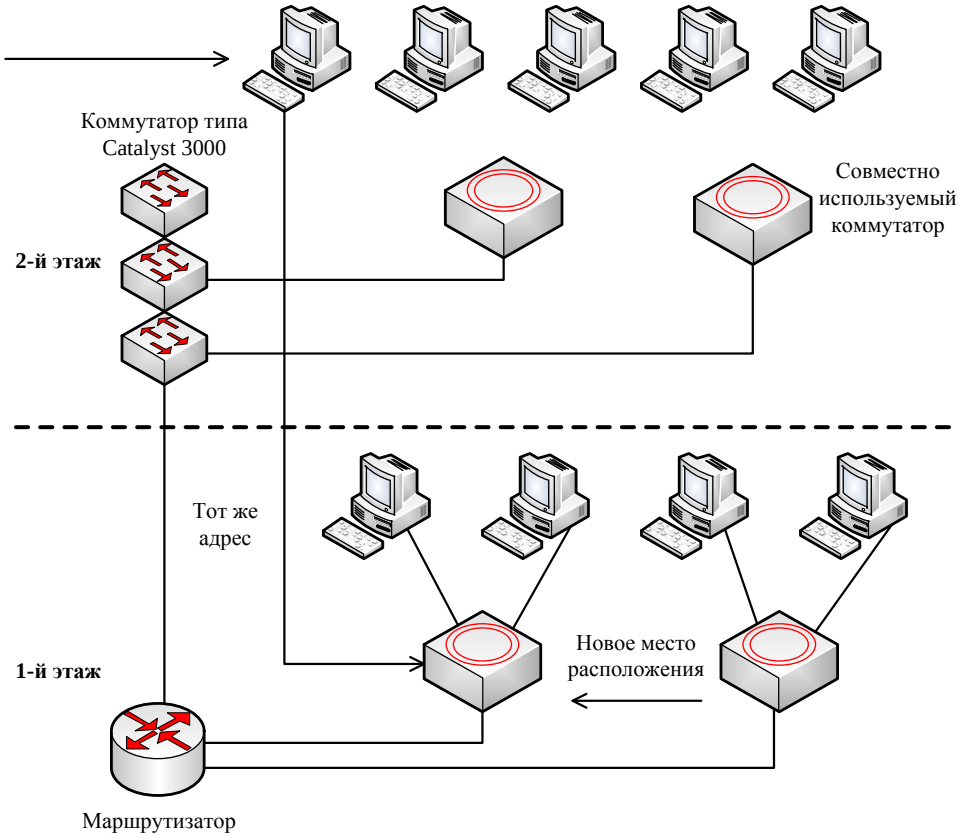


Рис. 5.6. Коммутаторы, способные создавать виртуальные сети, значительно упрощают решение проблем, связанных с изменением схемы прокладки кабелей, конфигурации сети, с переездом пользователя в другое место, а также задач отладки при повторном подсоединении пользователя к сети

Одним из эффективных в финансовом отношении и легко административно реализуемых методов повышения безопасности является сегментация сети на большое количество широковещательных групп, как показано на рисунке 5.7.

Это позволяет сетевому администратору:

– ограничить количество пользователей в группе виртуальной сети;

– запретить другим пользователям подсоединение без предварительного получения разрешения от приложения, управляющего виртуальной сетью;

– установить конфигурацию всех неиспользуемых портов в принимаемое по умолчанию состояние низкой активности VLAN.

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

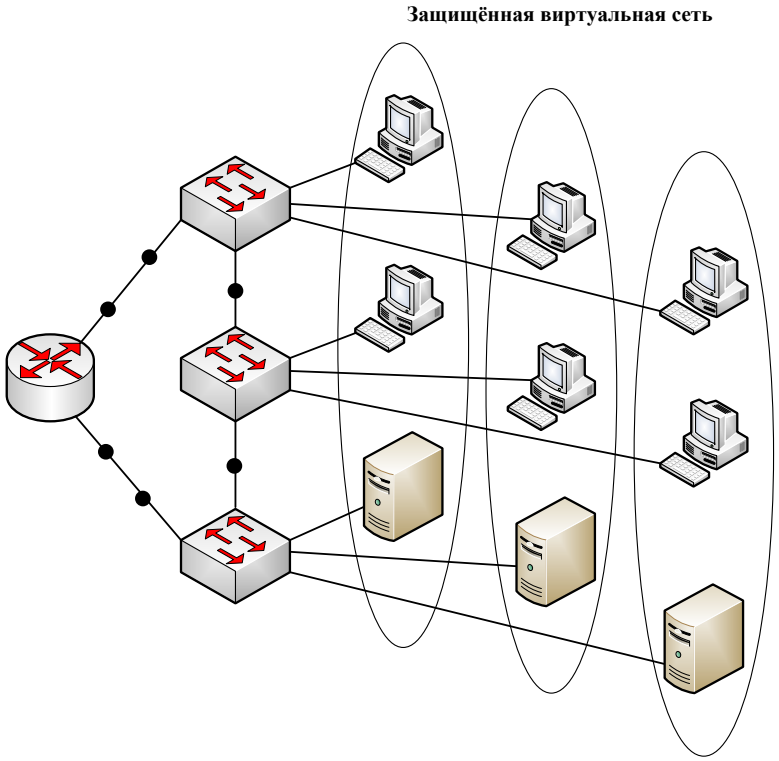


Рис. 5.7. Виртуальные сети позволяют использовать брандмауэры, ограничить доступ индивидуальных пользователей и уведомляют системного администратора о несанкционированном доступе в сеть

Обеспечить большую безопасность можно путем использования *списков управления доступом (access control list, ACL)*.

В защищенной виртуальной сети маршрутизатор ограничивает доступ к сетевой информации посредством задания соответствующей конфигурации коммутаторов и маршрутизаторов. Ограничения доступа могут основываться на адресах станций, типах приложений, типах протоколов времени.

ЗАКЛЮЧЕНИЕ

Компьютерные сети – целый мир интереснейших событий, сведений и технологий. Сегодня вычислительные сети продолжают быстро развиваться. Разрыв между локальными и глобальными сетями постоянно сокращается во многом из-за появления высокоскоростных территориальных каналов связи, не уступающих по качеству кабельным системам локальных сетей. Тема «Сетевые технологии передачи данных» очень широка и многогранна, а быстрый рост числа компьютерных сетей и их развитие сопровождаются сменой или совершенствованием сетевых технологий.

В глобальных сетях появляются службы доступа к ресурсам, такие же удобные и прозрачные, как и службы локальных сетей. Изменяются и локальные сети. Появилось разнообразное коммуникационное оборудование – коммутаторы, маршрутизаторы, шлюзы. Благодаря такому оборудованию имеется возможность построения больших корпоративных сетей, имеющих сложную структуру. Быстро и успешно развиваются беспроводные сети, сейчас уже можно говорить, что они конкурируют с традиционными сетями, построенными на кабельных линиях связи.

Еще одна очень важная тенденция – стали применяться методы обработки аудио- и видеоинформации в сетях. Сложность передачи такой информации, получившей название мультимедийной, по сети связана с ее чувствительностью к задержкам при передаче: задержки обычно приводят к искажению информации в конечных узлах сети. Сегодня эти проблемы решаются различными способами, но, несмотря на значительные усилия, предпринимаемые в этом направлении, до приемлемого решения проблемы пока далеко. Компьютерные сети уже сегодня работают на пределе своих возможностей, и нагрузку, которую предстоит испытать сетям при таком активном росте, они могут просто не выдержать. Развитие всех перечисленных тенденций возможно только после внедрения новой, более гибкой архитектуры компьютерных сетей.

Самая перспективная на сегодня технология/архитектура компьютерных сетей, которая способна вывести из кризиса, – технология программно-конфигурируемых сетей (ПКС). Ее основная ценность в том, что она позволяет уйти от «ручного» управления сетью, выводя на первый план программное обеспечение.

К основным направлениям и путям развития компьютерных сетей можно отнести следующие:

1. Развитие топологии сетей, направленное на обеспечение одновременного обслуживания запросов от большего количества абонентских систем и увеличение оперативности и надежности доставки пакетов адресатам за счет создания альтернативных маршрутов.

2. Создание новых, более совершенных протоколов обмена информацией и управления сетями, развитие информационных и телекоммуникационных технологий.

3. Совершенствование существующих и создание новых аппаратных средств передачи и обработки информации

4. Развитие программного обеспечения сетей.

5. Повышение надежности сетей по всем аспектам – техническому, программному, информационному, функциональному.

6. Развитие методов и средств обеспечения более высокого уровня безопасности информации, циркулирующей в сетях.

7. Расширение перечня предоставляемых информационно-вычислительных услуг.

8. Рациональная организация обслуживания очередей запросов пользователей сети.

9. Повышение эргономичности компьютерных сетей, достигаемое путем оптимизации трудовой деятельности пользователей сети, ее управленческого и обслуживающего персонала.

10. Создание и непрерывное совершенствование глобальной интеллектуальной сети, объединяющей сети всех государств. В рамках такой сети вполне реально решение задачи по удовлетворению запроса пользователя из любой точки планеты и в любое время.

В современных сетях функции управления и передачи данных совмещены, что делает контроль и управление очень сложными. ПКС-архитектура разделяет процесс управления и процесс передачи данных, что открывает колоссальные возможности для развития интернет-технологий.

СПИСОК ИСПОЛЬЗУЕМОЙ ЛИТЕРАТУРЫ

1. О связи : Федеральный закон от 7 июля 2003 года № 126-ФЗ (с изм. от 24.12.2023) // СПС «КонсультантПлюс».

2. Об утверждении структуры интегрированной мультисервисной телекоммуникационной системы органов внутренних дел : приказ МВД России от 26 сентября 2006 № 763 // СПС «КонсультантПлюс».

3. Берилин А. Н. Телекоммуникационные сети и устройства / А. Н. Берилин. – Москва : Биом, 2014. – 320 с.

4. Будылдина Н. В. Сетевые технологии высокоскоростной передачи данных : учебное пособие для вузов / Н. В. Будылдина; под ред. В. П. Шувалова. – Москва : Горячая линия – Телеком, 2016. – 342 с.

5. Добровольский Е. Е. Развитие и совершенствование радиосвязи, радиовещания и телевидения / Е. Е. Добровольский. – Москва, 2014. – 123 с.

6. Корячко В. П. Компьютерные сети: технологии, протоколы, алгоритмы: монография / В. П. Корячко, Д. А. Перепелкин. – Москва : Горячая линия – Телеком, 2017. – 216 с: ил.

7. Лукьянов А. С. Основы построения инфокоммуникационных систем и сетей : учебное пособие / А. С. Лукьянов. – Воронеж : Воронежский институт МВД России, 2022. – 79 с.

8. Самуйлов К. Е. Сети и системы передачи информации. Телекоммуникационные сети. Учебник и практикум / К. Е. Самуйлов. – Москва : Юрайт, 2017. – 346 с.

9. Семенов А. Б. Структурированные кабельные системы / А. Б. Семенов. – Москва : ДМКПресс, 2013. – 640 с.

10. Соболь Б. В. Сети и телекоммуникации : учебное пособие / Б. В. Соболь. – Ростов–на–Дону : Феникс, 2015. – 192 с.

11. Стрекалов А. В. Физические основы волоконной оптики / А. В. Стрекалов. – Москва : Дрофа, 2013. – 112 с.

12. Тимошкина, М. А. Повышение скорости передачи данных в мультисервисных сетях / М. А. Тимошкина. – Москва : LAP Lambert Academic Publishing, 2014. – 136 с.

13. Шевченко В. П. Вычислительные системы, сети и телекоммуникации / В. П. Шевченко. – Москва : Дрофа, 2017. – 245 с.

14. Шерстюков С. А. Принципы и практика использования информационных и технологических возможностей ЕИТКС ОВД Российской Федерации. Часть II / С. А. Шерстюков, Д. А. Жайворонок, А. Ю. Кожин. – Воронеж : Воронежский институт МВД России, 2010. – 72 с.

Учебное издание

Лукьянов Александр Сергеевич,
кандидат технических наук;
Терентьев Александр Андреевич,
кандидат технических наук;
Попов Алексей Вячеславович,
кандидат технических наук

СЕТЕВЫЕ ТЕХНОЛОГИИ ПЕРЕДАЧИ ДАННЫХ

Учебное пособие

Редактор А. Г. Лиопа
Компьютерная верстка А. С. Лукьянова

Подписано в печать 20.05.2024
Формат 60×84 1/16
Усл. печ. л. 4,88
Тираж 50 экз.
Заказ № 175

Воронежский институт МВД России
394065, Воронеж, просп. Патриотов, 53

Типография Воронежского института МВД России
394065, Воронеж, просп. Патриотов,53